Co-funded by the European Union

LOTTA ALLE TRUFFE SENTIMENTALI

2023-1-DE02-KA210-VET-000151265

Abstract

Fight Against Love Scam (FALS) è un'iniziativa europea creata per proteggere e rafforzare gli adulti over 50 dalle truffe sentimentali online. Il progetto riunisce partner provenienti da Germania, Paesi Bassi e Italia per sensibilizzare e fornire a educatori per adulti, anziani e alle loro famiglie le conoscenze e gli strumenti per riconoscere, prevenire e rispondere alle truffe sentimentali.

Attraverso la creazione di una guida digitale, test pratici e un corso online, FALS promuove la sicurezza online, il benessere emotivo e l'invecchiamento attivo. Il progetto incoraggia inoltre la collaborazione tra educatori, assistenti sociali e comunità per costruire sistemi di supporto più solidi per gli anziani.
Combinando istruzione, prevenzione ed empatia, FALS si impegna a rendere il mondo digitale uno spazio più sicuro per tutti.

Partner del progetto

EUTH WONDERS E.V

IGOR VITALE INTERNATIONAL

ECREC

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.

Indice

Co-funded by the European Union

Un messaggio dai partner del progetto

Cari lettori,

Vi diamo un caloroso benvenuto a questa guida, frutto del nostro impegno condiviso in Germania, Paesi Bassi e Italia per sostenere e dare forza a uno dei segmenti più vulnerabili della nostra società: gli anziani che navigano nel mondo digitale.

Fight Against Love Scam (FALS) nasce da un'esigenza semplice ma urgente: prevenire i danni emotivi e finanziari causati dalle truffe sentimentali e fornire a educatori per adulti, famiglie e anziani stessi gli strumenti per proteggersi online. Troppe persone sono state colpite in silenzio e crediamo che sia giunto il momento di portare la conoscenza, l'assistenza e la comunità al centro dell'attenzione.
Questo opuscolo è più di una risorsa educativa: è un gesto di solidarietà e rispetto. Offre spunti, indicazioni pratiche ed esperienze condivise per aiutare a riconoscere i segnali d'allarme, rafforzare la resilienza digitale e sostenersi a vicenda nella gestione delle relazioni online.

Ci auguriamo che queste pagine vi diano conforto, chiarezza e sicurezza.

Cordiali saluti,

Il team FALS
EUW (Germania)
ECREC (Paesi Bassi)
IVI (Italia)

Panoramica del manuale

Contenuti del manuale

Il manuale contiene 3 capitoli che formulano il contenuto del manuale metodologico:

1. Dietro la maschera: comprendere le truffe amorose Sostenere
2. con cura: buone pratiche per gli educatori Difesa digitale:
3. nozioni di base sulla sicurezza informatica per principianti
4. Conoscere e crescere: autovalutazione e valutazione.

Elementi chiave dei capitoli

Capitolo 1: Una panoramica su cosa sono le truffe amorose, come si verificano e come riconoscerle e prevenirle.

Capitolo 2: Guida pratica per educatori per adulti su come supportare gli anziani, riconoscere la vulnerabilità psicologica e rispondere alle truffe.

Capitolo 3: Introduzione alla sicurezza online, al rilevamento del phishing e alla consapevolezza della piattaforma per utenti non esperti di tecnologia.

Capitolo 4: Una serie di brevi test per valutare la comprensione delle truffe amorose, la consapevolezza emotiva e la sicurezza digitale. Include un'analisi basata su infografiche.

Informazioni su FALS

Co-funded by
the European Union

Introduzione

Il mondo digitale ha aperto innumerevoli opportunità di connessione, ma con esse si presentano anche nuove forme di rischio. Una delle minacce emotivamente più dannose per gli anziani oggi è la "truffa dell'amore", una forma di frode online che fa leva sulla vulnerabilità e sulla fiducia.

Il progetto Fight Against Love Scam (FALS) è stato lanciato come collaborazione europea tra partner in Germania, Paesi Bassi e Italia con una missione comune: proteggere, informare e responsabilizzare le persone dai 50 anni in su e coloro che le sostengono. Attraverso questo manuale, miriamo a fornire agli educatori per adulti le conoscenze e gli strumenti necessari per identificare i segnali delle truffe sentimentali online, offrire supporto psicologico e sociale e insegnare le pratiche di base della sicurezza informatica in modo accessibile ed empatico.

Questa guida non è solo un manuale, è un invito all'azione. Sensibilizzando e rafforzando le competenze di educatori e operatori socio-sanitari, possiamo prevenire i danni, supportare il recupero e promuovere la dignità e la sicurezza negli spazi digitali per gli anziani.

Ti invitiamo a esplorare i capitoli successivi, ognuno pensato per aiutarti a diventare un difensore, un protettore e un educatore più forte nella lotta contro le truffe amorose.

OBIETTIVI FALS

- **Sensibilizzare gli adulti più anziani (50+)** sui rischi e le tattiche delle truffe sentimentali online, aiutandoli a riconoscere i segnali d'allarme ed evitare danni emotivi e finanziari.
- **Fornire agli educatori per adulti** strumenti, conoscenze e metodologie per supportare gli anziani negli spazi digitali e individuare i primi segnali di vulnerabilità psicologica.
- **Supportare le famiglie e chi si prende cura dei propri cari** fornendo loro indicazioni pratiche per aiutarli a identificare i segnali di allarme, comunicare con i propri cari e reagire in modo appropriato alle sospette truffe.
- **Promuovere la sicurezza digitale** introducendo le nozioni fondamentali sulla sicurezza informatica che aiutano gli anziani a navigare sulle piattaforme online in modo più sicuro ed evitare interazioni ad alto rischio.
- **Creare uno strumento educativo sostenibile** attraverso lo sviluppo di una guida completa, di test di autovalutazione e di un corso video digitale che possa essere utilizzato da centri di istruzione per adulti, assistenti sociali e familiari in tutta Europa.
- **Incoraggiare l'invecchiamento attivo e la resilienza** promuovendo l'alfabetizzazione digitale e il benessere emotivo, consentendo agli anziani di rimanere coinvolti, indipendenti e sicuri nelle loro interazioni online.

Gruppi target

01 Gruppo target primario: anziani (50+ anni):

- I principali beneficiari del progetto. Questo gruppo è sempre più attivo online, ma spesso non ha le competenze digitali o il supporto emotivo necessari per proteggersi dalle truffe sentimentali e dalle frodi online correlate. Il progetto mira specificamente a rafforzare la loro consapevolezza, resilienza e sicurezza digitale.

02 Educatori e formatori per adulti

- Professionisti che lavorano nell'istruzione degli adulti, nei centri comunitari o nei programmi di alfabetizzazione digitale, che saranno formati e dotati degli strumenti per identificare, prevenire e affrontare le truffe amorose tra gli studenti più grandi.

03 Familiari e assistenti

- Parenti e contatti stretti degli anziani, che sono spesso i primi a notare cambiamenti comportamentali e possono offrire supporto emotivo o logistico in caso di sospetta truffa.

04 Assistenza sanitaria, assistenti sociali, centri comunitari, ONG e istituti di istruzione per adulti

- Professionisti che possono lavorare con anziani che soffrono di disagio psicologico a causa di truffe o vulnerabilità alla manipolazione online.
- Enti che possono adottare il manuale, le risorse formative e il corso digitale sviluppati da FALS nelle loro attività educative o di sensibilizzazione.

Dietro la maschera: capire le truffe amorose

Co-funded by
the European Union

Agnese Federica Gobbi

Agnese Federica Gobbi, nata in Slovenia, ha conseguito una laurea triennale in scienze e tecniche psicologiche e sta attualmente conseguendo una laurea magistrale in psicologia presso l'Università Guglielmo Marconi di Roma. Dal 2022 è una preziosa collaboratrice di Igor Vitale International s.r.l., dove si occupa di produzione audio-video, fotografia, content writing e creazione di pagine web. Agnese ha contribuito attivamente a oltre 15 progetti in diversi settori come l'ospitalità, l'artigianato, l'ecologia e la psicologia. Il suo lavoro l'ha portata in varie parti d'Europa, nei Caraibi d'Oltremare, nella Polinesia Francese, Oceano Pacifico, in Groenlandia e in regioni dell'Asia meridionale e orientale, mettendo a frutto la sua prospettiva globale e la sua competenza multidisciplinare.

1 INTRODUZIONE AL LOVE SCAM

La truffa dell'amore, nota anche come truffa romantica, rappresenta una forma di frode online in cui i truffatori sfruttano i legami emotivi per ingannare le persone a scopo di lucro. Radicate in tattiche di inganno storiche, come la truffa del "prigioniero spagnolo" del XVI secolo, le moderne truffe romantiche continuano a manipolare le vittime costruendo relazioni false e personaggi idealizzati. La proliferazione di piattaforme di comunicazione digitale ha fornito terreno fertile per questi schemi, consentendo ai truffatori di operare in modo anonimo ed espandere la loro portata a livello globale. Le vittime sono spesso attirate da profili accuratamente creati e storie convincenti, che causano significativi danni emotivi e finanziari (Cemmi, n.d.; Coluccia et al., 2020; Europol, 2023). Negli ultimi anni, le truffe d'amore sono diventate più sofisticate, con i truffatori che impiegano varie tattiche psicologiche per stabilire il controllo sulle vittime e garantire la conformità. Comprendere i meccanismi e gli impatti delle truffe d'amore, nonché riconoscere i primi segnali di allarme, è essenziale per combattere queste attività fraudolente.

1.1 Cos'è una truffa d'amore

La truffa dell'amore, nota a livello internazionale come romance scam, è una tipologia di frode digitale in cui i truffatori manipolano le vittime per ottenere denaro sfruttando false promesse d'amore tramite internet. Secondo una sentenza della Corte di Cassazione italiana (n. 25165/2019), chi finge un interesse romantico al solo scopo di ottenere vantaggi economici o materiali è perseguibile ai sensi dell'articolo 640 del codice penale (Coluccia et al., 2020 in Cemmi, n.d.). L'uso diffuso della tecnologia ha facilitato l'ascesa e l'evoluzione di queste truffe. Uno studio condotto in Italia ha rilevato che il 3% della popolazione è vittima di truffe sentimentali, con un'incidenza maggiore tra le donne di età compresa tra 40 e 60 anni. Questo gruppo tende a idealizzare le relazioni e a ricercare emozioni intense, rendendole più vulnerabili. Tuttavia, la vittimizzazione può colpire anche individui di successo professionale, come manager ed educatori (Cemmi, n.d.; Commissariato di PS, n.d.). Sebbene oggi si svolgano principalmente su piattaforme digitali, le truffe sentimentali hanno radici antiche. Un esempio precoce è la "truffa del prigioniero spagnolo" del XVI secolo, che prendeva di mira individui facoltosi. In questo schema, il truffatore si spacciava per un nobile spagnolo ingiustamente imprigionato con una fortuna nascosta. Fingendo di essere disperato, chiedeva denaro per la sua liberazione, promettendo in cambio una parte della sua fortuna.

Per rendere il piano più allettante, il truffatore menzionava una bellissima figlia nubile, usando richiami romantici e familiari per evocare empatia e coinvolgimento emotivo nelle sue vittime (Beek, 2016 in Cunha, n.d.; Gillespie, 2017 in Cunha, n.d.). L'analisi della truffa del prigioniero spagnolo fornisce una panoramica sui fondamenti della moderna truffa sentimentale. Nonostante i secoli trascorsi, il nucleo della frode si basa ancora sulla manipolazione emotiva. Sebbene metodi e tecnologie si siano evoluti, il piano rimane fondamentalmente invariato: il truffatore costruisce un rapporto di fiducia, facendo leva su promesse d'amore e di una futura vita insieme, inducendo la vittima a consegnare denaro e beni (Cunha, n.d.). Questa frode, tra le più ingegnose e di successo del suo tempo, richiedeva il coordinamento tra diversi paesi, rendendo difficile identificare e arrestare i truffatori. La collaborazione tra diverse giurisdizioni e la complessità logistica hanno permesso a questi truffatori di operare con un certo livello di impunità, sfruttando le limitate capacità di comunicazione e di applicazione della legge dell'epoca (Gregory & Nikiforova, 2012 in Cunha, n.d.).

Le frodi online, comprese le truffe sentimentali, comprendono un'ampia gamma di attività illecite e si basano su tecnologie digitali, tra cui social media e app di incontri, per attrarre e ingannare le vittime. I truffatori utilizzano strumenti digitali come VPN e RAT per mantenere l'anonimato e accedere alle informazioni personali e finanziarie delle vittime, con l'obiettivo di creare dipendenza emotiva e richiedere continuamente denaro (EUROPOL, 2023; Wang, 2022).

Le truffe sentimentali seguono in genere uno schema in cui il truffatore costruisce un legame emotivo con la vittima attraverso profili idealizzati e storie tragiche. Questo processo può durare mesi, portando la vittima a sviluppare un forte attaccamento emotivo al truffatore virtuale, una dinamica che, oltre alla perdita finanziaria, causa un significativo danno psicologico (Whitty, 2015, 2012, 2018, 2013 in Wang, 2022; Dodge, 2016 in Wang, 2022).

1.2 Come riconoscere i segnali d'allarme e prevenirli

Le truffe sentimentali impiegano sofisticate tattiche di manipolazione psicologica per stabilire un controllo emotivo e finanziario sulle vittime. Sebbene le truffe sentimentali siano una tipologia di crimine informatico relativamente moderna, si basano su una serie di tattiche ben studiate volte a sfruttare le vulnerabilità emotive per ottenere un guadagno economico.

Gli studi hanno identificato strategie ricorrenti che possono aiutare gli individui a riconoscere ed evitare di cadere vittime di truffe sentimentali. Un modello degno di nota che descrive queste fasi è stato sviluppato da Whitty (in Cemmi, n.d.), che ha delineato come le truffe sentimentali si evolvano tipicamente in cinque fasi. Queste fasi, che includono profilazione, preparazione, sfruttamento, abuso sessuale e rivelazione, dimostrano la struttura deliberata e il potere manipolativo che sono alla base delle truffe sentimentali.

La fase iniziale (profilazione) di una truffa sentimentale prevede la creazione di una falsa identità, pensata appositamente per attrarre direttamente la vittima. Questo processo spesso inizia con la raccolta di dati personali dai profili social e dalla presenza online della vittima, inclusi hobby, interessi, obiettivi di vita e valori personali.
Utilizzando queste informazioni, i truffatori creano personaggi progettati per rispecchiare la personalità e le aspirazioni della vittima. In questo modo, creano un'apparenza di compatibilità e interessi condivisi che li rendono rapidamente cari alla vittima. I truffatori possono anche affermare di vivere nelle vicinanze, ma di non potersi incontrare temporaneamente per motivi di lavoro, spesso citando lavori che richiedono viaggi internazionali, come il servizio militare o ruoli aziendali di alto livello. Questa vicinanza falsa ma condivisibile serve a creare un senso di fiducia e comunanza, consentendo al truffatore di approfondire il legame con la vittima e di trovare una scusa conveniente per la propria assenza (Whitty, 2015, in Wang, 2022).

Una volta stabilito il contatto iniziale, il truffatore entra in una fase di approfondimento emotivo (fase di preparazione). Questa fase va oltre gli scambi superficiali; il truffatore inizia a instaurare quella che sembra una relazione intensamente affettuosa e coinvolta con la vittima. Utilizza tattiche comunemente associate al "love bombing", in cui il truffatore inonda la vittima di complimenti, espressioni di affetto, promesse di un futuro insieme e attenzioni continue. La tattica è altamente efficace, poiché fa leva sul bisogno umano di connessione e appartenenza. I truffatori possono inviare fotografie alterate, messaggi romantici e persino poesie, tutti volti a rafforzare il legame emotivo. Col tempo, raccolgono informazioni personali dalla vittima, identificando eventuali lacune nella sua vita emotiva che possono essere manipolate. Ad esempio, una vittima che si sente sottovalutata può essere lusingata dall'ammirazione del truffatore, mentre una che si sente sola può diventare rapidamente dipendente dalle sue attenzioni costanti.

Imparando gradualmente a conoscere queste vulnerabilità emotive, il truffatore si pone come la risposta ai bisogni insoddisfatti della vittima, creando una dipendenza che diventa difficile da spezzare. Questa fase può essere lunga, durare settimane o addirittura mesi, durante la quale il truffatore costruisce un legame emotivo, assicurandosi che la vittima si senta coinvolta nella relazione. L'obiettivo finale è indurre dipendenza emotiva, per cui la vittima si affeziona profondamente al truffatore e diventa sempre più disposta a soddisfare le sue richieste, credendo di essere essenziale per il benessere dell'altra persona (Commissariato di PS, n.d.).

Il truffatore passa ora dalla costruzione della fiducia all'estrazione di risorse finanziarie (fase di sfruttamento). Avendo già instaurato un forte legame emotivo, inizia a sondare il terreno chiedendo piccoli favori, spesso presentati come bisogni urgenti. Le richieste iniziali possono sembrare banali o ragionevoli, come la copertura di una piccola spesa di emergenza, e vengono presentate in modo da rispecchiare la risposta empatica della vittima nei confronti di una persona a cui tiene. Questa tecnica è nota come "piede nella porta", in cui piccole richieste portano gradualmente a richieste finanziarie più consistenti. Una volta che il truffatore ha ricevuto denaro, continua ad aumentare le sue richieste. In alcuni casi, i truffatori presentano una "crisi" elaborata, come un'improvvisa emergenza sanitaria o una truffa da parte di un partner commerciale, che richiede una quantità di denaro significativa. Un'altra tattica, nota come "porta in faccia", consiste nel chiedere inizialmente una somma elevata e irrealistica per poi ridurre la richiesta a qualcosa di più piccolo.

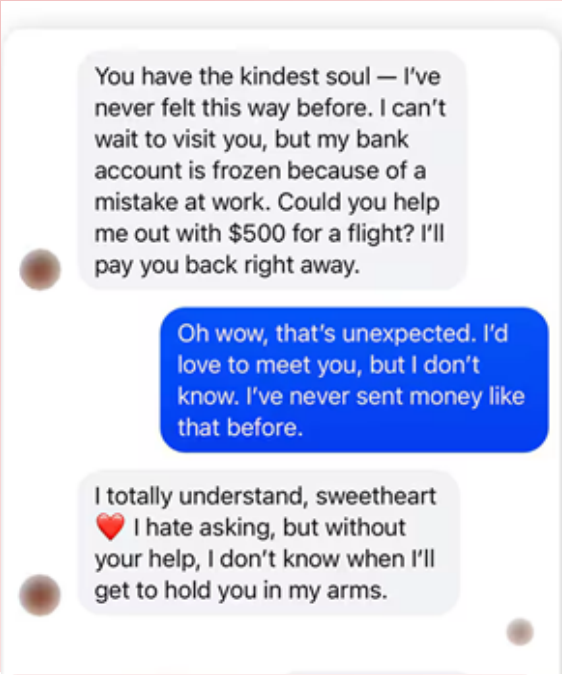
Questo approccio sfrutta la tendenza umana ad accettare una richiesta dopo averne rifiutata una più impegnativa. I truffatori possono anche utilizzare richieste continue e di importo ridotto per le spese quotidiane, cosa comune tra le vittime di sesso maschile. In questo caso, il truffatore richiede continuamente importi più piccoli sotto forma di necessità di routine, come bollette o affitto, mantenendo l'illusione di una relazione che culminerà in un incontro reale (Cemmi, n.d.; Whitty & Buchanan, 2012 in Wang, 2022).

Sebbene non sia presente in tutti i casi, alcuni truffatori spingono la manipolazione ulteriormente, introducendo un elemento sessuale. In questi casi, una volta ottenuta una notevole somma di denaro, il truffatore fa pressione sulla vittima affinché intraprenda attività sessuali tramite webcam, che spesso vengono registrate all'insaputa della vittima.

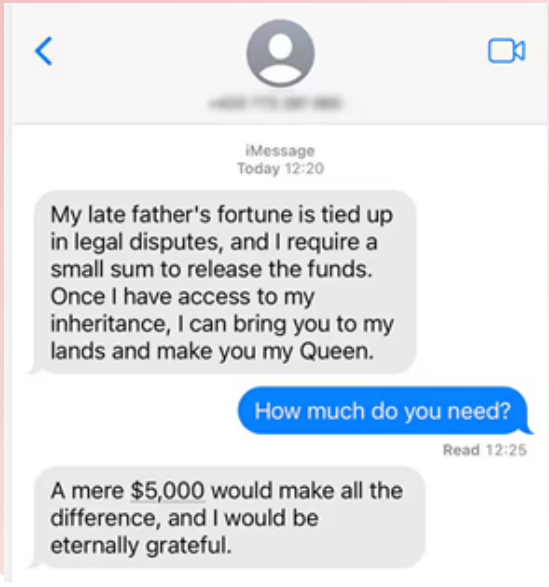
Il truffatore può quindi utilizzare queste registrazioni per ricattare la vittima, minacciandola di rilasciarla se non riceverà altro denaro. Questa tattica infligge alla vittima disagio psicologico e umiliazione, aggravando il danno emotivo causato dallo sfruttamento finanziario. Dimostra anche fino a che punto i truffatori sono disposti a spingersi per esercitare il controllo sulle loro vittime e massimizzare il guadagno finanziario (Whitty & Buchanan, 2012 in Wang, 2022). Quando il truffatore decide di aver ottenuto il massimo dalla relazione, interrompe bruscamente ogni contatto con la vittima, lasciandola spesso in uno stato di shock e confusione (fase di rivelazione e abbandono). Questa improvvisa dipartita costringe la vittima ad affrontare la dolorosa realtà dell'inganno. La perdita non è solo finanziaria, ma anche profondamente emotiva, poiché molte vittime hanno la sensazione di aver perso una relazione autentica. Le conseguenze sono spesso accompagnate da sentimenti di vergogna, umiliazione e tradimento. Le vittime vivono un processo di lutto simile a quello della perdita di una persona cara, e l'impatto psicologico può essere profondo, includendo depressione, ansia e problemi di fiducia. La consapevolezza che la relazione è stata costruita sulla manipolazione porta molte vittime a mettere in discussione il proprio giudizio e la propria autostima, aggravando il peso emotivo della truffa (Whitty & Buchanan, 2012 in Wang, 2022).

✦ Esempi di dialoghi di chat di truffa d'amore

1- Truffa militare:

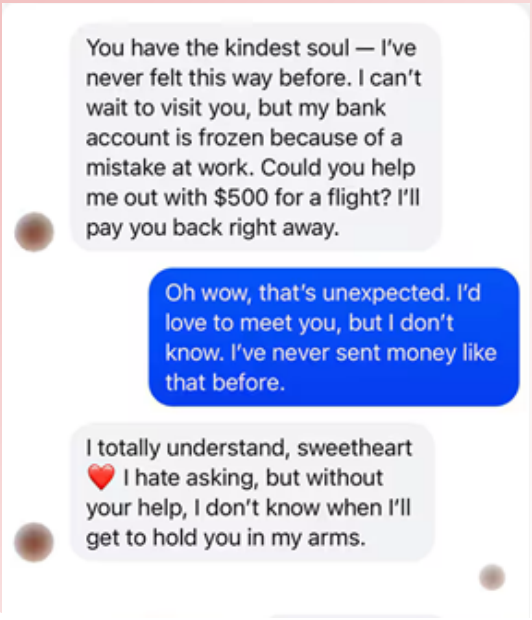


2- Truffa nigeriana:

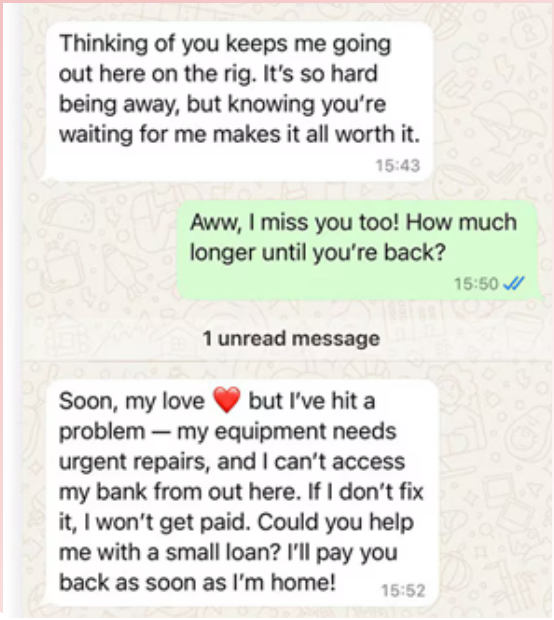


3- Truffa Crypto Romance

4- Truffa romantica su Facebook

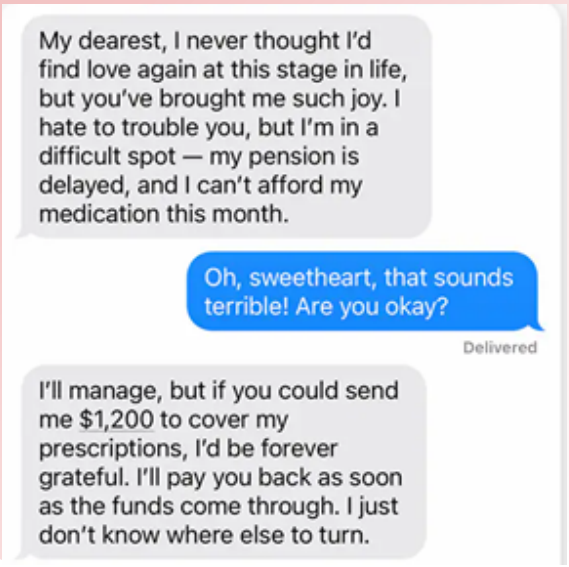


5- Truffa della piattaforma petrolifera

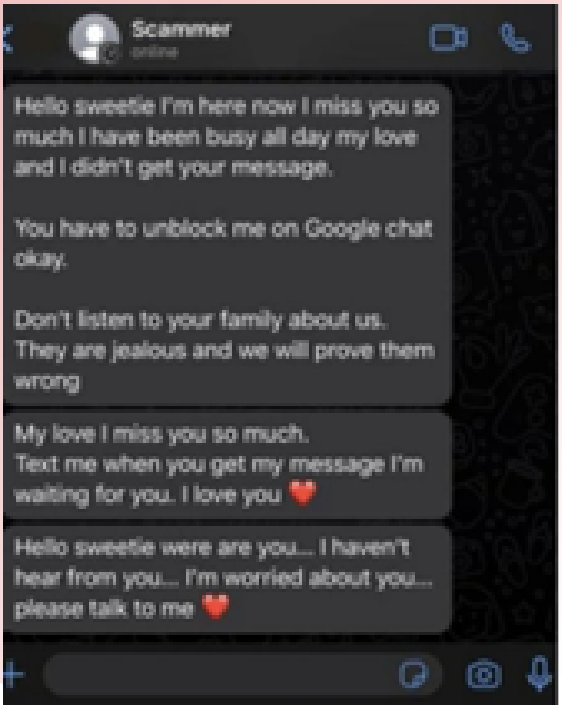


6- Storia d'amore con celebrità

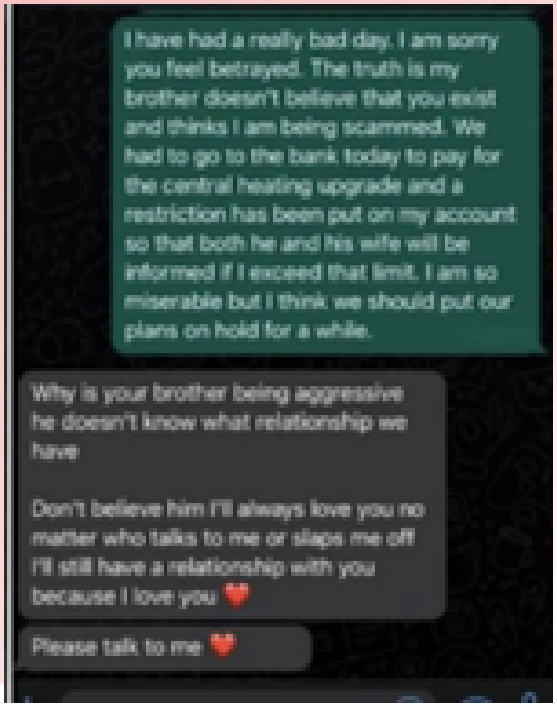
7- Truffa sentimentale tra anziani



8- Esempio di truffatore



9- Esempio di truffatore



1.2.1 Cos'è una "sextortion" e come riconoscerla?

La sextortion è una forma di estorsione sessuale, un crimine informatico in cui i criminali minacciano di distribuire immagini o video intimi a meno che la vittima non acconsenta alle loro richieste (Interpol, 2022; National Crime Agency, 2021 [NCA]; U.S. Immigration and Customs Enforcement [ICE], 2025). In questi schemi, i criminali spesso sfruttano relazioni sentimentali o intimità online per ottenere materiale compromettente, sfruttandolo poi per ottenere denaro, favori sessuali o sfruttamento continuato (Wang, 2024).
Per quanto riguarda le truffe sentimentali, l'estorsione emerge in genere dopo che è stata instaurata una relazione di fiducia online: i truffatori creano false identità su siti di incontri o social media, costruiscono un legame emotivo e poi incoraggiano la condivisione di immagini di nudo o interazioni sessuali tramite webcam, a volte registrandole di nascosto (Kloess et al., 2014). Una volta ottenuti, questi materiali diventano strumenti di coercizione, con i truffatori che minacciano di inviarli a familiari, amici o datori di lavoro, a meno che le loro richieste non vengano soddisfatte (Europol, 2017). In alcuni casi, i criminali usano la minaccia di essere scoperti come "ricatto implicito" per mantenere il controllo sulle vittime (Whitty & Buchanan, 2012).

✦ I segnali d'allarme includono:

• rapida escalation in conversazioni o richieste di natura sessuale (Europol, 2017);
• rifiuto di partecipare a normali videochiamate, insistendo nel ricevere materiale esplicito (Patchin & Hinduja, 2020);
• profili con foto rubate o incoerenti (Interpol, 2022);
• manipolazione emotiva o minacce di autolesionismo (Wang, 2024);
• e sollecitare le vittime a passare rapidamente dalle piattaforme pubbliche ai canali privati (NCA, 2021).

Psicologicamente, gli autori di reati utilizzano strategie di adescamento, spesso ricorrendo al "love bombing" o a un'eccessiva adulazione per abbassare le difese (Coluccia et al., 2020). Possono anche ricercare le vittime attraverso i social media per intensificare le minacce, facendo apparire imminente l'esposizione (Patchin & Hinduja, 2020). È importante sottolineare che la sextortion prospera sulla vergogna e sul silenzio delle vittime; la ricerca

mostra che molti esitano a denunciare per paura dello stigma (Cross, 2014; Pietilä & Korhonen, 2024). Riconoscere precocemente i segnali può dare la forza di interrompere i contatti e cercare aiuto da professionisti o dalle forze dell'ordine.

1.2.2 Casi di studio sulle vittime di truffe amorose

Le truffe sentimentali si sono evolute da semplici inganni online a complesse reti criminali di portata globale, come dimostrano diversi casi eclatanti. Questi esempi evidenziano come le truffe sentimentali possano essere sia emotivamente devastanti che finanziariamente distruttive, prendendo di mira individui vulnerabili attraverso tattiche di manipolazione emotiva.

Caso di studio 1

In Italia, una rete altamente organizzata di truffe sentimentali prendeva di mira uomini anziani, principalmente in Calabria. Questa rete era composta da cittadini rumeni che impiegavano giovani donne per stabilire relazioni personali, spesso fisiche, con le loro vittime. Costruendo un profondo legame emotivo, queste donne convincevano gli uomini anziani a trasferire ingenti somme di denaro, apparentemente per coprire emergenze familiari o sanitarie. Questo caso mostra come alcune truffe sentimentali si estendano oltre il mondo online, incorporando interazioni faccia a faccia che ne accentuano l'impatto sulle vittime. Operando in diversi paesi, la rete ha messo in atto sofisticate pratiche di riciclaggio di denaro, distribuendo il denaro ottenuto dalle vittime attraverso vari canali finanziari per evitare di essere scoperta. Questa operazione ha generato oltre un milione di euro, a dimostrazione degli ingenti profitti che le truffe sentimentali organizzate possono generare. La portata multinazionale e la natura strutturata di questa truffa rivelano le sfide che le autorità devono affrontare nell'indagare e perseguire tali casi, soprattutto perché queste reti spesso operano a livello transfrontaliero (EUROPOL, 2022).

Caso di studio 2

Un uomo di 53 anni, vulnerabile dopo un recente divorzio, è diventato vittima di una truffa sentimentale quando si è rivolto a un sito di incontri per stringere nuove amicizie. È stato contattato da una donna che affermava di essere spagnola ma residente negli Stati Uniti. La donna gli ha inviato delle foto, ma ha evitato qualsiasi contatto fisico o video, mantenendo la comunicazione tramite telefono, Skype ed e-mail. Dopo aver instaurato un legame, la donna ha iniziato a chiedere assistenza finanziaria, inizialmente sostenendo di non potersi permettere il cibo e in seguito sostenendo di aver bisogno di un passaporto per fargli visita. Nel corso del tempo, la vittima ha inviato oltre 15.000 sterline alla sua presunta compagna.

In seguito all'intervento della polizia e al supporto dei servizi per le vittime, l'uomo ha smesso di inviare denaro e ha iniziato a ricevere assistenza emotiva e pratica. Questo caso illustra come i truffatori sfruttino situazioni di vita vulnerabili, come il divorzio, e avanzino gradualmente le loro richieste, costruendo la fiducia attraverso contatti costanti ma superficiali (Polizia del Surrey, n.d.).

Caso di studio 3

Una vedova di 65 anni è diventata vittima di una truffa sentimentale dopo aver conosciuto su Facebook un uomo che sosteneva di essere un ufficiale dell'esercito. Sola dopo la scomparsa del marito, ha cercato compagnia e si è presto convinta delle sincere intenzioni dell'uomo. Il truffatore, che interagiva con lei solo tramite Facebook e telefono, sosteneva di aver bisogno di soldi per lasciare l'esercito e prendersi cura del figlio malato. La vittima, desiderosa di aiutarla, ha inviato 7.500 sterline. Poco dopo, il truffatore ha richiesto ulteriori 3.500 sterline per coprire le spese mediche del figlio. Tuttavia, la banca è intervenuta prima della transazione, attivando un'allerta ai sensi del proprio protocollo bancario e prevenendo ulteriori perdite. Questo intervento, insieme ai successivi consigli della polizia, ha aiutato la vittima a comprendere che si trattava di una truffa. Questo caso evidenzia l'importanza dei protocolli bancari e dei sistemi di supporto familiare nel proteggere le persone vulnerabili dalle truffe (Polizia del Surrey, n.d.).

Caso di studio 4

Un uomo di 66 anni, divorziato e residente da solo, è diventato bersaglio di molteplici truffe sentimentali dopo essersi iscritto a diverse piattaforme di incontri online. Mantenendo i contatti con diverse donne tramite e-mail, SMS e telefono, gli è stato fatto credere di sostenere le loro spese di sostentamento, inclusi affitto e bollette, e persino di coprire i voli per visite mai avvenute. Nell'arco di cinque anni, ha inviato oltre 100.000 sterline a diversi truffatori. Sua figlia ha infine sollevato la questione con la polizia, che è intervenuta. Gli istituti finanziari hanno successivamente impedito all'uomo di utilizzare i servizi di trasferimento di denaro per prevenire ulteriori perdite. Questo caso esemplifica come le truffe prolungate possano erodere la sicurezza finanziaria e sottolinea l'importanza del coinvolgimento della famiglia e del monitoraggio finanziario nell'identificare e fermare tali truffe (Polizia del Surrey, n.d.).

Caso di studio 5

Un'indagine sulle truffe sentimentali provenienti dalla Nigeria ha rivelato un dettagliato "manuale" che i truffatori usano per ingannare le loro vittime. Questo manuale fornisce istruzioni dettagliate

Linee guida passo passo per stabilire un rapporto di fiducia, manipolare le emozioni e aumentare gradualmente le richieste finanziarie. I truffatori in Nigeria spesso prendono di mira donne di mezza età o anziane, single o recentemente vedove, sfruttando la loro potenziale solitudine e il desiderio di stabilire un legame. Nelle fasi iniziali, i truffatori creano profili che appaiono sofisticati e affascinanti, utilizzando foto lusinghiere e impegnandosi in conversazioni apparentemente significative. Il manuale delinea le tattiche per costruire una "storia d'amore travolgente", una strategia volta a replicare le relazioni idealizzate spesso viste nei media. Col tempo, i truffatori manipolano la vittima inducendola a credere in un futuro insieme, avanzando al contempo richieste finanziarie sempre più consistenti. Questo manuale evidenzia l'approccio sistematico adottato da questi truffatori e i passaggi calcolati coinvolti nelle truffe sentimentali, sottolineando la natura professionalizzata delle frodi sentimentali come impresa criminale (DocumentCloud, n.d.).
Data la persistenza delle truffe sentimentali, sono disponibili alcuni strumenti tecnologici per aiutare a identificare i profili fraudolenti. Swindlerbuster Face Search, ad esempio, consente agli utenti di eseguire ricerche inverse sulle foto utilizzate nei profili di incontri. Identificando se un'immagine è collegata a più nomi o luoghi, gli utenti possono verificare meglio l'autenticità dei profili online.

1.3 Statistiche

La Polizia Postale e delle Comunicazioni monitora attivamente il web quotidianamente, con personale specializzato che presidia gli spazi online, in particolare le piattaforme dei social media, per prevenire e contrastare i comportamenti criminali. Questa divisione specializzata opera in modo coordinato a livello nazionale e internazionale, avvalendosi di uffici in tutto il Paese per gestire e indagare sui casi legati alla criminalità informatica. Tra le problematiche affrontate c'è la "romance scam", o truffa sentimentale, che ha registrato un aumento sbalorditivo del 118% nel 2021 rispetto ai casi gestiti nel 2020. Sebbene gli uomini siano generalmente meno colpiti da questa truffa, numerosi uomini italiani sono stati ingannati da autori che si spacciavano per donne straniere utilizzando account sui social media con immagini provocanti, spesso presentandosi come modelle o ricche ereditiere. Queste truffe possono comportare perdite finanziarie significative, con singoli casi che a volte ammontano a centinaia di migliaia di euro. Solo nel 2021,

Circa 4,5 milioni di euro sono stati segnalati come perdite a causa di queste truffe (Commissariato di Pubblica Sicurezza Online, n.d.). In Europa, le truffe sentimentali colpiscono tra l'1% e il 3% della popolazione, con perdite che dimostrano notevoli implicazioni finanziarie in diversi paesi. Ad esempio, i registri della polizia finlandese del 2020 riportano 210 incidenti, per un totale di 6,1 milioni di euro di perdite, che sono aumentate a 10,4 milioni di euro entro il 2023, riflettendo la crescente prevalenza di questi reati (Pietilä & Korhonen, 2024). L'impatto finanziario delle truffe sentimentali si estende a tutto il continente e il modello di inganno riscontrato in questi incidenti sottolinea l'importanza della consapevolezza pubblica e dell'alfabetizzazione digitale nella lotta alle frodi online.

La piattaforma CybSafe riporta che circa il 20% delle persone subisce truffe sentimentali, con i Millennial (18%) e la Generazione Z (15%) più colpiti. Nonostante gli alti tassi di vittimizzazione, solo il 55% delle vittime denuncia queste truffe e, di queste, il 36% si rivolge alle autorità. Queste statistiche evidenziano sia le differenze generazionali nella vulnerabilità che nei comportamenti di segnalazione, suggerendo la necessità di strategie preventive mirate e di un maggiore supporto tra i gruppi demografici (CybSafe, 2023).

1.4 Vittimologia della truffa amorosa

1.4.1 Conseguenze psicologiche delle vittime di truffe amorose

La vittimizzazione attraverso reati informatici, come truffe sentimentali, cyberstalking o frodi, provoca profondi impatti psicologici che sono paragonabili a quelli di reati analoghi commessi offline. Le vittime subiscono una serie di effetti emotivi, sociali e fisiologici. La ricerca mostra che, ad esempio, le vittime di cyberbullismo subiscono conseguenze simili a quelle del bullismo tradizionale, tra cui ansia sociale, depressione e un ridotto senso di sicurezza (Smith et al., 2008, in Open University, 2024).

Allo stesso modo, il disagio causato dal cyberstalking riflette quello dello stalking di persona, portando le vittime a sopportare alti livelli di paura, ipervigilanza e stress (Dreßing et al., 2014, in Open University, 2024). Sebbene gli effetti del trolling siano meno studiati, prove emergenti suggeriscono che anche questo può contribuire a danni psicologici significativi, indicando la necessità di

Un'ulteriore esplorazione del suo impatto sulle vittime. Le truffe sentimentali, in particolare, hanno conseguenze psicologiche uniche e profonde a causa della natura multidimensionale del danno che provocano. La ricerca mostra che le vittime di truffe sentimentali sperimentano quello che Button et al. (2014) chiamano un "doppio colpo", ovvero la perdita finanziaria e la devastazione emotiva che derivano dal crollo percepito di una relazione autentica. Gli studi evidenziano che questo tradimento emotivo può spesso eclissare il danno finanziario, creando profondo disagio nelle vittime. Button et al. (2014) osservano che la combinazione di perdita finanziaria e tradimento emotivo causati da queste truffe porta molte vittime a subire gravi traumi emotivi. Il lavoro di Whitty e Buchanan (2012; 2016) rafforza questo concetto, rivelando che le vittime spesso lottano con vergogna, senso di colpa e autoaccusa, che spesso le dissuadono dal cercare aiuto. Tale vergogna interiorizzata può essere amplificata dal giudizio esterno, poiché le vittime vengono talvolta etichettate come “ingenue” o “credulone” dagli altri (Buchanan & Whitty, 2014, in Open University, 2024).

Gli impatti psicologici della vittimizzazione da reati informatici sono estesi e spesso duraturi. Molte vittime riferiscono di soffrire di depressione, isolamento sociale, sintomi simili al PTSD, comportamenti ossessivi, bassa autostima e una profonda sfiducia negli altri (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012; Bates, 2017, in Open University, 2024). Le vittime riferiscono anche frequentemente sintomi fisici, come mal di testa persistenti, problemi digestivi e disturbi del sonno, che aggravano ulteriormente la tensione emotiva e complicano il recupero. Le strategie di coping inizialmente tendono a meccanismi disadattivi, tra cui l'uso di sostanze e comportamenti di evitamento, prima che le vittime possano passare a metodi più positivi come la consulenza psicologica o la partecipazione a iniziative di advocacy. Tuttavia, il recupero è spesso ostacolato da atteggiamenti sociali, in particolare dal pervasivo problema della colpevolizzazione della vittima. La colpevolizzazione della vittima rappresenta un ostacolo critico nel processo di recupero, soprattutto per le vittime di reati informatici. La ricerca sulla vittimologia, risalente alle prime tipologie di Mendelsohn degli anni '30, suggeriva che le vittime potessero svolgere un ruolo nella loro vittimizzazione. Tuttavia, la moderna teoria della vittimologia generalmente ritiene responsabili i colpevoli, riconoscendo che fattori al di fuori del controllo della vittima spesso contribuiscono al loro sfruttamento. Ciononostante, le vittime di reati informatici vengono spesso accusate di responsabilità parziale, spesso a causa di convinzioni profondamente radicate di un "mondo giusto" (Lerner, 1980, in Open University, 2024). Questo sistema di credenze suggerisce che il mondo operi secondo un principio di equità, che porta le persone a

credono che le vittime debbano aver fatto qualcosa per attirare l'attenzione. Questa mentalità, spesso applicata alle truffe sentimentali, implica che le vittime abbiano agito per avidità o credulità e avrebbero potuto evitare il crimine astenendosi dalle interazioni online o dall'uso dei social media (Cross, 2015, in Open University, 2024).

Questo tipo di colpevolizzazione della vittima può esacerbare il peso psicologico delle vittime di truffe sentimentali, che già lottano con sentimenti di tradimento e vergogna. Molte vittime riferiscono che l'aspetto più doloroso della loro esperienza è il giudizio e la mancanza di empatia che incontrano da parte di familiari e amici, che potrebbero vederle come complici della loro vittimizzazione. Quando si verifica la colpevolizzazione della vittima, può anche rafforzare l'auto-colpevolizzazione nella vittima, rendendole difficile cercare supporto o parlare apertamente delle proprie esperienze. Questa mancanza di supporto non solo ostacola la guarigione emotiva, ma può far sentire le vittime ulteriormente isolate e incomprese, con conseguenti impatti psicologici più profondi nel tempo (Wang, 2022). Le truffe sentimentali spesso portano a un profondo disagio emotivo che va oltre la perdita finanziaria, lasciando le vittime con sentimenti di vergogna, colpa e isolamento sociale. Molte vittime possono auto-colpevolizzare o sentirsi troppo in imbarazzo per denunciare la truffa, mentre alcune affrontano gravi conseguenze finanziarie, perdendo i risparmi di una vita o indebitandosi. Le vittime che sviluppano legami emotivi con il truffatore possono sperimentare la sindrome di Stoccolma, provando simpatia o affetto per l'autore anche dopo che l'inganno è stato scoperto. Questo attaccamento complica la loro capacità di sfuggire alla truffa o di denunciarla (The Debt Advisor, 2023).

1.4.2 Profilo della vittima

La ricerca sulla vittimologia delle truffe sentimentali online rivela specifici tratti demografici e psicologici che aumentano la vulnerabilità a tali schemi. Studi di Wang (2022) indicano che gli individui a maggior rischio di cadere vittima di truffe sentimentali tendono ad essere donne, di mezza età e con un buon livello di istruzione. I dati demografici suggeriscono che il 60% delle vittime di truffe sentimentali sono donne, mentre il 40% sono uomini. Tra le vittime, il 63% è di mezza età, seguito dal 21% di giovani adulti e dal 16% di anziani. Le persone di mezza età sono spesso prese di mira a causa della loro stabilità finanziaria e della maggiore probabilità di utilizzare piattaforme di incontri online, in particolare dopo cambiamenti nella vita come il divorzio o la perdita del coniuge, che possono aumentare la loro suscettibilità alle promesse di compagnia presentate dai truffatori.

Anche i tratti della personalità giocano un ruolo: gli individui con livelli più elevati di fiducia, impulsività e basso autocontrollo sono particolarmente vulnerabili. I truffatori sfruttano queste caratteristiche, trascinando le vittime in relazioni sentimentali fittizie attraverso narrazioni ben costruite che suscitano empatia, compassione e spesso un profondo attaccamento emotivo (Wang, 2022). L'impatto psicologico delle truffe sentimentali è profondo, spesso caratterizzato da quello che Button et al. (2014) definiscono un "doppio colpo": perdita finanziaria unita alla devastazione emotiva di un percepito tradimento relazionale.

Le vittime soffrono tipicamente di un grave disagio emotivo, tra cui vergogna, senso di colpa e calo dell'autostima. Studi di Whitty e Buchanan (2012, 2016) evidenziano come questi effetti emotivi possano spesso superare il disagio associato alle perdite finanziarie, poiché le vittime elaborano il tradimento di una relazione che credevano autentica. Molte vittime esitano a cercare supporto o a denunciare il reato, temendo critiche o accuse da parte di familiari e amici che potrebbero considerarle "ingenue" o "credulone" (Buchanan e Whitty, 2014 in Open University, 2024). Cross et al. (2016) hanno esaminato le dinamiche delle truffe sentimentali attraverso la lente della teoria della violenza domestica, esplorando come i truffatori utilizzino la manipolazione psicologica per stabilire il controllo sulle loro vittime. Secondo i loro risultati, le vittime di truffe sentimentali mostrano spesso alti livelli di fiducia e vulnerabilità nelle interazioni online, il che le rende più suscettibili alla manipolazione emotiva. I truffatori sfruttano questa fiducia presentando una facciata di affetto, inducendo la vittima a credere nella legittimità della relazione. Questo approccio rispecchia le tattiche di manipolazione emotiva tipiche della violenza domestica, in cui i criminali creano dipendenza e isolano le vittime dalle loro reti di supporto. L'isolamento è una caratteristica comune nelle truffe sentimentali, poiché i truffatori scoraggiano le vittime dal condividere i dettagli della loro relazione con amici o familiari. Questa tattica accresce il coinvolgimento emotivo della vittima e la sua dipendenza dal truffatore, rendendole sempre più difficile riconoscere o sfuggire all'inganno (Cross et al., 2016).
Il costo finanziario per le vittime di truffe sentimentali è spesso elevato. Molte vittime si separano da ingenti risparmi o vendono beni personali per soddisfare le richieste finanziarie dei truffatori. Questo impatto finanziario, aggravato dalla tensione emotiva, può portare a un senso di disperazione e impotenza. Per alcuni, le perdite possono compromettere la loro stabilità finanziaria per anni, aggravando i problemi di salute mentale che devono affrontare. Cross et al. (2016) osservano che lo sfruttamento finanziario possa scatenare profondi

sentimenti di vergogna e colpa, mentre le vittime si confrontano con la consapevolezza della manipolazione subita. Oltre al danno finanziario ed emotivo, le vittime di truffe sentimentali lamentano vari sintomi fisici e psicologici associati al trauma. Gli studi indicano che le vittime manifestano frequentemente sintomi di disturbo da stress post-traumatico (PTSD), depressione, isolamento sociale, comportamenti ossessivi e un opprimente senso di sfiducia verso gli altri. Sono comuni anche sintomi fisici, come mal di testa, problemi digestivi e disturbi del sonno, che spesso esacerbano il danno emotivo della truffa. Inizialmente, le vittime possono ricorrere a strategie di coping disadattive, come l'uso di sostanze o comportamenti di evitamento, prima di cercare un supporto più costruttivo attraverso la consulenza o l'advocacy. Tuttavia, il recupero è spesso ostacolato da atteggiamenti sociali di colpevolizzazione della vittima, comuni nei casi di cyber-vittimizzazione.

La colpevolizzazione della vittima, un ostacolo significativo al recupero, è radicata negli atteggiamenti e nelle percezioni sociali riguardanti la criminalità informatica. Le prime teorie sulla vittimologia, come le tipologie di Mendelsohn degli anni '30, postulavano che le vittime potessero avere un ruolo nella loro vittimizzazione. Sebbene i quadri teorici moderni generalmente ritengano responsabili gli autori, le vittime di reati informatici si scontrano ancora con il giudizio della società, soprattutto nei casi che coinvolgono truffe sentimentali. Questo giudizio è spesso legato alle convinzioni del "mondo giusto", che suggeriscono che il mondo operi secondo principi di equità; pertanto, le vittime devono aver fatto qualcosa per attirare il danno (Lerner, 1980 in Open University, 2024). Applicata alle truffe sentimentali, questa mentalità implica che le vittime avrebbero potuto evitare la truffa rimanendo offline o esercitando maggiore cautela, creando uno stigma intorno alle loro esperienze (Cross, 2015 in Open University, 2024).

1.4.3 Riabilitazione psicologica della vittima di una truffa amorosa

Le truffe sentimentali lasciano profondi danni psicologici ed emotivi. Le vittime spesso subiscono un "doppio trauma": perdita finanziaria e crollo di quella che credevano essere una relazione autentica (Cross, 2014; Cross et al., 2018). Gli studi dimostrano che quasi due terzi delle vittime di frode segnalano danni alla salute o psicologici che persistono a lungo dopo la truffa (Button et al., 2014).

Le conseguenze psicologiche includono stress acuto e risposte traumatiche, con alcuni sintomi di PTSD in via di sviluppo come ricordi intrusivi, flashback, incubi e ipervigilanza (Coluccia et al., 2020). Depressione, vergogna e autoaccusa sono comuni.

Le vittime spesso si chiedono come abbiano potuto "essere così ingenue" (Whitty, 2018). Molte sviluppano anche problemi di fiducia duraturi, mettendo in dubbio il proprio giudizio e faticando a costruire nuove relazioni (Rege, 2019 in Pietilä & Korhonen, 2024). Le vittime spesso si isolano socialmente, abbracciando sentimenti di isolamento e umiliazione (Whitty & Buchanan, 2012). Il lungo percorso verso la guarigione richiede un supporto multilivello:

• La consulenza basata sul trauma, in particolare gli approcci cognitivo-comportamentali e incentrati sul dolore, ha dimostrato efficacia nell'aiutare le vittime a riformulare le proprie esperienze e a ridurre l'auto-colpevolizzazione (Against Scams, 2024).
• I gruppi di supporto tra pari offrono spazi sicuri in cui i sopravvissuti possono condividere esperienze, convalidare le emozioni e ricostruire la resilienza (AARP, 2021). Le comunità online contrastano anche l'isolamento, fornendo connessione e normalizzazione (AARP, n.d.).
• Comprendere le tattiche relazionali e manipolative utilizzate dai truffatori aiuta i sopravvissuti a spostare la colpa da se stessi e a riacquistare fiducia in se stessi (Coluccia et al., 2020).
• I servizi sociali, finanziari e comunitari, che vanno dalla consulenza legale alla formazione sulla sicurezza digitale, favoriscono la ripresa ripristinando il controllo e l'agenzia (Pietilä & Korhonen, 2024).

Sebbene il recupero sia graduale, le vittime spesso segnalano una crescita post-traumatica una volta affrontata la vergogna e messe in atto reti di supporto (Cross et al., 2018; Whitty, 2018).

Sostenere con cura: buone pratiche per gli educatori

Co-funded by
the European Union

Salma Alaaelden

Salma è assistente di progetto e ricercatrice presso EUth Wonders e. V., con una solida formazione in economia e oltre sei anni di esperienza nel lavoro con i giovani e nella gestione di progetti. Ha collaborato con organizzazioni in tutto il mondo, contribuendo a iniziative che mettono in contatto i giovani e promuovono il dialogo interculturale. Salma ha contribuito a numerose ricerche sulla salute mentale e, in qualità di formatrice, ha tenuto workshop sul benessere mentale attraverso i suoi progetti. Presso EUth Wonders e. V., svolge un ruolo chiave nella progettazione, nel coordinamento e nella realizzazione di progetti Erasmus+ e di altri progetti internazionali, lavorando durante l'intero ciclo di vita del progetto, garantendo che le attività siano significative, inclusive e in linea con la nostra missione: connettere i giovani oltre i confini nazionali e migliorare le loro competenze e opportunità.

2 BUONE PRATICHE PER GLI EDUCATORI

2.1 Scopo di questo capitolo

Poiché le truffe sentimentali e amorose che prendono di mira gli anziani rappresentano una forma di criminalità informatica in rapida crescita in Europa e comportano enormi perdite sociali e finanziarie, nonché impatti psicologici quali isolamento sociale, sfruttamento delle vulnerabilità emotive e perdite finanziarie, il ruolo degli educatori e degli operatori giovanili diventa cruciale nel proteggere gli anziani dalle truffe legate all'amore, fornendo supporto sociale, gestendo la vulnerabilità psicologica e offrendo percorsi chiari a questi anziani.

In base all'importanza del ruolo degli operatori giovanili e degli educatori, questo capitolo completo fornirà le informazioni necessarie per comprendere le vulnerabilità psicologiche che rendono le vittime inclini alle truffe, le conseguenze emotive e psicologiche delle truffe amorose e, di conseguenza, questo capitolo fornirà anche agli educatori le conoscenze e gli strumenti su come fornire supporto sociale e psicologico agli anziani vulnerabili alle truffe amorose attraverso misure preventive e reattive e per offrire loro risorse utili in caso di verificarsi di una truffa amorosa e per creare reti di supporto per promuovere un ambiente sicuro e di fiducia per gli anziani.

2.1.1 Obiettivi e approcci chiave di questo capitolo:

Questo capitolo si concentra su diversi obiettivi chiave volti a consentire agli anziani e alle loro reti di supporto di riconoscere, rispondere e prevenire le truffe. Gli obiettivi sono:

1. Identificare le vulnerabilità psicologiche, sociali e situazionali: comprendere i fattori che rendono gli anziani particolarmente vulnerabili alle truffe, inclusi gli elementi psicologici, sociali e situazionali, aiuterà a riconoscere i fattori di rischio e ad adottare misure preventive.
   1.2. Studiare l'impatto psicologico ed emotivo delle truffe amorose sulle vittime: analizzare l'impatto psicologico e i problemi di salute mentale sulle vittime di truffe amorose ci aiuterà a comprendere e riconoscere come supportare le vittime dopo la truffa in modo più efficace in qualità di educatori.
3. Casi di studio reali su situazioni di truffe amorose: per fornire una visione più completa sui metodi di prevenzione e risposta alle truffe amorose, alcuni

verranno spiegati e analizzati casi di studio.

4. **Comprendere l'importante ruolo degli operatori giovanili e degli educatori**: questa parte spiegherà i diversi fattori che evidenziano la necessità degli educatori di supportare gli anziani inclini alle truffe amorose.
5. **Fornire indicazioni agli educatori sulle misure preventive per proteggere gli anziani dal rischio di cadere vittime di truffe amorose**: identificare le diverse misure preventive che gli educatori possono mettere in atto per garantire che gli anziani siano consapevoli e per salvarli dal rischio di cadere potenzialmente in truffe amorose.
5. **Fornire indicazioni agli educatori su come individuare una truffa in corso**: questa parte spiegherà come individuare una truffa in corso attraverso indicatori comportamentali e segnali delle vittime e come supportare le vittime anziane in tali casi.
6. **Fornire una guida dettagliata per rispondere ai casi di truffa**: offrire una procedura chiara e pratica che gli anziani e gli assistenti possano seguire quando si imbattono in una truffa, assicurandosi che sappiano come segnalare e gestire la situazione in modo efficace.
7. **Creazione di reti di supporto a lungo termine: c**reazione e rafforzamento di sistemi di supporto continuo che possano aiutare gli anziani a evitare di diventare vittime di truffe future, promuovendo l'istruzione, la vigilanza e i legami con la comunità.
8. **Mettere in contatto educatori e anziani con risorse essenziali**: fornire a educatori, anziani e a chi si prende cura di loro le risorse e gli strumenti necessari per il recupero e la protezione, garantendo loro l'accesso alle informazioni e al supporto per proteggersi dalle truffe.
9. **Casi di studio pratic**i: questa parte consisterà in un esercizio pratico con diversi casi di studio ipotetici che gli educatori analizzeranno e spiegheranno come dovrebbero comportarsi in ogni situazione per supportare le vittime anziane.

Questi obiettivi aiuteranno gli anziani a rimanere informati, protetti e resilienti contro le truffe, garantendo la sicurezza sia immediata che a lungo termine.

2.1.2 Approcci

L'obiettivo educativo di questo capitolo enfatizza un duplice approccio per proteggere gli anziani dalle truffe sentimentali. In primo luogo, le misure preventive si concentreranno sull'educazione degli anziani e dei loro caregiver sulle tattiche truffaldine più comuni, fornendo loro le competenze digitali e il supporto sociale necessari per riconoscere ed evitare le truffe.

In secondo luogo, Responsive Actions fornisce protocolli chiari per l'intervento e il supporto quando si verifica una truffa, guidando gli educatori in ogni fase, dalla documentazione iniziale e dalla segnalazione alle risorse per il recupero emotivo e finanziario.

2.2 Riconoscere la vulnerabilità psicologica e sociale

C'è poco aiuto e supporto per le vittime anziane prima, durante e dopo il processo di truffa, il che non solo rende difficile per loro ottenere assistenza tempestiva e professionale dopo aver subito truffe online, ma corre anche il rischio di essere nuovamente truffate per amore in seguito, moltiplicando i danni sociali, psicologici e finanziari.

Prima di affrontare le diverse misure per prevenire o fornire supporto agli anziani truffati come educatori, e la loro necessità, è importante comprendere innanzitutto i fattori di rischio che rendono gli anziani più vulnerabili alle truffe. Questo è fondamentale per educatori, assistenti e leader della comunità, perché riconoscere questi fattori consente un intervento tempestivo ed efficace e offre l'opportunità di attuare misure preventive prima che gli anziani cadano vittime di frode.

Diversi fattori psicologici, sociali e situazionali contribuiscono alla vulnerabilità degli anziani, spesso sfruttata dai truffatori. Tra questi fattori rientrano, tra gli altri, l'isolamento sociale, il declino cognitivo e il bisogno emotivo.

✦ **Isolamento sociale:**

Uno dei principali fattori che aumentano la vulnerabilità degli anziani alle truffe è l'isolamento sociale. Molti anziani soffrono di una mancanza di interazioni sociali regolari, che può portare a sentimenti di solitudine e noia. In alcuni casi, questo isolamento spinge gli anziani a cercare compagnia o un legame emotivo attraverso piattaforme online. I truffatori, consapevoli di questa esigenza, spesso usano la scusa delle relazioni online per approfittarsi di questi individui, costruendo fiducia e legami emotivi per manipolarli. Col tempo, la vittima può essere convinta a inviare denaro o fornire informazioni personali. Combattere l'isolamento incoraggiando interazioni sociali regolari e costruendo reti comunitarie di supporto è fondamentale per prevenire tale sfruttamento.

Declino cognitivo e suscettibilità alle truffe:

Con l'avanzare dell'età, le persone possono sperimentare un declino cognitivo, che include vuoti di memoria, difficoltà nell'elaborare nuove informazioni e una ridotta capacità di formulare giudizi sensati. Questi deficit cognitivi possono rendere difficile per gli anziani riconoscere i segnali d'allarme associati alle truffe, come telefonate indesiderate, e-mail di phishing o programmi di investimento fraudolenti. Il declino cognitivo può anche ridurre la capacità di un anziano di comprendere le conseguenze della condivisione di informazioni personali o finanziarie con estranei. Pertanto, è essenziale che educatori e assistenti siano consapevoli della salute cognitiva degli anziani e offrano strategie per identificare i segnali di allarme ed evitare situazioni rischiose. Esercizi mentali regolari, controlli di routine e l'uso di tecnologie affidabili possono contribuire a preservare le funzioni cognitive e a prevenire le truffe.

Bisogno emotivo:

La vulnerabilità emotiva è un altro fattore significativo sfruttato dai truffatori. Gli anziani possono affrontare diverse sfide emotive, come il dolore, la perdita del coniuge o la solitudine. Queste emozioni possono indurli a cercare attivamente nuove relazioni o conferme, il che rappresenta un'opportunità ideale per i truffatori che sfruttano il bisogno emotivo. I truffatori possono fingersi interessati a qualcosa di romantico, promettendo affetto, compagnia o un senso di appartenenza. Sfortunatamente, queste truffe possono comportare perdite finanziarie, poiché gli anziani possono essere manipolati per inviare denaro o offrire altre forme di supporto. Comprendere lo stato emotivo degli anziani e offrire supporto sia emotivo che sociale è fondamentale per mitigare questo tipo di truffe. Fornire accesso a servizi di consulenza per il lutto, gruppi di supporto e altre risorse sociali può contribuire a ridurre la vulnerabilità emotiva sfruttata dai truffatori.

Fidarsi della natura (credulità):

Sulla base di molteplici studi, le persone che hanno un alto grado di fiducia hanno maggiori probabilità di essere vittime di truffe amorose. Molti anziani, soprattutto quelli che hanno vissuto periodi di fiducia e stabilità, possono avere una natura più fiduciosa, che può essere sfruttata dai truffatori. I truffatori spesso giocano sul desiderio di gentilezza e disponibilità degli anziani, sia attraverso una presunta causa benefica che una presunta necessità finanziaria urgente. Gli anziani potrebbero non mettere in dubbio le intenzioni della persona con cui stanno comunicando, rendendoli obiettivi privilegiati per le frodi finanziarie. Incoraggiare un sano senso di scetticismo e consigliare agli anziani di verificare sempre le richieste di denaro o di informazioni personali, anche se provengono da

fonti apparentemente familiari, è un'importante misura preventiva.

In sintesi, questi sono alcuni dei fattori che rendono gli anziani più inclini alle truffe. Vale la pena notare che, di solito, affinché una truffa si verifichi, non esiste una sola vulnerabilità, ma piuttosto un'interazione di vulnerabilità psicologiche, cognitive e sociali che creano condizioni di sfruttamento gravi come i cosiddetti fattori di rischio chiave, che aumentano la probabilità di essere presi di mira e adescati.

2.3 L'impatto psicologico delle truffe amorose sulle vittime

Le truffe amorose causano danni che vanno oltre la perdita finanziaria. Spesso provocano profondo disagio emotivo, problemi di salute mentale a lungo termine e isolamento sociale. La ricerca identifica costantemente questo tipo di truffa come una delle forme di frode più dannose e profonde, in particolare per gli anziani, poiché le vittime possono continuare a sperimentarne gli effetti psicologici, tra cui vergogna, insicurezza e trauma, anche per un decennio dopo l'evento.

Di seguito sono riportati i diversi impatti psicologici e di altro tipo a cui sono soggetti gli anziani in caso di truffa amorosa.

✦ Doppio trauma: perdita emotiva e finanziaria

Le truffe sentimentali in genere comprendono quello che può essere descritto come un "doppio colpo", ovvero il tradimento emotivo di una relazione percepita come intima, unito allo sfruttamento finanziario. Queste truffe spesso si svolgono nell'arco di mesi, durante i quali il truffatore costruisce una narrazione emotiva convincente e si guadagna la fiducia della vittima. Di conseguenza, l'impatto della frode costituisce non solo un tradimento finanziario, ma anche un profondo danno psicologico in cui le vittime sperimentano un profondo senso di abbandono, manipolazione e confusione di identità, che porta a un trauma emotivo più devastante della perdita economica.

I risultati empirici indicano che le vittime di problemi finanziari riportano un disagio emotivo significativamente più elevato rispetto alle vittime di problemi non finanziari, e che la truffa amorosa è il tipo di frode con il più alto impatto emotivo, e che molte delle vittime subiscono abusi emotivi, in particolare quando il grooming è stato prolungato e ha implicato una fiducia intima. In questi casi, la perdita improvvisa della "relazione" porta spesso a sintomi di disturbo dell'adattamento o a condizioni legate al trauma.

Vergogna e senso di colpa

Dopo una truffa, le vittime anziane spesso si incolpano per essere state ingannate, interiorizzando spesso la truffa come un fallimento personale. La vergogna crea una forte barriera alla richiesta di aiuto, anche alla propria cerchia ristretta. Secondo uno studio condotto, molte vittime evitano di parlare con familiari, amici o professionisti per paura di essere rifiutate o ridicolizzate. Questa risposta può radicare sentimenti di inutilità e ritardare il recupero emotivo, ed è qui che il ruolo dell'educatore diventa fondamentale per rassicurare le vittime, guadagnarsi la loro fiducia e farle sentire considerate, e per supportarle nell'agire contro la truffa.

Depressione e ansia

Molte vittime riferiscono sintomi di depressione clinica, tra cui disperazione, disturbi del sonno e scarsa energia. Spesso si manifesta anche ansia, soprattutto in relazione a questioni finanziarie, privacy o esposizione al pubblico. Questi effetti sono accentuati quando la vittima presenta vulnerabilità emotive preesistenti come dolore o solitudine. Questi sintomi non sono temporanei, poiché gli studi indicano danni psicologici a lungo termine e un maggiore bisogno di supporto psicosociale.

Ritiro sociale

Dopo la rivelazione, le vittime anziane potrebbero isolarsi dai coetanei e dalla comunità per l'imbarazzo. Alcune tagliano i ponti con le persone che hanno messo in dubbio la relazione o le hanno lanciate minacce quando erano a conoscenza della falsa "relazione". Questo isolamento e questa perdita di fiducia si estendono sia alle relazioni personali che a quelle istituzionali, contribuendo a una maggiore solitudine e al rischio di rivittimizzazione.

Attaccamento emotivo e dolore

Le vittime spesso instaurano veri e propri legami psicologici con la persona inventata dal truffatore, in base alla relazione che hanno costruito online prima della truffa. Quando l'inganno viene svelato, molte vittime provano un dolore paragonabile alla perdita di un partner romantico, e le vittime descrivono il truffatore come il loro "partner ideale" o "supporto emotivo", anche se la relazione era interamente online. Alcune vittime riferiscono un senso di lutto più intenso dell'effettiva perdita finanziaria. Ciò è dovuto al love bombing, alle false promesse di matrimonio e al costante rinforzo emotivo utilizzato durante la fase di adescamento.

Perdita di autostima e fiducia in se stessi

Molte vittime riferiscono un calo del senso di competenza personale e dignità dopo la truffa. Il tradimento spesso mina la loro fiducia nel processo decisionale e aumenta la dipendenza dagli altri. Questa perdita di potere può portare a fragilità emotiva a lungo termine e a riluttanza a intraprendere nuove relazioni o opportunità di apprendimento, oltre a sollevare dubbi sulla propria identità e sul proprio ruolo sociale.

Paura del giudizio e rifiuto della divulgazione

A causa dello stigma sociale, le vittime sono spesso riluttanti a denunciare la truffa o a cercare supporto emotivo. Chi denuncia spesso riporta reazioni di non supporto, che rafforzano ulteriormente il senso di colpa e la vergogna. Queste risposte di non supporto portano a un ulteriore isolamento, che contribuisce alla sottostima e riduce l'accesso ai servizi di supporto, rendendo la sensibilità e il ruolo degli educatori essenziali per creare un ambiente non giudicante che promuova la denuncia e l'intervento precoce.

Rischio di rivittimizzazione

Le vittime che non riconoscono o non accettano la truffa, soprattutto quelle che ignorano gli avvertimenti perché fiduciose, corrono un rischio maggiore di essere nuovamente prese di mira. Questa vittimizzazione ripetuta è legata alla negazione emotiva e alla convinzione persistente che l'intenzione del truffatore fosse sincera.

La situazione peggiora ulteriormente quando le vittime ignorano gli avvertimenti di terze parti; ecco perché gli educatori devono essere in grado di affrontare con delicatezza queste convinzioni, mantenendo al contempo fiducia e sostegno.

Declino della salute fisica e mentale

Nei casi più gravi, lo stress psicologico si manifesta fisicamente, con le vittime che riferiscono mal di testa, disturbi del sonno, attacchi di panico o esacerbazione di malattie croniche. Alcuni sperimentano ideazione suicidaria, soprattutto se non vivono in un ambiente di supporto, e sono vittime di vergogna e senso di colpa da parte delle loro cerchie più vicine, e hanno scelto di autoisolarsi.

Danni finanziari e dipendenza

Le vittime di truffe amorose hanno riportato perdite finanziarie che vanno da 50 a oltre 800.000 euro,

con perdite medie comprese tra 1.000 e 10.000 euro a caso. A causa di ciò, molte vittime soffrono di instabilità economica a lungo termine, accesso ridotto ai beni di prima necessità e, in alcuni casi, diventano dipendenti dal welfare familiare o pubblico. Alcune perdono persino la casa, i risparmi pensionistici o le eredità, il che può compromettere in modo permanente la loro qualità di vita.

Effetti psicologici a lungo termine

Molto tempo dopo la truffa amorosa, è diventato evidente che le vittime potrebbero continuare a provare dolore e traumi da tradimento, rifiuto della comunicazione online, sfiducia negli altri, relazioni interpersonali compromesse e persistente insicurezza finanziaria ed emotiva, bassa autostima e ansia fino a dieci anni dopo l'incidente.

2.4 Casi di studio reali su situazioni di truffe amorose:

Dopo aver compreso l'impatto della truffa amorosa e le vulnerabilità comportamentali e sociali delle vittime anziane potenzialmente vittime di truffe amorose, questa sezione menzionerà alcuni casi di studio reali, per rivelare non solo le tattiche impiegate dai truffatori, ma anche il costo emotivo, finanziario e psicologico per le vittime. Queste narrazioni servono come strumenti di apprendimento fondamentali per gli educatori, illustrando come si sviluppano le dinamiche della truffa, per individuare i segnali d'allarme in contesti reali e sottolineando la complessa interazione tra vulnerabilità, fiducia e inganno. I seguenti casi di studio si basano su episodi documentati in Europa e Australia, con enfasi sulla loro rilevanza per i temi comportamentali, emotivi e sistemici discussi nelle sezioni precedenti.

2.4.1 Caso di studio 1: La vittima francese di una truffa di impersonificazione di una celebrità

Uno dei casi di frode sentimentale più pubblicizzati degli ultimi anni ha coinvolto una donna francese di 53 anni, Anne, che è stata truffata per circa 830.000 euro da un truffatore che si spacciava per l'attore Brad Pitt. Secondo notizie e interviste condotte da Euronews e Le Monde, la truffa è iniziata quando Anne è stata contattata sui social media da un individuo che affermava di essere la madre di Pitt. Questo contatto si è poi trasformato in una comunicazione online diretta con un finto "Brad Pitt", supportata da foto generate dall'intelligenza artificiale, falsi eventi di beneficenza e immagini di ospedali. Nel corso di più di un anno, la relazione si è approfondita, Anne è diventata socialmente isolata e sempre più diffidente nei confronti di amici e familiari che mettevano in dubbio la legittimità della storia d'amore, e lei trasferì denaro per sostenere quelle che riteneva

Lfossero urgenti necessità finanziarie legate alle spese mediche e ai conti bancari congelati durante il divorzio di Pitt. La truffa sfruttava sia la manipolazione emotiva che l'inganno tecnologico, incluso l'uso di immagini di intelligenza artificiale e video chat simulate.
Dopo aver riconosciuto di essere stata truffata, Anna ha sofferto di gravi sentimenti psicologici di umiliazione, violazione emotiva e depressione. Dopo che la truffa è stata resa pubblica, ha dovuto subire cyberbullismo e scherni, aggravando il suo declino mentale.

2.4.2 Caso di studio 1: La vittima francese di una truffa di impersonificazione di una celebrità

Nel 2024, le autorità spagnole hanno scoperto un truffatore transnazionale che si spacciava per Brad Pitt, responsabile di aver truffato diverse donne anziane attraverso i social media, prendendo di mira i propri contatti in base alla profilazione psicologica.

In questo caso, il truffatore ha creato falsi profili, con tanto di convincenti narrazioni di interessi romantici e iniziative imprenditoriali. Le vittime sono state convinte a investire in progetti cinematografici di fantasia o in iniziative umanitarie presumibilmente guidate da Pitt. Complessivamente, le donne sono state truffate per oltre 325.000 euro. Gli investigatori hanno rintracciato i fondi attraverso una complessa rete di riciclaggio che coinvolgeva diversi account "mulo". Le autorità hanno sequestrato una serie di apparecchiature digitali, documenti e dispositivi mobili utilizzati per costruire e mantenere l'inganno.

Questo caso illustra due importanti spunti di riflessione educativa. In primo luogo, le truffe amorose coinvolgono sempre più reti criminali organizzate con portata transnazionale e capacità digitali. In secondo luogo, le vittime spesso nutrono un profondo attaccamento emotivo alla relazione costruita, che può compromettere la capacità di giudizio anche di fronte a un crescente sospetto. Ciò rafforza la necessità per gli educatori di affrontare sia la dimensione cognitiva che quella emotiva nei programmi di prevenzione delle truffe.

2.4.3 Caso di studio 3: Veronica Watson e le conseguenze della fiducia

Veronica Watson, una nonna australiana di 59 anni, è diventata un caso internazionale dopo essere stata arrestata in Brasile per contrabbando di cocaina a sua insaputa nel 2013. L'inganno è iniziato con un uomo che aveva incontrato online, il quale sosteneva di aver bisogno di aiuto per consegnare i documenti per un investimento. Dopo mesi di adescamento e di conquista della sua fiducia, l'uomo l'ha convinta a trasportare una valigia in Brasile, contenente 5kg di cocaina.

tVeronica fu poi arrestata all'aeroporto internazionale di San Paolo e trascorse oltre due anni in prigione prima di essere assolta. Il tribunale riconobbe che era stata vittima di frode. Tuttavia, il prezzo psicologico fu irreparabile, tra cui ansia persistente, stigma sociale e perdita di fiducia nelle sue capacità.

Questo caso sottolinea l'intersezione tra truffe sentimentali e altre forme di sfruttamento criminale, tra cui il traffico di droga e il riciclaggio di denaro. Illustra inoltre come l'adescamento possa portare le vittime non solo a perdite finanziarie, ma anche a conseguenze legali che cambiano la vita. Da una prospettiva educativa, rivela l'importanza di insegnare agli anziani non solo le truffe finanziarie, ma anche il "reclutamento basato sull'amore e sulle relazioni sentimentali" per attività criminali.

2.4.4 Caso di studio 4: Caso di truffa amorosa di Annette Ford

Annette Ford, una donna di 57 anni di Perth, in Australia, è stata vittima di truffe amorose due volte su diverse piattaforme di incontri. In totale, ha perso circa 780.000 dollari, tutti i risparmi di una vita. Le truffe sono avvenute dopo il suo divorzio, durante un periodo di vulnerabilità emotiva. In entrambi i casi, gli uomini che ha incontrato online hanno dichiarato di essere stati oggetto di rapide dimostrazioni d'affetto e di love bombing, per poi spacciarsi per professionisti in difficoltà finanziarie temporanee a causa di complicazioni all'estero.

Annette vendette la sua casa, svuotò il suo fondo pensione e prese in prestito denaro da inviare ai suoi truffatori. Si allontanò dalla sua famiglia, che non era d'accordo con le sue decisioni. In seguito alla truffa, Annette rimase senza casa e dipendente dal sostegno pubblico. Le conseguenze psicologiche includevano depressione, insonnia e attacchi di panico.

Il suo caso include conseguenze a lungo termine, tra cui perdita di potere economico, isolamento sociale e grave disagio psicologico. Dimostra inoltre come un trauma pregresso, derivante da un divorzio, possa interagire con l'esposizione a truffe, esacerbando la vulnerabilità emotiva. Per gli educatori, questo evidenzia la necessità di strategie di prevenzione basate sul trauma, adattate ai contesti complessi in cui si verificano le truffe.

2.4.5 Uomo dell'Irlanda del Nord truffato di oltre 200.000 sterline

Un altro caso riguarda un uomo dell'Irlanda del Nord che ha perso più di 200.000 sterline dopo aver avuto una presunta relazione sentimentale iniziata su un'app di incontri e proseguita dal 2020 al 2025.

Credeva di avere una relazione con una donna conosciuta online e, nel corso di due anni, aveva trasferito ingenti somme di denaro in risposta a richieste apparentemente urgenti: spese legali legate al testamento di un parente, spese mediche per un incidente d'auto e un falso link manipolato per un servizio bancario online.

Questa truffa sfruttava sia la dipendenza emotiva che la manipolazione tecnologica. La vittima ha dichiarato che la truffa era di proporzioni tali da avergli quasi distrutto la vita e lasciato un profondo stato emotivo e finanziario. Alla fine ha contattato il Servizio di Polizia dell'Irlanda del Nord (PSNI), che lo ha aiutato a recuperare i fondi.

2.4.6 Uomo di Wrexham truffato per 25.000 sterline

Inoltre, all'inizio del 2024, un uomo di 65 anni di Wrexham, nel Regno Unito, è stato truffato di circa 25.000 sterline dopo essersi iscritto a un sito di incontri online nel marzo 2023, a causa di un periodo di solitudine e allontanamento familiare. Di conseguenza, ha interagito con una persona tramite il sito di incontri, che ha spostato la conversazione su WhatsApp e lo ha contattato quotidianamente.

Poco dopo, il truffatore ha richiesto dei fondi come deposito per acquistare una casa insieme e ha reindirizzato la vittima affinché inviasse denaro, buoni regalo Apple, gioielli e un iPhone attraverso più indirizzi.

Ciò è continuato fino a gennaio 2021, quando l'uomo ha denunciato la vittima alla polizia. È rimasto profondamente colpito, poiché la promessa emotiva di un "futuro condiviso" ha giocato un ruolo centrale nel suo coinvolgimento e nella sua perdita. Gli sono state offerte chiamate di supporto per superare la situazione.

2.4.7 Conclusioni dei casi di studio sopra riportati e implicazioni educative

Questi casi di studio rivelano sia la diversità delle tattiche di truffa sia le emozioni comuni

e modelli cognitivi sfruttati dai truffatori. Si può concludere che, sebbene le vittime provengano da contesti socioeconomici e paesi diversi, sono accomunate da temi psicologici come il dolore, l'isolamento e le narrazioni romantiche idealizzate. È qui che entra in gioco il ruolo degli educatori e degli operatori giovanili, che devono riconoscere la profondità dell'attaccamento emotivo che le vittime sviluppano, la sofisticatezza delle tattiche dei truffatori e la complessità del recupero post-vittimizzazione, che include non solo il danno finanziario, ma anche il deterioramento della salute mentale e lo stigma sociale.

2.5 Casi di studio reali su situazioni di truffe amorose:

Sulla base delle informazioni precedentemente illustrate sulle vulnerabilità psicologiche delle vittime, sugli impatti e sulle intuizioni derivanti dai casi di studio reali sopra menzionati, diventa più chiaro che questa minaccia emergente e in rapida crescita delle truffe amorose tra gli anziani richiede un approccio coordinato e proattivo. In qualità di attori in prima linea all'interno delle infrastrutture comunitarie, educative e sociali, educatori e operatori giovanili svolgono un ruolo centrale in quanto professionisti in una posizione unica per identificare i segnali di allarme precoci, implementare quadri preventivi e facilitare il recupero in caso di vittimizzazione. Pertanto, data la loro importanza, è fondamentale comprendere più chiaramente perché educatori e operatori giovanili debbano essere coinvolti, e non solo le autorità legali o la comunità.

2.5.1 Gli educatori come guardiani della consapevolezza e della prevenzione delle truffe

Gli educatori che lavorano con gli anziani, in particolare nei centri comunitari e nei programmi di formazione per adulti, hanno una grande capacità di individuare i primi segnali di coinvolgimento in una truffa. Sono spesso il primo punto di contatto costante per gli anziani al di fuori delle strutture familiari, grazie alla loro capacità di osservare oggettivamente i cambiamenti comportamentali, avviare conversazioni non minacciose e fornire ambienti di apprendimento strutturati che supportano la diagnosi precoce.

Secondo uno studio di ricerca, è stato spiegato che gli anziani sono più propensi a rivelare le esperienze di truffa agli educatori che alle autorità o alla famiglia, soprattutto quando esiste questo rapporto di supporto e non giudicante. Questa fiducia pone gli educatori in una posizione privilegiata per avviare conversazioni preventive, indirizzare i ragazzi verso servizi appropriati e normalizzare le discussioni sulle esperienze di truffa.

Inoltre, secondo studi sperimentali, è stato scoperto che attività educative come giochi e workshop anti-truffa migliorano significativamente la consapevolezza delle truffe negli anziani, riducono la suscettibilità e aumentano l'autoefficacia nell'identificare le tattiche di truffa, nonché la loro alfabetizzazione digitale, riducendo la dipendenza da interazioni online false. Inoltre, questa strategia educativa è considerata la strategia di intervento precoce più efficace contro lo sfruttamento finanziario. Inoltre, gli educatori possono fungere da impalcature cognitive, soprattutto per gli individui che sperimentano un declino cognitivo in fase iniziale, rafforzando la memoria, il giudizio e il pensiero critico attraverso un coinvolgimento regolare. Questi risultati evidenziano la capacità dei formati educativi e degli educatori di influenzare sia il comportamento che la mentalità degli studenti più anziani.

2.5.2 Gli operatori giovanili come ponti verso la sicurezza digitale e l'empatia

Gli operatori giovanili svolgono un ruolo fondamentale nel promuovere l'apprendimento intergenerazionale. Gli anziani spesso non possiedono competenze digitali, un fattore di rischio chiave nelle truffe amorose. Attraverso il mentoring, gli educatori possono insegnare agli anziani come riconoscere i profili falsi, segnalare messaggi sospetti e gestire le impostazioni sulla privacy online. È importante sottolineare che questo scambio rafforza anche la resilienza emotiva attraverso l'inclusione sociale e la condivisione di obiettivi, entrambi fattori che riducono la suscettibilità alle truffe.
La ricerca ha inoltre sottolineato che gli sforzi preventivi devono includere programmi educativi adattati alle vulnerabilità delle popolazioni più anziane. Ciò include l'importanza di formare gli educatori per gestire non solo i deficit informativi, ma anche i traumi emotivi e la dissonanza cognitiva associati all'esposizione alle truffe.

2.5.3 Fiducia professionale e accesso sistemico

Gli educatori spesso godono di una posizione di fiducia che può incoraggiare le vittime a rivelare informazioni sensibili che potrebbero nascondere alla famiglia o alle autorità senza provare vergogna o senso di colpa. Questo pone gli educatori in una posizione di forza, dopo aver creato una rete sicura per guidare le vittime verso percorsi di denuncia, collaborare con le forze dell'ordine e gli avvocati e coinvolgere servizi di supporto per la salute mentale e il recupero finanziario.

Gli educatori hanno anche una portata istituzionale attraverso partnership con biblioteche, centri sanitari, chiese e reti di club per anziani che possono essere mobilitate per raggiungere gli anziani e supportarli in tali truffe attraverso misure preventive e reattive.

2.5.4 Gli operatori giovanili come agenti di empowerment intergenerazionale

Gli operatori giovanili vengono spesso trascurati nelle discussioni sulla tutela degli anziani, eppure il loro ruolo è fondamentale per promuovere la sicurezza digitale e la connessione sociale. Gli operatori giovanili, in quanto educatori, si concentrano principalmente sulla promozione della crescita e del cambiamento. Questo è in stretta linea con le esigenze degli anziani che si muovono in relazioni online non familiari. È stato anche studiato che i programmi intergenerazionali che abbinano anziani a mentori digitali più giovani hanno mostrato risultati promettenti nell'aumentare i tassi di individuazione delle truffe, nel migliorare la fiducia negli strumenti online e nel ridurre l'isolamento sociale, che è uno dei fattori di rischio più potenti per le truffe sentimentali, poiché gli operatori giovanili facilitano questi impegni, modellando al contempo sani confini digitali e una valutazione critica delle identità online.

2.5.5 Importanza della formazione e del supporto strutturale

Educatori e operatori giovanili dispongono di strumenti e formazione utili per supportare adeguatamente gli anziani. Tra questi:

- Conoscenza delle tipologie di truffa, delle tattiche di adescamento e dei segnali comportamentali
- Accesso a checklist, guide digitali sull'igiene e modelli di segnalazione
- Collaborazioni con le forze dell'ordine, gli operatori sanitari e le agenzie di tutela finanziaria degli anziani.
- Strumenti per la segnalazione anonima e il percorso di segnalazione.

Sulla base degli elementi sopra menzionati, è evidente che nel nostro mondo frenetico, il ruolo degli educatori nel supportare le vittime o potenziali vittime di truffe amorose e romantiche non è solo importante, ma anche necessario, poiché hanno un grande impatto nell'applicazione delle diverse misure preventive e reattive, come verrà spiegato più avanti in questo capitolo.

2.6 Misure preventive per proteggere gli anziani dai truffatori

Per proteggere efficacemente gli anziani da possibili truffe amorose, è essenziale implementare misure preventive che riducano la probabilità di cadere in queste truffe. Fornendo agli anziani gli strumenti e le conoscenze necessarie per riconoscere ed evitare le truffe, nonché promuovendo un ambiente sociale di supporto e migliorando le competenze delle vittime, possiamo ridurre significativamente il rischio di diventarne vittime. Queste misure includono lo sviluppo dell'alfabetizzazione digitale e la promozione delle relazioni sociali, entrambi fattori fondamentali per aiutare gli anziani a orientarsi in un mondo che si basa sempre più sulla tecnologia e sulle reti personali.

2.6.1 Consapevolezza dell'alfabetizzazione digitale

Una delle misure preventive più importanti per gli anziani è migliorare la loro alfabetizzazione digitale. Con l'avanzare della tecnologia, i truffatori adattano costantemente i loro metodi per creare giochi di ruolo con diversi scenari simili alla vita reale, in cui gli educatori possono osservare come gli anziani rilevano profili falsi, capiscono le impostazioni sulla privacy, notano segnali d'allarme negli scenari online e eseguono ricerche inverse per immagini, per poi riflettere con loro attraverso discussioni coinvolgenti. Mettere gli anziani in situazioni simili alla vita reale li aiuterà ad applicare quanto appreso nel mondo reale.

Workshop sulle tattiche truffaldine più comuni:

Offrire workshop mirati è un modo efficace per istruire gli anziani sulle truffe online più comuni in cui potrebbero imbattersi. Questi workshop dovrebbero coprire le basi per identificare email di phishing, profili falsi sui social media o sui siti di incontri, intelligenza artificiale e altre truffe come le false chiamate di supporto tecnico. Gli educatori dovrebbero concentrarsi sulla fornitura di esempi pratici di queste tattiche, mostrando come i truffatori spesso utilizzino un linguaggio pressante, promesse di ricompense o appelli emotivi per manipolare le loro vittime. Gli educatori dovrebbero anche concentrarsi sull'uso dell'intelligenza artificiale e su come confrontare o concludere immagini o testi prodotti da strumenti di intelligenza artificiale. L'obiettivo di questi workshop è fornire agli anziani la capacità di riconoscere i segnali di allarme e di sentirsi sicuri di poter identificare potenziali truffe.

Formazione pratica:

L'alfabetizzazione digitale va oltre la semplice comprensione delle truffe: si tratta di fornire agli anziani le competenze per utilizzare la tecnologia in modo sicuro. Sessioni di formazione pratica possono insegnare agli anziani come utilizzare i social media in modo sicuro, ad esempio come modificare le impostazioni sulla privacy, verificare l'identità delle persone incontrate online, riconoscere link sospetti o richieste di informazioni personali e osservare gli script di conversazione più comuni spesso utilizzati dai truffatori. Ad esempio, possono imparare a individuare un'email di phishing controllando l'indirizzo del mittente, cercando errori di ortografia o identificando allegati sospetti. Gli insegnanti possono anche insegnare loro come utilizzare siti web sicuri (con "https://" nell'URL) e come evitare di scaricare file da fonti non attendibili. Inoltre, gli anziani dovrebbero essere istruiti su come segnalare attività sospette, che si tratti di un'email fraudolenta, di una telefonata truffaldina o di un profilo online discutibile. Per rendere questa formazione più efficace, è consigliabile che gli insegnanti svolgano esercizi e attività applicative come parte della formazione, come la creazione di giochi di ruolo con diversi scenari simili alla vita reale, in cui gli insegnanti possano notare

l'individuazione da parte dell'anziano di profili falsi, la comprensione delle impostazioni sulla privacy, l'individuazione di segnali d'allarme in scenari online e la ricerca inversa di immagini, per poi riflettere con loro attraverso discussioni coinvolgenti. Mettere gli anziani in situazioni simili nella vita reale li aiuterà ad applicare quanto appreso nel mondo reale.

- **Sessioni di coinvolgimento della comunità:**

Dovrebbero essere organizzate anche sessioni di sensibilizzazione per fornire indicazioni sul ruolo delle forze dell'ordine, sulle procedure di sicurezza bancaria e finanziaria, sulla sicurezza informatica e su come comportarsi in caso di truffa sentimentale, nonché sulle relative procedure. Anche gli esperti dovrebbero essere invitati a queste sessioni di sensibilizzazione periodiche. Inoltre, dovrebbero essere condivisi modelli per la segnalazione delle diverse voci. Tutto ciò può essere incluso anche in dispense stampate e supporti visivi, per fungere da promemoria e rassicurare l'anziano sui passi successivi da compiere in caso di truffa.

2.6.2 Promuovere la connessione sociale

Un'altra misura preventiva fondamentale è promuovere le relazioni sociali. Molte truffe prendono di mira anziani vulnerabili che si sentono isolati o soli. Costruire un senso di comunità e incoraggiare l'interazione sociale non solo aiuta gli anziani a rimanere in contatto, ma fornisce loro anche il supporto e le risorse di cui hanno bisogno per riconoscere quando qualcosa non va. Questo può essere fatto attraverso discussioni di gruppo, incontri di supporto tra pari e sistemi di amicizia.

Attività di gruppo e sistema di amicizia

- **Attività di gruppo:**

Incoraggiare gli anziani a partecipare ad attività di gruppo può ridurre significativamente il senso di isolamento, che spesso porta alla vulnerabilità. Club tra pari, circoli di hobby e incontri virtuali sono ottimi modi per riunire gli anziani, condividere interessi comuni e costruire relazioni significative. Interagendo regolarmente con gli altri, gli anziani hanno meno probabilità di essere influenzati da truffatori che cercano di sfruttare i loro bisogni emotivi o sociali. Le attività di gruppo offrono anche uno spazio sicuro in cui discutere di eventuali incontri sospetti, ricevere consigli dai coetanei e rimanere informati sulle potenziali truffe che circolano nella comunità. Ad esempio, un club del libro o un gruppo di artigianato possono essere un modo prezioso per coinvolgere gli anziani in un ambiente sociale, promuovendo sia la stimolazione mentale che il benessere sociale.

- **Sistemi di amici:**

Un altro modo efficace per promuovere la connessione sociale e ridurre l'isolamento è l'implementazione di sistemi di "buddy". Mettere in coppia gli anziani per incontri regolari, condividere esperienze e offrirsi supporto reciproco aiuta a creare un senso di cameratismo. Quando gli anziani si sentono più connessi con gli altri, hanno meno probabilità di cadere vittime di truffe, perché hanno una persona di fiducia a cui rivolgersi in caso di situazioni sospette. Un sistema di "buddy" offre anche agli anziani un modo per rimanere informati su potenziali truffe, poiché possono scambiarsi informazioni su truffe recenti o segnali d'allarme riscontrati. Inoltre, il supporto emotivo di un "buddy" può far sentire gli anziani più sicuri, riducendo la probabilità che cerchino compagnia da fonti potenzialmente fraudolente.

B. Ampliare il supporto sociale ed emotivo

- Oltre alle attività di gruppo e ai sistemi di supporto reciproco, è essenziale promuovere una rete più ampia di supporto. Centri comunitari locali, organizzazioni per anziani e gruppi online focalizzati su interessi specifici possono aiutare gli anziani a mantenere una vita sociale attiva, riducendo il rischio di isolamento o vulnerabilità emotiva. Quando gli anziani hanno una solida rete sociale, sono meglio attrezzati a gestire situazioni in cui potrebbero sentirsi manipolati o sotto pressione, poiché possono contare sulla guida di amici o familiari fidati.

- Inoltre, fornire supporto emotivo agli anziani in lutto, in solitudine o alle prese con altre difficoltà emotive può aiutare a impedire ai truffatori di sfruttare queste vulnerabilità. Offrire servizi di consulenza per l'elaborazione del lutto, gruppi di terapia e programmi di tutoraggio può essere fondamentale per aiutare gli anziani a gestire il proprio benessere emotivo, riducendo le probabilità di essere presi di mira da truffatori in cerca di una preda facile.

Combinando gli sforzi per sviluppare l'alfabetizzazione digitale con strategie per promuovere le relazioni sociali, gli anziani possono diventare più resilienti a truffe e frodi. Educatori, operatori sanitari e leader della comunità svolgono un ruolo fondamentale nell'attuazione di queste misure preventive. Che si tratti di workshop che insegnano la sicurezza digitale o di programmi sociali che riducono l'isolamento, queste iniziative aiutano gli anziani a mantenere la propria indipendenza e sicurezza in un mondo che si affida sempre più alla tecnologia e alle interazioni sociali. Insieme, queste misure preventive creano una solida base per salvaguardare gli anziani dalla minaccia sempre crescente delle truffe.

2.7 Come fermare le truffe amorose nelle fasi iniziali in base agli indicatori comportamentali di chi è vittima di truffa:

Dopo aver appreso le misure che gli educatori possono adottare per impedire che gli anziani cadano in truffe in futuro, vale la pena riflettere anche sulle misure che gli educatori dovrebbero adottare nel caso in cui si accorgano di truffe sentimentali in corso tra le vittime anziane. Per affrontare questo problema, verranno menzionati gli indicatori comportamentali, alcuni dei quali sono stati presi in considerazione nei casi di studio reali sopra menzionati, per supportare educatori, operatori giovanili e operatori sanitari nell'individuazione precoce delle truffe sentimentali. Successivamente, verranno menzionati alcuni strumenti di valutazione e misure affinché gli educatori siano informati su come agire una volta individuato un caso di truffa sentimentale in corso.

2.7.1 Segnali di allarme comportamentali delle vittime anziane

Prevenire i danni causati dalle truffe sentimentali non si basa solo su una consapevolezza diffusa, ma anche sull'identificazione precoce di segnali e segnali d'allarme comportamentali ed emotivi che indicano che un individuo potrebbe essere entrato nel processo di truffa amorosa. Numerosi studi confermano che le truffe sentimentali seguono in genere una progressione strutturata dal contatto iniziale, al grooming emotivo, alla richiesta di finanziamenti e, infine, all'isolamento sociale, e ciascuna di queste fasi è caratterizzata da specifici cambiamenti nel comportamento che, se interpretati correttamente, possono segnalare la necessità di un intervento tempestivo e mirato. Questi segnali d'allarme includono quanto segue:

- **Segretezza che circonda le nuove relazioni online:**

Le vittime spesso nascondono la loro comunicazione con il truffatore per paura di essere giudicate o di essere percepite come tradite dal loro "partner" online. Questo è in linea con i risultati di studi di ricerca che hanno evidenziato come le vittime evitino deliberatamente di rivelare i propri dati, soprattutto quando sono emotivamente coinvolte.

- **Uso eccessivo e improvviso del telefono o di Internet:**

Le vittime tendono a impegnarsi in modo compulsivo nella comunicazione digitale, spesso apparendo emotivamente dipendenti dalle app di messaggistica o dalle video chat.

- **Ritiro sociale:**

Con l'intensificarsi dell'adescamento, le vittime possono iniziare a evitare eventi della comunità, incontri tra coetanei,

e persino le interazioni familiari. Potrebbero anche assumere un atteggiamento difensivo nei confronti delle attività online. Uno studio di ricerca ha scoperto che i truffatori prosperano isolando le proprie vittime da fonti di influenza concorrenti.

- **Stati emotivi intensificati:**

Le vittime possono provare sensazioni che vanno dall'euforia (quando ricevono messaggi dal truffatore) all'ansia o alla tristezza (quando il truffatore è assente o chiede denaro). Inoltre, possono riscontrare improvvisi cambiamenti di umore o di comportamento. Queste fluttuazioni affettive non devono essere liquidate come una generale instabilità dell'umore, ma piuttosto valutate nel contesto di nuovi legami sociali.

- **Attività finanziaria inspiegabile:**

Insegnanti e familiari potrebbero notare prelievi allo sportello bancomat, bonifici bancari improvvisi o richieste di assistenza per operazioni bancarie internazionali. Uno studio di ricerca spiega che tali transazioni sono spesso precedute da una riduzione del monitoraggio cognitivo e delle capacità di calcolo finanziario.

2.7.2. Il ruolo dell'educatore nell'individuare una truffa in corso e nel supportare gli anziani

Educatori e operatori giovanili sono in una posizione privilegiata per individuare questi indicatori precoci. A differenza dei familiari, che potrebbero non avere una visione oggettiva dello stato emotivo dell'individuo, gli educatori sono spesso inseriti in contesti di gruppo strutturati, dove possono osservare oggettivamente i cambiamenti nel tempo. Ad esempio, gli anziani che si entusiasmano insolitamente per una nuova conoscenza online, menzionano spesso una relazione idealizzata o iniziano a ritirarsi dagli eventi della comunità, come menzionato sopra.
Gli educatori dovrebbero combinare l'osservazione con la capacità di distinguere i comportamenti dall'invecchiamento generale o dalle fluttuazioni dell'umore. Gli educatori possono utilizzare strumenti di screening brevi e non invasivi in contesti di gruppo o conversazioni individuali. In caso di dubbi, gli educatori possono avviare una conversazione individuale ponendo domande neutre e aperte che evitino il confronto e la vergogna, come: "Ti sei sentito al sicuro e rispettato nelle tue interazioni online?" oppure "Hai notato richieste o conversazioni insolite online?", "Hai incontrato qualcuno di nuovo online di recente?" o "Qualcuno ti ha chiesto un'informazione finanziaria?"

"favorire o mantenere un segreto?". Queste domande permettono agli anziani di riflettere senza mettersi sulla difensiva. In questo modo, gli educatori promuovono un clima di fiducia piuttosto che di intrusione. Nel caso in cui si noti che la vittima anziana non risponde molto bene alle domande, si possono utilizzare discussioni simulate attraverso l'uso di storie anonime o personaggi ipotetici, in cui gli educatori possono esplorare e informare sui rischi senza confrontarsi direttamente con l'individuo. È stato dimostrato che questo metodo riduce la vergogna e aumenta il pensiero riflessivo.

Una volta individuati i segnali comportamentali e confermata l'esistenza di una truffa da parte degli anziani, gli educatori dovrebbero adottare un modello di triage soft: coinvolgere, educare e valutare. La fase di coinvolgimento si concentra sull'ascolto e sulla dimostrazione di preoccupazione, confermando al contempo che si tratta di un ambiente non giudicante. La fase educativa prevede la fornitura di informazioni generali sulle truffe sentimentali online, idealmente attraverso formati neutri come opuscoli, video o discussioni di casi anonimi. Questo metodo indiretto consente agli individui di identificarsi con i modelli descritti senza sentirsi accusati. La fase di valutazione, spesso svolta in modo informale, consiste nel valutare se l'individuo è aperto a ulteriori discussioni o supporto, o se potrebbe essere necessario un rinvio esterno.

Inoltre, gli approcci indiretti basati su gruppi migliorano ulteriormente la diagnosi precoce. Quando l'educazione alla truffa è integrata nella programmazione regolare, gli anziani sono più propensi a riconoscere la manipolazione nelle proprie esperienze o in quelle altrui, e si sentiranno anche considerati e non soli, il che li porterà a provare meno vergogna e ad essere più aperti a ricevere aiuto. Inoltre, avere contesti di gruppo e cercare di coinvolgerli nuovamente nelle diverse attività li aiuterà a sentirsi di nuovo più coinvolti nella comunità e meno coinvolti con il truffatore, portandoli infine ad abbandonarlo.

In sintesi, gli educatori devono trattare i primi indicatori comportamentali non come curiosità isolate, ma come potenziali sostenitori. Sviluppando la sensibilità all'osservazione, utilizzando una comunicazione informata e integrando il riconoscimento delle truffe, possono individuare e interrompere le truffe sentimentali nella loro fase iniziale, prima che si verifichino danni finanziari o psicologici.

2.8 Misure di risposta nel caso in cui una vittima cada in una truffa amorosa

Dopo aver analizzato le misure da adottare per prevenire una truffa sentimentale, o cosa dovrebbero fare gli educatori per individuare un anziano che sta per cadere in una truffa e per salvarlo dal rischio di ricadere in essa nelle fasi iniziali, questa sezione analizzerà le misure di risposta da adottare nel caso in cui un anziano cada completamente vittima di una truffa sentimentale. In questo caso, è essenziale gestire la situazione con attenzione, empatia e un approccio strutturato. Queste truffe sono particolarmente dannose perché fanno leva sulla vulnerabilità emotiva degli anziani, causando spesso un notevole disagio emotivo e perdite finanziarie. È importante reagire rapidamente, assicurandosi che l'anziano si senta supportato e in grado di intraprendere le azioni necessarie per riprendersi dalla truffa. Di seguito sono riportate le misure da adottare in caso di truffa in fase avanzata:

Ascolta e rassicura

Il primo passo per affrontare una truffa amorosa è ascoltare l'esperienza dell'anziano senza giudicarlo. Molti anziani che cadono vittime di truffe sentimentali spesso si sentono in imbarazzo, in imbarazzo o persino umiliati. Potrebbero aver investito non solo denaro, ma anche la loro energia emotiva in una relazione che credevano autentica. È fondamentale convalidare i loro sentimenti e rassicurarli sul fatto che non hanno alcuna colpa. Pertanto, gli educatori devono rispondere con un approccio strutturato e consapevole del trauma, che tenga conto della dignità della vittima e della sua stabilizzazione psicologica, poiché una gestione scorretta del momento della rivelazione può portare a un nuovo trauma o a un ulteriore silenzio, in particolare tra gli anziani, che potrebbero già lottare contro l'esclusione digitale e la sfiducia generazionale nelle autorità.

I truffatori sono abili nel manipolare le emozioni e creare un falso senso di intimità, facilitando le truffe per gli anziani. Pertanto, è importante che gli educatori convalidino l'esperienza della vittima e spieghino con delicatezza che non è sola e che molti altri sono caduti vittime di truffe simili. Rassicurateli sul fatto che questi autori sono criminali e che le loro perdite emotive e finanziarie sono il risultato diretto di azioni fraudolente, non del loro scarso giudizio.

Offrire empatia e comprensione può aiutare ad alleviare sensi di colpa o imbarazzo, che possono rappresentare un ostacolo alla segnalazione dell'incidente e alla ricerca di aiuto. Fai sapere all'anziano che ha il tuo pieno supporto e che la guarigione è possibile, e non incolparli, non interrogarli o minimizzare la loro esperienza, poiché ciò causerebbe un danno emotivo molto profondo e li renderebbe inclini a ricadere in truffe più e più volte in futuro.

B. Documentare l'incidente

Una volta che l'anziano si sente supportato, il passo successivo è aiutarlo a documentare i dettagli della truffa. Registrare informazioni importanti aiuterà le forze dell'ordine e le agenzie per la tutela dei consumatori nelle loro indagini. Incoraggiate l'anziano a scrivere i seguenti dettagli:

- Date: registra quando è iniziata la truffa, quando sono stati effettuati i pagamenti e qualsiasi altra interazione significativa.
- Nomi utilizzati dal truffatore: il/i nome/i utilizzato/i dal truffatore, anche se fittizi o fittizi. Questo può aiutare le autorità a rintracciare il truffatore.
- Importi inviati: registra l'importo di denaro inviato al truffatore, nonché eventuali altre transazioni finanziarie e le informazioni sui suoi conti.
- Canali di comunicazione: documentare il modo in cui il truffatore ha comunicato con l'anziano (ad esempio, e-mail, telefonate, social media o siti di incontri).

Questa documentazione è fondamentale, in quanto fornisce una chiara testimonianza della truffa e può fungere da prova per le indagini. Sarà inoltre utile per presentare segnalazioni alle agenzie competenti.

C. Segnalare tempestivamente

Il passo successivo fondamentale è segnalare la truffa. Agire rapidamente è essenziale per limitare ulteriori perdite finanziarie e facilitare le indagini. Aiutate l'anziano a segnalare la truffa alle autorità competenti, come le forze dell'ordine locali, le agenzie per la tutela dei consumatori o il numero verde nazionale dedicato alla segnalazione delle frodi. Alcuni luoghi chiave per segnalare una truffa sentimentale includono:

- Forze dell'ordine locali: sporgere denuncia alla polizia il prima possibile. In caso di perdite finanziarie significative, le forze dell'ordine locali possono avviare un'indagine o mettere in contatto la vittima con l'agenzia competente.

- Federal Trade Commission (FTC): la FTC è l'agenzia governativa statunitense responsabile della tutela dei consumatori. Gli anziani possono segnalare le truffe tramite il sito web ReportFraud.ftc.gov. La FTC fornisce anche preziose risorse su come proteggersi da future truffe.
- Internet Crime Complaint Center (IC3): gli anziani che sono stati presi di mira da truffatori che utilizzano piattaforme online (come siti di incontri o social media) possono segnalare la truffa all'IC3, una partnership tra l'FBI e il National White Collar Crime Center. Visita IC3.gov per maggiori informazioni.
- Numero verde nazionale per le frodi: i paesi dispongono di servizi di segnalazione delle frodi che possono essere utilizzati per aiutare le autorità a indagare e rintracciare il truffatore. Ad esempio, nel Regno Unito, gli anziani possono contattare Action Fraud all'indirizzo ActionFraud.police.uk per ricevere assistenza.
- Agenzie per la tutela dei consumatori: molti stati o comuni dispongono di agenzie per la tutela dei consumatori che gestiscono i casi di frode. Il formatore dovrebbe cercare l'agenzia nel proprio paese e indirizzare la vittima ad essa. In Germania, ad esempio, gli anziani possono contattare la Verbraucherzentrale Bundesverband (VZBV), l'agenzia centrale tedesca per la tutela dei consumatori che fornisce un ampio supporto alle vittime di frode, inclusi modelli legali, sessioni di consulenza e linee guida sulla sicurezza digitale. A livello europeo, le vittime possono segnalare frodi digitali transfrontaliere tramite la Rete dei Centri Europei dei Consumatori (ECC-Net) o presentare reclami transnazionali tramite l'interfaccia di EUROPOL per la segnalazione dei reati su Internet.
- Istituti finanziari e banche: assicuratevi di segnalare la truffa alla banca locale da cui la vittima ha trasferito il denaro al truffatore. Questo aiuterà a tracciare il trasferimento ed eventualmente a segnalarlo per recuperare il denaro della vittima.
- Centri di supporto psicologico: le vittime dovrebbero anche essere indirizzate a organizzazioni che offrono consulenza psicologica, assistenza alle vittime e accompagnamento in tribunale. Ad esempio, in Germania, possono essere indirizzate a Weißer Ring, la più grande organizzazione tedesca per le vittime di reati, che offre supporto psicologico gratuito. Inoltre, i casi transfrontalieri che coinvolgono truffatori internazionali possono essere segnalati all'OLAF (Ufficio europeo per la lotta antifrode) o tramite l'Ufficio europeo per la lotta finanziaria e la lotta contro le frodi di Europol.

- Centro per la criminalità economica (EFECC) per un potenziale tracciamento internazionale.

Segnalando tempestivamente la truffa, gli anziani non solo si proteggono da ulteriori perdite, ma aiutano anche le forze dell'ordine a rintracciare i truffatori e a impedire che altri cadano vittime di truffe simili.

2.9 Creazione di reti di supporto a lungo termine:

Dopo aver aiutato le vittime anziane a denunciare i truffatori, è fondamentale continuare a contattare la vittima nelle settimane e nei mesi successivi alla denuncia. Gli studi dimostrano che molti anziani subiscono vittimizzazioni secondarie, tra cui rifiuto, incredulità o scherno da parte della famiglia o della comunità, che possono aggravare il trauma e portare a un isolamento prolungato, a una nuova vittimizzazione o a sintomi da stress post-traumatico. Pertanto, la riabilitazione emotiva a lungo termine, il reinserimento sociale e l'empowerment sono fondamentali, e educatori e operatori giovanili svolgono un ruolo fondamentale in questa fase, per mantenere i contatti e offrire il reinserimento nella comunità, nonché il reinserimento emotivo.

Per raggiungere questo obiettivo, in primo luogo, gli operatori giovanili e gli educatori dovrebbero incoraggiare le vittime a partecipare a gruppi di supporto o circoli di recupero guidati dai pari, dove i sopravvissuti possano condividere le proprie esperienze in modo confidenziale e senza giudizio. Questi gruppi possono essere ospitati da centri di formazione per adulti, dove lavorano, o da circoli aperti a tutte le fasce d'età. Questo ridurrà il loro isolamento e rafforzerà l'integrazione sociale, poiché, secondo studi di ricerca, è stato riscontrato che gli anziani che partecipano a un coinvolgimento strutturato tra pari dopo una truffa segnalano un significativo miglioramento della resilienza psicologica e una riduzione della vulnerabilità alla recidiva.

Un altro aspetto fondamentale è che gli educatori forniscano un follow-up attraverso la programmazione di incontri di controllo e un rafforzamento educativo continuo. Questo aiuta gli educatori a comprendere i bisogni delle vittime e le fa sentire supportate, il che le aiuterà a riprendersi emotivamente e a reinserirsi socialmente. Vale anche la pena notare che, in tutte le fasi della risposta, il principio guida deve rispettare l'autonomia e la dignità della vittima, e gli educatori non sono investigatori o consulenti, ma alleati fidati in un percorso di recupero che può coinvolgere più professionisti. Il loro ruolo è quello di confermare l'esperienza della vittima, rimetterla in contatto con l'agire e garantire che non venga lasciata sola ad affrontare le conseguenze del trauma.

Inoltre, gli educatori possono incoraggiare le vittime a partecipare a terapie di gruppo, counseling basato sul trauma ed esercizi di ricostruzione narrativa, poiché è stato dimostrato che aiutano a ricostruire identità e capacità di azione. Ad esempio, in Germania, i sopravvissuti possono accedere a tali servizi tramite le assicurazioni sanitarie pubbliche locali (ad esempio, AOK, TK) o organizzazioni come Weißer Ring, che offrono consulenza specializzata per traumi correlati al crimine. Anche i centri per anziani comunali e le reti sanitarie possono fungere da punti di accesso a servizi di salute mentale non stigmatizzanti.

Il reinserimento digitale è un altro elemento chiave per il recupero a lungo termine. Molte vittime hanno paura di interagire nuovamente con gli strumenti digitali, aumentando così il loro isolamento. Educatori e operatori giovanili possono contribuire a ripristinare la fiducia offrendo workshop di reinserimento digitale, pensati per insegnare la sicurezza online, le impostazioni della privacy, l'identificazione delle truffe e i limiti della comunicazione. Questo sarà particolarmente efficace nell'aiutare gli anziani a reinserirsi nel mondo digitale in modo sicuro e solidale.

Un altro punto cruciale è la creazione di kit di strumenti e workshop informativi e di orientamento per le famiglie e gli amici di queste vittime, in cui si incoraggi il dialogo aperto e si forniscano informazioni su come reagire e supportare gli anziani per migliorare il loro percorso di guarigione, nonché su come affrontare le conversazioni difficili. Ciò garantirà un ambiente per le vittime che non le colpevolizzi o le umili, ma piuttosto le sostenga.

Infine, il reinserimento deve includere opportunità di empowerment, in cui i sopravvissuti siano incoraggiati a parlare della propria esperienza, poiché godono di maggiore fiducia da parte dei loro coetanei. Le vittime che diventano educatori, sostenitori o sostenitori tra pari spesso riferiscono un maggiore senso di controllo e di guarigione. Le piattaforme comunitarie dovrebbero anche consentire ai sopravvissuti di condividere le proprie storie in forma anonima tramite newsletter, forum pubblici o campagne di sensibilizzazione, trasformando il danno personale in protezione collettiva. Questo recupero partecipativo non solo avvantaggia l'individuo, ma rafforza anche la vigilanza collettiva contro le frodi.

In sintesi, il recupero autosostenuto non è un processo lineare ma circolare, che richiede un supporto emotivo continuo, una riabilitazione digitale strutturata, un solido coordinamento istituzionale e una partecipazione sociale significativa. Il ruolo dell'educatore in questo percorso è

sia facilitante che riparatrice, aiutando le vittime non solo ad andare oltre la truffa, ma anche a diventare persone più forti e resilienti.

2.10 Casi di studio pratici

Sulla base delle sezioni precedenti che delineano l'individuazione delle truffe, l'impatto psicologico, il ruolo dell'educatore e le strategie di intervento, vengono forniti i seguenti scenari pratici per aiutare educatori e operatori giovanili ad applicare i risultati di apprendimento chiave. Ogni caso rappresenta una situazione comune e reale ed è accompagnato da domande riflessive per valutare il giudizio, le strategie di comunicazione e la sensibilità etica.

2.10.1 Caso di studio 1:

Anna, 71 anni, è diventata molto attiva su Facebook negli ultimi mesi. Durante una pausa caffè al workshop del vostro centro comunitario, racconta con entusiasmo di aver incontrato "un vedovo meraviglioso". "Mi capisce davvero", dice, "è come se sapesse esattamente cosa provo". Aggiunge che potrebbe venire a trovarmi presto e, ultimamente, ha fatto domande sui servizi bancari internazionali.

Domande riflessive:
Quali segnali suggeriscono che Anna potrebbe essere a rischio?
Quali segnali specifici suggeriscono che Anna potrebbe essere vulnerabile a una truffa romantica?
Come affronteresti una conversazione non conflittuale e volta a costruire la fiducia per approfondire la conoscenza del truffatore senza provocare vergogna?
Quali strumenti educativi o strategie di discussione tra pari potresti utilizzare per aiutare Anna a riflettere criticamente sulla sua situazione?
Se Anna rimane irremovibile, come potresti costruire una rete di sicurezza senza privarla della sua autonomia?

2.10.2 Caso di studio 2:

Walter, 78 anni, ha recentemente iniziato a saltare le sessioni del tuo gruppo di discussione per anziani. Quando partecipa, siede in silenzio ed evita il contatto visivo. Noti che passa molto tempo a mandare messaggi, visibilmente ansioso. Un giorno, lo senti dire che sta inviando denaro per aiutare un "amico" conosciuto online a ottenere un passaporto per raggiungerlo in Germania.

Domande riflessive:

Quali segnali d'allarme comportamentali di Walter sono in linea con gli indicatori noti di coinvolgimento in truffe?

Come si potrebbe avviare un dialogo rispettoso, consapevole del trauma e che eviti di innescare atteggiamenti difensivi?

Quali risorse di supporto o partnership potresti attivare (ad esempio, assistenza legale, linee di assistenza per la lotta alle truffe)?

Come puoi preservare la dignità e l'autonomia di Walter incoraggiando al contempo azioni protettive?

2.10.3 Caso di studio 3:

Ricevi una telefonata da Lara, la figlia di Maria, una delle tue partecipanti di lunga data. Lara è sconvolta e preoccupata: "Mia madre ha appena mandato 5.000 euro a un uomo che non ha mai incontrato! Dice di essere nell'esercito e di essere bloccato all'estero. Lei pensa che siano innamorati: è una follia!" Lara è furiosa e insiste che sua madre sta facendo una sciocchezza. Vorrebbe che tu affrontassi Maria e la convincessi a smettere.

Domande riflessive:

Come ti rivolgeresti a Maria per preservare la sua fiducia e al contempo esprimere delicatamente le sue preoccupazioni?

Quali strategie di assistenza informata sul trauma potresti utilizzare per ridurre la vergogna e creare uno spazio sicuro per la rivelazione?

Come potresti coinvolgere Lara in modo solidale e non coercitivo, aiutandola a comprendere le dimensioni emotive di tali truffe?

Quale ruolo puoi svolgere nell'aiutare entrambe le parti a trovare un terreno comune per il recupero e la protezione futura?

Difesa digitale: nozioni di base sulla sicurezza informatica per principianti

Co-funded by
the European Union

Jim Boelhouwer

Sono un affermato Project Manager ed esperto IT, con una passione per l'apprendimento continuo e il raggiungimento di risultati eccellenti. Con una solida esperienza nella gestione di progetti complessi e una profonda conoscenza dei sistemi IT, Jim porta una vasta competenza in ogni progetto che intraprende.

Ho una comprovata esperienza nella gestione e realizzazione di progetti di alto profilo nel settore IT. La mia vasta esperienza abbraccia diversi ambiti, tra cui lo sviluppo software, l'implementazione di infrastrutture e l'integrazione di sistemi. La mia capacità di gestire efficacemente team interfunzionali e di allineare gli obiettivi di progetto con quelli organizzativi si è tradotta costantemente nel completamento dei progetti nei tempi previsti e nel rispetto del budget.

3 Nozioni di base sulla sicurezza informatica per principianti

3.1 Componenti chiave della consapevolezza della sicurezza

Nel capitolo precedente vengono spiegate le tattiche e i metodi utilizzati dai criminali per avvicinare le persone anziane vulnerabili e derubarle economicamente.

Uno degli aspetti di come queste tattiche e metodi vengono sfruttati è l'uso della comunicazione digitale. Siamo sempre più connessi tra loro grazie a un mondo digitalizzato. Ciò significa che le persone anziane vulnerabili devono essere consapevoli dei rischi che ciò comporta. Ricevere e-mail o avviare conversazioni in chat può essere l'inizio di un processo di sfruttamento finanziario.

La consapevolezza della sicurezza è la comprensione e il riconoscimento delle potenziali minacce alla sicurezza informatica e delle migliori pratiche per la protezione di informazioni e sistemi sensibili. Implica la formazione delle persone su vari aspetti della sicurezza informatica per ridurre il rischio di violazioni della sicurezza e perdita di dati. Gli elementi chiave della consapevolezza della sicurezza sono:

- Attacchi di phishing e come riconoscerli
- Sicurezza delle password e autenticazione avanzata
- Utilizzo sicuro dei supporti rimovibili
- Tattiche di ingegneria sociale
- Uso corretto dei social media e della posta elettronica
- Le migliori pratiche per la sicurezza nel cloud

3.2 Attacchi di phishing e come riconoscerli

- Gli attacchi di phishing sono tentativi fraudolenti di ottenere informazioni sensibili come nomi utente, password, dati di carte di credito o altre informazioni personali, spacciandosi per un'entità affidabile. Gli aggressori in genere utilizzano e-mail, messaggi di testo o siti web ingannevoli che sembrano legittimi per indurre i destinatari a rivelare i propri dati o a cliccare su link dannosi che portano all'installazione di malware. Ecco una panoramica dei tipi più comuni di attacchi di phishing e come identificarli.

Tipi di attacchi di phishing:
Email phishing: si tratta di una delle forme di phishing più diffuse. Gli aggressori utilizzano le email per impersonare organizzazioni o individui affidabili, con l'obiettivo di indurre i destinatari a condividere dati sensibili o a cliccare su link dannosi.

- Spear phishing: una versione più mirata del phishing che prevede l'invio di e-mail personalizzate a individui o organizzazioni specifici.

- Smishing (SMS Phishing): gli aggressori utilizzano messaggi di testo contenenti link o numeri di telefono dannosi per raccogliere informazioni personali o infettare i dispositivi con malware.

- Vishing (phishing vocale): si tratta di chiamate telefoniche per impersonare persone fidate. Grazie alla replica vocale basata sull'intelligenza artificiale, queste chiamate possono avere un suono estremamente realistico.

- Clone phishing: gli aggressori creano duplicati di email legittime, sostituendo i link originali con link dannosi.

- Pop-Up Phishing: pop-up dannosi sui siti web che possono innescare il download di malware o reindirizzare gli utenti a siti falsi.

- Evil Twin Phishing: gli aggressori creano falsi hotspot Wi-Fi per intercettare i dati degli utenti che vi si connettono.

Come identificare gli attacchi di phishing

Per identificarli, cercate informazioni insolite sul mittente, linguaggio urgente o minaccioso, richieste di informazioni personali, link e allegati sospetti e saluti generici. Prestate particolare attenzione alle email che sembrano troppo belle per essere vere, come le offerte di prodotti o servizi gratuiti.

Caratteristiche delle e-mail sospette:
- Richieste di informazioni sensibili (ad esempio, password, dettagli della carta di credito)
- Messaggi urgenti o allarmanti che creano un senso di panico
- Indirizzi email del mittente sconosciuti o leggermente modificati

- Errori di ortografia e grammatica
- Saluti generici invece di quelli personalizzati

Segnali di pericolo relativi a link e allegati:

- URL abbreviati o mascherati che nascondono la destinazione effettiva
- Testo del collegamento non corrispondente e URL effettivo (passa il mouse per controllare)
- Allegati indesiderati, in particolare da mittenti sconosciuti

Segnali di avvertimento sui contenuti:

- Offerte che sembrano troppo belle per essere vere (ad esempio, carte regalo gratuite)
- Avvisi o problemi imprevisti relativi all'account
- Richieste di verifica o aggiornamento delle informazioni dell'account tramite e-mail

Precauzioni tecniche:

- Verificare la presenza di HTTPS negli URL dei siti Web, in particolare per le transazioni sensibili
- Fai attenzione agli hotspot Wi-Fi duplicati nei luoghi pubblici
- Utilizzare i blocchi pop-up e fare attenzione alle richieste di notifica del browser

Rimanendo vigili e seguendo queste linee guida, è possibile ridurre significativamente il rischio di cadere vittima di attacchi di phishing. Ricordate, le organizzazioni legittime non chiederanno mai informazioni sensibili tramite e-mail o messaggi indesiderati.

3.3 Sicurezza delle password e autenticazione avanzata

La sicurezza delle password e l'autenticazione avanzata sono componenti cruciali della sicurezza informatica nel panorama digitale odierno. Per garantire la protezione degli account online e delle informazioni sensibili, è essenziale implementare solide misure di sicurezza.

3.3.1 Password complesse

Creare password complesse è la prima linea di difesa contro gli accessi non autorizzati. Una password complessa dovrebbe:

- Essere lungo almeno 10 caratteri
- Includi un mix di lettere maiuscole e minuscole, numeri e simboli

- Evita parole comuni o sequenze facilmente indovinabili

- Per creare una password complessa a partire da una frase, è possibile utilizzare diverse tecniche. Un metodo popolare prevede l'utilizzo della prima lettera di ogni parola della frase, eventualmente aggiungendo numeri o simboli, e assicurandosi che la password sia sufficientemente lunga.

Ecco una ripartizione dei metodi:

1. Acronimi:
Prendi la prima lettera di ogni parola della frase scelta.
Ad esempio, la frase "Il mio colore preferito è il blu" potrebbe diventare "Mfcib".
Per renderlo più incisivo, potresti aggiungere numeri o simboli, come "Mfcib12!".

2. Sostituzione:
Sostituisci le lettere con numeri o simboli simili (ad esempio, "a" con "@", "e" con "3").
Ad esempio, la frase "Amo i gatti" potrebbe diventare "1 l0v3 c@ts".

3. Errori di ortografia e uso delle maiuscole:
Scrivi deliberatamente parole sbagliate nella tua frase o scrivi alcune lettere in maiuscolo per creare una combinazione unica.
Ad esempio, "The quick brown fox" potrebbe diventare "Th3 q!ck br0wn f0x" o "ThE qUiCk bRoWn FoX".

- 4. Combinazione di tecniche:
- Per ottenere una password ancora più efficace, puoi combinare acronimi, sostituzioni, errori di ortografia e uso delle maiuscole.
- Ad esempio, usando la frase "Questo è un test" potresti diventare "T!s!s@t3s7t".

3.3.2 Best Practice per la gestione delle password

Le migliori pratiche per una politica di password sicura includono l'impostazione di una lunghezza minima della password, l'obbligo di utilizzare un mix di caratteri (maiuscole, minuscole, numeri, simboli) e l'incoraggiamento all'uso di passphrase o gestori di password. Per migliorare la sicurezza delle password:

- Utilizzare password univoche per ogni account
- Cambiare le password regolarmente, idealmente ogni 3 mesi
- Prendi in considerazione l'utilizzo di un gestore di password per archiviare e generare in modo sicuro password complesse
- Evitare di condividere password o di utilizzare informazioni facilmente indovinabili

3.3.3 Autenticazione a più fattori (MFA)

L'autenticazione forte va oltre le password, implementando l'autenticazione a più fattori. L'autenticazione a più fattori richiede almeno due componenti di identità per verificare l'identità di un utente. Questi componenti in genere includono:

-
- Qualcosa che l'utente conosce (ad esempio, password o PIN)
- Qualcosa che l'utente possiede (ad esempio, uno smartphone o un token hardware)
- Qualcosa che l'utente è (ad esempio, dati biometrici come impronte digitali o riconoscimento facciale)

L'abilitazione dell'MFA su tutti gli account, ove possibile, aumenta significativamente la sicurezza aggiungendo un ulteriore livello di protezione.

3.3.4 Tecniche di autenticazione forte

L'autenticazione forte mira a verificare in modo affidabile l'identità degli utenti e a impedire accessi non autorizzati. Alcuni aspetti chiave dell'autenticazione forte includono:

-
- Non fare affidamento esclusivamente su segreti condivisi o chiavi simmetriche
- Respingere i tentativi di phishing e di impersonificazione delle credenziali
- Utilizzo di token crittografici basati su hardware, come chiavi FIDO o smart card, per il massimo livello di sicurezza

3.3.5 Vantaggi dell'autenticazione forte

L'implementazione di pratiche di autenticazione avanzate offre diversi vantaggi:

- Protezione avanzata contro il furto di credenziali e l'accesso non autorizzato

- Rischio ridotto di attacchi di phishing riusciti
- Maggiore conformità ai requisiti normativi
- Maggiore fiducia nelle identità degli utenti e nella sicurezza complessiva del sistema

Combinando password complesse con l'autenticazione a più fattori e seguendo le best practice, puoi migliorare significativamente la tua sicurezza informatica e proteggere le informazioni sensibili da potenziali minacce.

3.4 Utilizzo sicuro dei supporti rimovibili

L'uso di dispositivi multimediali rimovibili come chiavette USB, dischi rigidi esterni, schede SD, ecc. è diventato diffuso grazie alle loro dimensioni compatte e all'elevata capacità di archiviazione. Tuttavia, queste stesse caratteristiche che li rendono facili da usare li rendono anche obiettivi interessanti per i criminali informatici che cercano di rubare informazioni sensibili.

Secondo uno studio di IBM Security, l'errore umano è responsabile di oltre il 90% degli incidenti di sicurezza che coinvolgono dispositivi multimediali rimovibili. Errori comuni come lo smarrimento o la perdita di questi dispositivi possono portare ad accessi non autorizzati o al furto di dati riservati.

Inoltre, attacchi dannosi come infezioni da malware tramite USB infette stanno diventando sempre più comuni.

Secondo Astra Security e DeepStrike, ogni giorno vengono rilevati circa 560.000 nuovi malware. Questa cifra rappresenta un volume significativo, che si aggiunge al già vasto numero di programmi malware esistenti, che supera il miliardo.

Per garantire un utilizzo sicuro dei supporti rimovibili, seguire queste buone pratiche:

Utilizzare solo dispositivi attendibili:

- Non collegare mai al computer supporti rimovibili trovati o sconosciuti.

1. Implementare misure di sicurezza:

- Installare e mantenere aggiornato un software antivirus che esegua la scansione attiva dei supporti rimovibili quando vengono connessi.

- Disattiva le funzioni di esecuzione automatica e riproduzione automatica sul tuo computer per impedire l'esecuzione automatica di codice dannoso.
- Crittografare tutti i dispositivi multimediali rimovibili per proteggere i dati in caso di smarrimento o furto.

Applicare una protezione con password complessa ai dispositivi multimediali rimovibili.

- 3. Gestire i dati correttamente:
- Mantieni separati i dati personali da quelli di lavoro.
- Elimina in modo sicuro i dati sensibili dai supporti rimovibili dopo l'uso.
- Limitare l'uso dei supporti rimovibili solo quando necessario e autorizzato.
- 4. Mantenere la sicurezza fisica:
- Non lasciare mai incustoditi i supporti rimovibili; conservarli in un luogo sicuro quando non vengono utilizzati.
- Disattivare i servizi wireless non necessari come Bluetooth e Wi-Fi sui dispositivi.
- 5. Manutenzione ordinaria:
- Eseguire scansioni di routine dei supporti rimovibili per rilevare eventuali malware.
- Eseguire controlli regolari e monitorare l'utilizzo dei supporti rimovibili per rilevare attività sospette.

Seguendo queste linee guida, è possibile ridurre significativamente i rischi associati all'utilizzo di supporti rimovibili, continuando a beneficiare della loro praticità e portabilità.

3.5 Tattiche di ingegneria sociale

L'ingegneria sociale è la manipolazione psicologica delle persone per ottenere l'accesso a informazioni riservate o per indurle a compiere azioni che potrebbero non essere nel loro interesse. Oltre alle tattiche di phishing già menzionate, esistono anche le seguenti tattiche:

Baiting: offrire qualcosa di allettante (come software gratuito) che contiene malware o compromette la sicurezza quando vi si accede.
Quid pro quo: promettere un vantaggio in cambio di informazioni o azioni, come offrire supporto IT gratuito che installa malware.
Scareware: utilizzo di tattiche basate sulla paura per manipolare le vittime e indurle ad agire, ad esempio falsi avvisi di virus.
Attacchi watering hole: compromissione dei siti web visitati frequentemente dal bersaglio per diffondere malware.

Nei prossimi due paragrafi approfondiremo due noti tipi di ingegneria sociale: la truffa romantica e la truffa della macellazione del maiale.

3.5.1 truffa romantica

Una truffa sentimentale è una truffa che consiste nel fingere intenzioni romantiche nei confronti di una vittima, conquistarne l'affetto e poi usare tale benevolenza per indurla a inviare denaro al truffatore sotto falsa apparenza o a commettere frodi ai suoi danni. Le frodi possono comportare l'accesso al denaro, ai conti bancari, alle carte di credito, ai passaporti, agli account di posta elettronica o ai numeri di identificazione nazionale della vittima, oppure costringere le vittime a commettere frodi finanziarie per loro conto. Queste truffe sono spesso perpetrate dalla fabbrica delle frodi gestita da bande criminali organizzate che collaborano per sottrarre denaro a più vittime contemporaneamente. Le truffe del macello di maiali (PBS o PB Scam) sono un tipo di truffa sentimentale sempre più diffuso e diffuso, che di solito include anche la truffa dei programmi di investimento ad alto rendimento (HYIP). Discuteremo di questo tipo di truffa in un paragrafo separato.

Immagini rubate

I truffatori sentimentali creano profili personali utilizzando fotografie rubate di persone attraenti allo scopo di chiedere ad altri di contattarli. Questo è spesso noto come catfishing. Spesso vengono utilizzate foto di attrici o modelle sconosciute per indurre la vittima a credere di stare parlando con quella persona. Anche i membri dell'esercito statunitense vengono impersonati, poiché fingere di prestare servizio nell'esercito spiega perché il truffatore non è disponibile per un incontro di persona.

Poiché i truffatori spesso non assomigliano per niente alle foto che inviano alle vittime, raramente incontrano le vittime di persona o addirittura tramite videochiamata. Ingannano le loro vittime prescelte inventando scuse plausibili sulla loro riluttanza a mostrarsi, ad esempio dicendo che non possono ancora incontrarsi perché sono temporaneamente in viaggio o hanno una webcam rotta.

Ingannare la vittima

I truffatori sono molto abili nel "giocare" con le loro vittime: inviano poesie d'amore, giochi sessuali via e-mail, costruiscono una "relazione amorosa" con tante promesse del tipo "un giorno ci sposeremo". I truffatori pongono molte domande alle loro vittime, ma rivelano poco di sé.

Spesso ricoprono di complimenti le vittime.
Le comunicazioni tra il truffatore e la vittima si susseguono per un certo periodo, a volte mesi o addirittura un anno intero, finché il truffatore non ritiene di aver instaurato un legame sufficiente con la vittima da richiedere denaro. I truffatori sfruttano il falso senso di relazione delle vittime per convincerle a inviare denaro.
Queste richieste possono riguardare la benzina, biglietti dell'autobus o dell'aereo per andare a trovare la vittima, spese mediche o scolastiche. Di solito c'è la promessa che un giorno il truffatore raggiungerà la vittima a casa sua.

Le vittime possono essere invitate a recarsi nel paese del truffatore; in alcuni casi, le vittime arrivano con i soldi richiesti come regalo per i familiari o con tangenti da parte di funzionari corrotti, solo per essere picchiate, derubate o uccise.
La truffa di solito termina quando la vittima si rende conto di essere stata truffata o smette di inviare denaro. Tuttavia, le persone sono spesso lente a credere alla realtà e lo stigma di cadere in tale inganno può dissuaderle dal denunciare la frode alla polizia. Molte vittime, anche di fronte a prove concrete, non riescono a credere che la persona che sembra così amorevole nei messaggi di testo sia in realtà un truffatore criminale. Possono reagire con rabbia o violenza contro chiunque si opponga. Le banche possono bloccare il denaro della vittima, soprattutto quando si sospetta un abuso finanziario ai danni di un anziano.

✦ gruppi criminali

Le reti criminali truffano persone sole in tutto il mondo con false promesse di amore e romanticismo. I truffatori pubblicano profili su siti di incontri, account di social media non dedicati agli incontri, siti di annunci e persino forum online per cercare nuove vittime. Il truffatore di solito cerca di ottenere un metodo di comunicazione più riservato, come un'e-mail o un numero di telefono, per creare un rapporto di fiducia con la vittima.

Poiché i truffatori lavorano in gruppo, qualcuno del gruppo può essere online e disponibile a inviare e-mail o messaggi di testo alla vittima a qualsiasi ora. La rotazione tra diversi truffatori, che affermano tutti di essere la stessa persona, è difficile da rilevare nelle truffe basate su testo, mentre sarebbe ovvio se si presentasse una persona diversa a un incontro di persona o a una videochiamata o telefonata.

3.5.2 Truffa della macellazione dei maiali:

Le truffe legate alla macellazione dei maiali hanno avuto origine nel 2016 o prima come truffa regionale in Cina, inizialmente trovando le loro vittime su siti di incontri per persone dello stesso sesso, prima di espandersi anche a siti di incontri per persone del sesso opposto. Il termine "macellazione dei maiali" deriva da un'analogia che paragona la fase iniziale di conquista della fiducia delle vittime all'ingrasso dei maiali prima della macellazione.

Il modus operandi si è poi diffuso in tutto il sud-est asiatico al culmine della pandemia di Covid. In Cambogia, un tempo prospera città del gioco d'azzardo, molte bande locali di giocatori d'azzardo hanno trasformato i casinò in centri operativi di truffe, mettendo in atto truffe di macellazione di maiali. Ciò è stato probabilmente dovuto alla mancanza di frequentazione dei casinò a causa della pandemia di Covid e alla repressione del gioco d'azzardo commerciale da parte del governo cambogiano. Molte operazioni sono gestite anche da aree del Myanmar che sono fuori dal controllo del governo centrale a causa della guerra civile, con un importante snodo nella città di Myawaddy, vicino al confine con la Thailandia. Secondo l'Ufficio delle Nazioni Unite per i Diritti Umani, centinaia di migliaia di persone sono state vittime di tratta e sono intrappolate in centri di truffe in Cambogia e Myanmar, mentre altre operazioni sono gestite da Laos, Filippine e Thailandia. Molti dei gruppi che gestiscono truffe di macellazione di maiali sono organizzazioni criminali cinesi all'estero con sede nel sud-est asiatico, che trafficano persone di etnia cinese e di altre etnie in fabbriche di frodi e costringono queste persone a commettere frodi.

Le truffe legate alla macellazione dei maiali hanno acquisito popolarità a livello internazionale grazie allo sfruttamento delle app di incontri online e delle piattaforme di social media. I truffatori creavano elaborate identità false per stabilire legami sentimentali o emotivi con le vittime, segnando così un distacco dalle truffe finanziarie convenzionali, integrando la manipolazione psicologica. Questa fase iniziale di queste truffe prendeva di mira principalmente le popolazioni locali, ma si è rapidamente espansa con la crescita della connettività digitale.

Le truffe si sono evolute in modo significativo con l'integrazione di tecniche sofisticate, tra cui la creazione di false piattaforme di investimento online e l'uso dell'ingegneria sociale.

Con l'uso più diffuso di piattaforme come WhatsApp e Telegram, persone casuali possono essere prese di mira semplicemente avviando una conversazione involontaria. Un aspetto chiave di questa evoluzione è stato l'uso delle criptovalute per le transazioni, che hanno attirato i truffatori per la loro difficoltà di tracciamento e recupero. La globalizzazione delle truffe può essere attribuita alla crescente ubiquità delle interazioni digitali e alla crescente popolarità delle criptovalute, che hanno aperto una nuova strada per tali attività fraudolente su scala globale.

Gruppi criminali

Le truffe che coinvolgono la macellazione dei maiali prevedono una serie di passaggi meticolosamente pianificati per ingannare e sfruttare le vittime, concentrandosi solitamente su frodi relative agli investimenti in criptovalute.

Guadagnare fiducia: le truffe spesso iniziano con conversazioni informali avviate dal truffatore, che può fingere di aver ricevuto i dati di contatto della vittima accidentalmente o tramite un conoscente comune. Queste interazioni iniziali sono progettate per creare fiducia e possono comportare l'uso di immagini del profilo accattivanti per adescare le vittime.
Presentazione dell'investimento: una volta instaurato un rapporto di fiducia, il truffatore presenta alla vittima un sistema di investimento fraudolento, promettendo rendimenti significativi in un breve periodo. I truffatori utilizzano tattiche persuasive e portafogli di investimento contraffatti per convincere le vittime della legittimità del sistema.
Raccolta di denaro: dopo aver convinto la vittima a investire, i truffatori raccolgono fondi, spesso tramite piattaforme di pagamento digitali o criptovalute, per complicare il monitoraggio e la rintracciabilità delle transazioni.
Scomparsa del truffatore: una volta che è stata raccolta una somma considerevole o quando le vittime tentano di prelevare i fondi, i truffatori diventano irraggiungibili, eliminano la loro presenza online o creano nuove identità, lasciando le vittime senza modo di recuperare i loro fondi.

Inoltre, i truffatori sviluppano falsi siti web di intermediazione e applicazioni mobili per dare legittimità al loro schema, rendendo difficile per le vittime distinguerli dalle piattaforme autentiche.

3.6 Uso corretto dei social media e della posta elettronica

I social media, ovviamente, non sono poi così negativi. Spesso, il loro utilizzo comporta benefici tangibili. Molti di noi accedono ai social media per un senso di appartenenza, per esprimere se stessi, per curiosità o per il desiderio di connettersi. App come Facebook, Instagram, WhatsApp, Telegram e Twitter ci permettono di rimanere in contatto con familiari e amici geograficamente distanti, di comunicare con persone che condividono i nostri stessi interessi e di unirci a una comunità online per sostenere cause che ci stanno a cuore.

Ognuno di noi deve prendere le proprie decisioni individuali sull'uso dei social media, basandosi sulla propria esperienza personale. Basandosi sulla ricerca, ci aiuta a soppesare il bene e il male e a prendere le decisioni appropriate. Anche se il genio è uscito dalla lampada, potremmo scoprire, come affermano Shakya e Christakis, che "le interazioni sociali online non sostituiscono quelle reali" e che le relazioni sane e di persona sono vitali per la società e per il nostro benessere individuale. Faremmo bene a ricordare questa verità e a non puntare tutto sui social media.

Linee guida generali:

- Mantenere la privacy rivedendo regolarmente le impostazioni
- Pensa prima di pubblicare: i contenuti possono rimanere online indefinitamente
- Siate rispettosi e premurosi in tutte le interazioni
- Verificare le informazioni prima di condividerle per evitare di diffondere disinformazione
- Ricorda che la tua impronta digitale influenza la tua reputazione personale e professionale

Consapevolezza della sicurezza:

- Fai attenzione ai link e agli allegati
- Verificare gli indirizzi dei mittenti prima di rispondere alle email sospette
- Non condividere mai informazioni sensibili a meno che tu non sia certo della sicurezza
- Utilizzare la crittografia per le comunicazioni sensibili
- Utilizzare password complesse e univoche e abilitare l'autenticazione a due fattori

3.7 L'introduzione dell'intelligenza artificiale (IA)

L'intelligenza artificiale (IA) si riferisce allo sviluppo di sistemi informatici in grado di svolgere compiti che in genere richiedono l'intelligenza umana. Questi compiti includono l'apprendimento, Risoluzione dei problemi, processo decisionale e comprensione del linguaggio naturale.

L'intelligenza artificiale comprende un'ampia gamma di tecniche e approcci, dai semplici sistemi basati su regole ai complessi modelli di apprendimento automatico. Ecco un'analisi più dettagliata dei concetti chiave:

Imitare l'intelligenza umana: l'intelligenza artificiale mira a creare macchine in grado di svolgere compiti che gli esseri umani solitamente svolgono utilizzando la loro intelligenza.
Apprendimento e risoluzione dei problemi: i sistemi di intelligenza artificiale possono imparare dai dati, identificare modelli e prendere decisioni basate su tale apprendimento.
Applicazioni diversificate: l'intelligenza artificiale viene utilizzata in vari settori, tra cui sanità, finanza, istruzione e trasporti.
Apprendimento automatico: componente fondamentale dell'intelligenza artificiale moderna, in cui gli algoritmi apprendono dai dati senza una programmazione esplicita.
Elaborazione del linguaggio naturale: consente alle macchine di comprendere e interagire con il linguaggio umano.
Visione artificiale: consente alle macchine di "vedere" e interpretare immagini e video.

Esempi di utilizzo dell'IA:
Assistenti vocali: come Siri o Alexa, che comprendono e rispondono ai comandi vocali.
Sistemi di raccomandazione: utilizzati dalle piattaforme online per suggerire prodotti o contenuti in base alle preferenze degli utenti.

- Auto a guida autonoma: utilizzo dell'intelligenza artificiale per la navigazione e il processo decisionale nei veicoli autonomi.
- Rilevamento delle frodi: utilizzo dell'intelligenza artificiale per identificare transazioni sospette nei sistemi finanziari.

- In sostanza, l'intelligenza artificiale è un campo in rapida evoluzione con il potenziale di trasformare diversi aspetti della nostra vita. Gli stessi principi si applicano alle truffe sentimentali, in cui personaggi generati dall'intelligenza artificiale che si spacciano per amici, familiari o colleghi del truffatore interagiscono con la vittima per convalidare la relazione e fugare i suoi dubbi. Queste interazioni simulano la riprova sociale, rendendo più difficile per le vittime mettere in discussione le incongruenze.

3.7.1 Contatto iniziale

La credibilità del profilo di un truffatore è fondamentale nelle fasi iniziali di una frode sentimentale, poiché aiuta a determinare se una vittima interagisce con un personaggio falso. Mentre i truffatori tradizionalmente rubavano immagini di utenti reali, la ricerca inversa di immagini e l'analisi forense delle foto potrebbero essere utilizzate per smascherare questi inganni. Tuttavia, grazie all'integrazione di LLM e alla generazione di immagini deepfake, i truffatori possono ora facilmente produrre in serie personaggi sintetici che imitano fedelmente gli utenti reali. Questi profili sono progettati per aggirare i meccanismi di rilevamento sui social media, sulle piattaforme di incontri e sui network professionali, ingannando efficacemente le vittime.

La portata della creazione di profili basata sull'intelligenza artificiale è enorme. Ad esempio, Meta avrebbe rimosso miliardi di account falsi nel 2024 (inclusi tutti gli account che l'azienda riteneva fossero stati creati con intenti malevoli o per entità non umane). L'aumento dei profili fraudolenti generati dall'intelligenza artificiale ha costretto la piattaforma di incontri Tinder ad ampliare il suo programma di verifica dell'identità nel 2024, implementando misure potenziate negli Stati Uniti e nel Regno Unito. Queste misure richiedono agli utenti di inviare documenti d'identità rilasciati dal governo e video autoregistrati. Tuttavia, potrebbero non essere sufficienti per affrontare la crescente sofisticazione dell'intelligenza artificiale generativa, con la tecnologia che pone sfide ai controlli KYC e ad altri processi di verifica dell'identità.

I profili generati dall'intelligenza artificiale non operano in modo isolato. I truffatori possono combinare profili sintetici con attività di outreach automatizzate, creando pipeline ad alto volume in cui migliaia di profili realistici distribuiscono simultaneamente messaggi generati da LLM. Come discusso nella sezione precedente, è probabile che i truffatori sfruttino gli LLM nella fase di outreach iniziale piuttosto che nelle interazioni successive. Questo perché:

Il primo messaggio richiede una personalizzazione minima, il che lo rende facile da generare su larga scala.
L'invio di messaggi introduttivi è un'attività altamente ripetitiva, per cui l'automazione è una priorità assoluta per i truffatori che cercano di aumentare l'efficienza.
Gli LLM danno il massimo in scenari strutturati e poco contestualizzati, il che li rende particolarmente adatti a questa fase.

Ciò significa che l'intelligenza artificiale è già ben posizionata per migliorare la scalabilità iniziale delle truffe sentimentali. I truffatori possono implementare la tecnologia su più piattaforme, basandosi sui messaggi generati da LLM per avviare conversazioni in modo efficiente.

Una volta che la vittima interagisce, i truffatori possono quindi passare all'intervento manuale o a interazioni raffinate assistite dall'intelligenza artificiale per sostenere l'inganno.

Man mano che i profili generati dall'intelligenza artificiale e le attività di sensibilizzazione diventano più sofisticati, i metodi di rilevamento tradizionali, come la verifica del profilo e il rilevamento delle anomalie basato sul testo, potrebbero avere difficoltà a tenere il passo, rendendo necessarie contromisure adattive.

3.7.2 Costruzione di relazioni

Una volta stabilito il contatto iniziale, i truffatori passano alla fase di costruzione della relazione, in cui cercano di approfondire il coinvolgimento emotivo e instaurare un rapporto di fiducia con le loro vittime. Gli strumenti basati sull'intelligenza artificiale hanno migliorato la capacità dei truffatori di scalare e personalizzare l'inganno, ma hanno solo una capacità limitata di automatizzare questa fase. A differenza del contatto iniziale, che trae vantaggio da script generici e automazione su larga scala, la costruzione della relazione richiede adattabilità, intelligenza emotiva e risposte personalizzate alle interazioni con le vittime.

Una distinzione fondamentale tra l'inganno guidato dall'intelligenza artificiale e quello guidato dall'uomo è l'adattabilità. I truffatori umani possono adattare dinamicamente le loro narrazioni in base alle risposte delle vittime, garantendo che le conversazioni rimangano emotivamente coinvolgenti e procedano verso lo sfruttamento finanziario. Sebbene gli LLM possano generare messaggi truffaldini proceduralmente accurati, faticano a mantenere continuità e una personalizzazione approfondita nelle interazioni prolungate. Senza la supervisione umana, i messaggi generati dall'intelligenza artificiale rischiano di presentare incoerenze di tono, contraddizioni e frasi ripetitive, che possono indebolirne la credibilità nel tempo. L'Ufficio delle Nazioni Unite contro la droga e il crimine[29] segnala che, sebbene l'intelligenza artificiale sia già utilizzata nei crimini informatici, la maggior parte delle truffe si basa ancora sulla supervisione umana per mantenere la credibilità e gestire complesse dinamiche interpersonali.

Tuttavia, l'intelligenza artificiale può migliorare questa fase in diversi modi:

Ottimizzazione degli script truffa: i truffatori possono utilizzare gli LLM per perfezionare gli script truffa, testando diverse formulazioni e richiami emotivi per massimizzare il coinvolgimento.

Assistenza chat multilingue: la traduzione consente ai truffatori di interagire con le vittime in più lingue con maggiore fluidità.
Gestione automatizzata delle relazioni: gli strumenti di intelligenza artificiale possono aiutare i truffatori a gestire più vittime contemporaneamente, fornendo risposte suggerite e strategie di coinvolgimento, riducendo al minimo le incongruenze tra le conversazioni.

Mentre il testo generato da LLM facilita un coinvolgimento scalabile e personalizzato, i media deepfake forniscono un ulteriore livello di autenticità, rendendo i profili fraudolenti più convincenti e sempre più difficili da verificare. Gli strumenti di clonazione vocale basati sull'intelligenza artificiale consentono ai truffatori di generare contenuti che imitano schemi di linguaggio, accenti e inflessioni emotive, riducendo la necessità di un'interazione umana diretta. Allo stesso modo, i truffatori possono utilizzare video generati dall'intelligenza artificiale per fabbricare una prova visiva dell'identità, consentendo loro di aggirare le richieste di verifica e rafforzare la fiducia delle potenziali vittime. Sebbene le interazioni deepfake completamente autonome rimangano tecnicamente complesse, i truffatori sfruttano già contenuti video sintetici preregistrati, che consentono loro di mantenere un inganno più a lungo.

Casi recenti di alto profilo evidenziano il crescente impatto delle truffe basate sui deepfake. Un'azienda di ingegneria britannica ha segnalato nel gennaio 2024 che alcuni criminali hanno utilizzato un video deepfake per impersonare con successo dirigenti senior, facilitando una frode aziendale da 25 milioni di dollari. Nell'ottobre 2024, alcuni truffatori sentimentali hanno utilizzato immagini generate da deepfake per ingannare le vittime, facendole credere di essere in una relazione autentica, estorcendo loro 46 milioni di dollari. Sebbene i casi più recenti si siano concentrati sul ruolo dei deepfake nelle truffe sentimentali, le tattiche sottostanti si stanno espandendo ad altri settori, tra cui le frodi sugli investimenti.

I progressi nella tecnologia di inpainting dell'IA, che integra perfettamente i contenuti generati in immagini o video esistenti, hanno ulteriormente migliorato il realismo di questi materiali ingannevoli, rendendone sempre più difficile il rilevamento sia per gli esseri umani che per i sistemi automatizzati. Con lo sviluppo di nuove capacità dell'IA, è probabile che il suo ruolo nella costruzione di relazioni fraudolente si evolva, combinando l'inganno automatizzato con la supervisione umana strategica per massimizzare l'efficacia delle truffe.

3.7.3 Manipolazione

Con l'approfondirsi di una relazione, i truffatori passano dalla generica costruzione della fiducia alla manipolazione psicologica altamente mirata. Questa fase, comunemente nota come adescamento, comporta l'intensificazione della dipendenza emotiva e l'isolamento della vittima da influenze esterne per aumentarne la vulnerabilità allo sfruttamento finanziario o personale. L'intelligenza artificiale migliora e personalizza questo processo analizzando il comportamento online della vittima, monitorandone lo stato emotivo e adattandone i modelli di comunicazione, potenzialmente in tempo reale. Automatizzando queste tecniche manipolative, l'intelligenza artificiale consente ai truffatori di ottimizzare l'inganno su larga scala, rendendo le loro tattiche più sofisticate ed efficienti, nonché più difficili da individuare.

I sistemi basati sull'intelligenza artificiale possono raccogliere e analizzare rapidamente dati da molteplici fonti, inclusi social media e registri pubblici, per creare un profilo psicologico completo delle potenziali vittime. Tradizionalmente, tale profilazione richiedeva un notevole impegno manuale, ma l'intelligenza artificiale può automatizzare e perfezionare questo processo in pochi secondi, consentendo ai truffatori di identificare e dare priorità a obiettivi altamente vulnerabili. La profilazione basata sull'intelligenza artificiale è ampiamente documentata nell'ingegneria sociale, in particolare negli attacchi di spear phishing, che personalizzano i messaggi per sfruttare le paure, i desideri o le insicurezze degli individui.

I truffatori possono estendere questa profilazione basata sull'intelligenza artificiale all'analisi comportamentale in tempo reale, monitorando le risposte, i modelli di coinvolgimento e gli stimoli emotivi della vittima. Elaborando le conversazioni in corso, l'intelligenza artificiale può aiutare i truffatori ad adattare dinamicamente tono, tempi e messaggi per creare l'illusione di una connessione autentica. Ciò consente un graduale ma altamente calcolato approfondimento della dipendenza emotiva dalla personalità inventata dal truffatore.

La capacità dell'IA di creare ambienti online immersivi rafforza ulteriormente il processo di adescamento, rafforzando l'identità fittizia del truffatore e riducendo lo scetticismo delle vittime al riguardo. La ricerca sulla persuasione politica e di marketing basata sull'IA ha dimostrato che i modelli possono mirare a singoli individui con messaggi personalizzati, aumentando così il loro coinvolgimento e plasmando le loro convinzioni. Gli stessi principi si applicano alle truffe sentimentali, in cui personaggi generati dall'IA che si spacciano per amici, familiari o colleghi del truffatore interagiscono con la vittima per convalidare la relazione e dissipare i suoi dubbi. Queste interazioni simulano la riprova sociale, rendendo più difficile per le vittime mettere in discussione le incongruenze.

Inoltre, il tipo di creazione di contenuti basata sull'intelligenza artificiale e l'amplificazione guidata dai bot spesso

Le truffe osservate nelle campagne di influenza politica possono inondare gli spazi online di narrazioni di rinforzo. Questo fa sì che, quando una vittima cerca il nome del proprio partner, trovi testimonianze inventate, profili falsi o articoli generati dall'intelligenza artificiale che rafforzano la credibilità della truffa. Proprio come i personaggi pubblici possono usare l'intelligenza artificiale per orientare il discorso pubblico e rafforzare le narrazioni politiche, i truffatori possono sfruttarla per creare una rete digitale artificiale che isola la vittima.

3.7.4 Esecuzione

Con l'aumentare della fiducia, i truffatori passano dalla manipolazione emotiva allo sfruttamento finanziario, sfruttando l'attaccamento della vittima per giustificare le richieste di pagamento. Questa fase spesso comporta crisi inventate come emergenze mediche, complicazioni logistiche o problemi legali, tutte progettate per creare urgenza e spingere la vittima a inviare denaro. Le carte regalo rimangono un metodo comune di estorsione finanziaria, presenti nel 24% dei casi di truffe sentimentali segnalati, ma criptovalute e bonifici bancari comportano perdite significativamente più elevate per vittima. I rapporti indicano che le perdite derivanti da truffe sentimentali sono aumentate negli ultimi anni, costando al pubblico del Regno Unito oltre 80 milioni di sterline all'anno. In Australia, le perdite segnalate hanno superato i 23 milioni di dollari australiani nel 2024, con l'intelligenza artificiale che ha svolto un ruolo significativo in questo aumento.

Oltre a tempi e dimensioni, l'IA aiuta i truffatori a mettere in atto sofisticati inganni, a falsificare la legittimità finanziaria e a semplificare il riciclaggio di denaro, rendendo l'estrazione finanziaria più subdola ed efficace. Uno sviluppo preoccupante riguarda la capacità dell'IA di falsificare la credibilità finanziaria. Come molti altri criminali, i truffatori sentimentali utilizzano società fittizie per nascondere i loro guadagni illeciti. I truffatori ora utilizzano l'IA generativa per falsificare bilanci, documenti legali e identità sintetiche convincenti per aggirare i controlli degli istituti finanziari. Come discusso, i criminali utilizzano sempre più identità sintetiche generate dall'IA per aggirare la verifica KYC, consentendo loro di aprire conti bancari fraudolenti e facilitare il riciclaggio di denaro su larga scala. Le loro identità generate dall'IA possono infiltrarsi nelle reti finanziarie legittime in modi che i sistemi tradizionali di monitoraggio delle frodi faticano sempre di più a rilevare.

L'intelligenza artificiale sta inoltre svolgendo un ruolo fondamentale nell'aumento delle truffe della "macellazione dei maiali", una delle più

Forme redditizie di estrazione finanziaria nelle frodi sentimentali. In questi schemi, i truffatori adescano le vittime per settimane o mesi prima di introdurle a false piattaforme di criptovalute o di investimento, sulle quali vengono ingannate per effettuare depositi sempre più ingenti. I truffatori aumentano la credibilità e il realismo di questi falsi siti di investimento non solo copiando il codice da piattaforme di investimento reali, ma anche utilizzando l'intelligenza artificiale per generare contenuti per loro. Impiegano anche chatbot basati sull'intelligenza artificiale come falsi consulenti finanziari per guidare le vittime attraverso la piattaforma, assicurandosi che anche gli utenti scettici si sentano rassicurati da tendenze di mercato inventate e da una guida personalizzata. Questi chatbot intrappolano ulteriormente le vittime incorporando link dannosi nelle loro comunicazioni, indirizzandole verso altri schemi fraudolenti e aggravando le loro perdite finanziarie.

Si stima che i ricavi derivanti dalle truffe legate alle criptovalute abbiano raggiunto i 12,4 miliardi di dollari negli Stati Uniti nel 2024, con le truffe legate alla macellazione dei maiali che hanno rappresentato una quota significativa di queste perdite. Nel frattempo, gli strumenti di programmazione assistiti dall'intelligenza artificiale hanno ridotto le competenze tecniche necessarie per lanciare false piattaforme di investimento, consentendo ai truffatori di produrre in serie siti fraudolenti con il minimo sforzo.

Mentre l'intelligenza artificiale continua ad automatizzare l'inganno e a semplificare le operazioni fraudolente, le truffe legate alla macellazione dei maiali si intrecciano sempre più con le truffe sentimentali. La capacità di creare truffe di investimento iper-personalizzate e guidate dall'intelligenza artificiale rende questi schemi ancora più insidiosi, danneggiando le vittime sia finanziariamente che psicologicamente.

3.7.5 Uscita o escalation

Quando le truffe sentimentali raggiungono la fase finale, i truffatori o spariscono improvvisamente dopo aver estorto denaro alle vittime, oppure intensificano i loro inganni per ottenere ancora di più. L'intelligenza artificiale consente strategie di uscita sempre più complesse, prolungando lo sfruttamento delle vittime attraverso tecniche come il ricatto deepfake e le truffe di impersonificazione.

Come ha recentemente riportato la Federal Trade Commission, una tattica in crescita prevede l'uso dell'intelligenza artificiale per impersonare le forze dell'ordine o i servizi di recupero crediti. In questo tipo di truffa, i truffatori contattano le vittime con false promesse di risarcimento finanziario, fingendosi agenti di polizia, autorità di regolamentazione finanziaria o investigatori, sostenendo di poter recuperare i fondi persi dietro pagamento.

3.8 Caso di studio sulla truffa sentimentale di Sarah Thompson

Sfondo

Sarah Thompson, una vedova di 58 anni di Portland, Oregon, ha perso il marito per un cancro nel 2022. Dopo un anno di lutto, i suoi figli adulti l'hanno incoraggiata a provare gli incontri online come un modo per riallacciare i rapporti sociali. Con un'esperienza limitata nel mondo degli incontri nell'era digitale, Sarah ha creato un profilo su un popolare sito di incontri nel marzo 2023.

Contatto iniziale

Entro due settimane dall'iscrizione alla piattaforma, Sarah ricevette un messaggio da "William Pierce", che sosteneva di essere un ingegnere civile americano di 62 anni impegnato in un contratto in Malesia. Il suo profilo mostrava le foto di un uomo attraente, dai capelli argentati e dal sorriso caloroso. William dichiarava di essere anche lui vedovo e in cerca di compagnia.

Le loro conversazioni si spostarono rapidamente dalla piattaforma di incontri alle email e a WhatsApp, il che avrebbe dovuto essere il primo campanello d'allarme. William era attento, romantico e sembrava profondamente interessato alla vita di Sarah. Comunicavano quotidianamente tramite messaggi e occasionali chiamate vocali, anche se William trovava sempre delle scuse per giustificare l'impossibilità di effettuare videochiamate: scarsa connessione internet, impegni di lavoro intensi o differenze di fuso orario.

Sviluppo delle relazioni

Nei due mesi successivi, William ha costruito un legame emotivo con Sarah attraverso:
Messaggi quotidiani di buongiorno e buonanotte
Condividendo storie personali sulla moglie e i figli defunti
Discutere i piani futuri per incontrarsi e possibilmente costruire una vita insieme
Inviare regali occasionali (fiori, cioccolatini) a casa di Sarah
Esprimere sentimenti romantici profondi in tempi relativamente rapidi

Le richieste finanziarie

Dopo circa tre mesi dall'inizio della loro relazione, William iniziò a fare richieste finanziarie:

Richiesta iniziale: William sosteneva che il suo progetto fosse stato ritardato a causa di un guasto all'attrezzatura. Aveva bisogno di 3.000 dollari per sostituire dei pezzi e non poteva accedere ai suoi fondi a causa di "problemi bancari all'estero". Sarah, preoccupata per la sua situazione, gli inviò il denaro tramite bonifico bancario.
Escalation: Dopo aver espresso profonda gratitudine, William annunciò che il progetto era quasi completato e che sarebbe tornato negli Stati Uniti entro poche settimane. Tuttavia, affermò di avere un'emergenza medica (appendicite) e di aver bisogno di 7.500 dollari per un intervento chirurgico non coperto dalla sua assicurazione. Sarah, ora emotivamente coinvolta, chiese un prestito sulla sua pensione per inviare i fondi.
Situazione di crisi: poco prima del suo presunto ritorno in America, William affermò di aver avuto un incidente sul posto di lavoro. Aveva bisogno di 15.000 dollari per le spese mediche e per risolvere una controversia legale con l'azienda locale per il rilascio del passaporto. Promise di rimborsare tutto al suo ritorno.

Segnali di pericolo che Sarah non ha notato

Ripensandoci, Sarah ha individuato diversi segnali d'allarme che aveva trascurato:

La riluttanza di William a fare videochiamate
Incongruenze nei suoi racconti sulla famiglia e sul lavoro
La sua conoscenza dell'ingegneria sembrava vaga quando gli veniva chiesto di fornire dettagli
Le foto non lo hanno mai mostrato in Malesia o nei luoghi di lavoro
Tutte le conversazioni erano incentrate sulla loro relazione o sui suoi problemi
I suoi scritti contenevano errori grammaticali incoerenti con quelli di un madrelingua inglese
Le ragioni per cui non riusciva ad accedere ai suoi ingenti fondi diventavano sempre più elaborate

Il punto di svolta

Sarah cominciò a insospettirsi quando le richieste di William aumentarono e le sue storie si fecero più complesse. Quando lei gli parlò di fargli visita in Malesia, lui la sconsigliò vivamente. Sua figlia, preoccupata per la situazione finanziaria della madre, insistette per esaminare le comunicazioni di William e riconobbe i modelli di una truffa sentimentale.

Per confermare i loro sospetti, la figlia di Sarah ha condotto una ricerca inversa delle immagini sulle foto di William, scoprendo che appartenevano a un professore in pensione in Canada che non aveva

collegamenti con il truffatore.

Risoluzione e conseguenze

Sarah alla fine perse circa 25.500 dollari a causa del truffatore prima di interrompere i contatti. Affrontato, "William" inizialmente negò l'inganno, poi divenne aggressivo prima di scomparire del tutto. Sarah ha segnalato la truffa a:

Polizia locale
Centro di denuncia dei reati su Internet (IC3) dell'FBI
La piattaforma di incontri dove si sono incontrati
La sua banca e le sue istituzioni finanziarie

Sebbene non sia riuscita a recuperare i fondi persi, l'esperienza ha portato Sarah a:
Unisciti a un gruppo di supporto per sopravvissuti a truffe romantiche
Collaborare con un consulente finanziario per ricostruire i suoi risparmi pensionistici
Diventa un sostenitore della sensibilizzazione sulle truffe sentimentali nelle comunità di anziani
Sviluppare confini più sani nelle relazioni

Impatto psicologico

Sarah ha subito un trauma emotivo significativo a causa della truffa:
Profonda vergogna e imbarazzo
Problemi di fiducia nelle nuove relazioni
Depressione e ansia
Stress finanziario dovuto alle perdite
Dolore per la relazione che pensava di avere

Lezioni chiave

Questo caso mette in luce diversi aspetti importanti delle truffe sentimentali:

I truffatori prendono di mira le persone vulnerabili, in particolare quelle che hanno subito perdite recenti

1. Costruiscono connessioni emotive prima di fare richieste finanziarie

3. Isolano le vittime dalle reti di supporto che potrebbero identificare la truffa
4. Creano urgenza e pressione emotiva attorno alle richieste finanziarie
5. Hanno spiegazioni plausibili sul perché non possono effettuare videochiamate o incontrarsi di persona

Strategie di prevenzione

Dall'esperienza di Sarah emergono diverse strategie di prevenzione:
Non inviare mai denaro a qualcuno che non hai incontrato di persona
Insistere sulle videochiamate all'inizio delle relazioni online
Ricerca le informazioni e le foto della persona
1. Discutere di nuove relazioni con amici fidati o familiari
2. Fai attenzione alle relazioni che progrediscono insolitamente rapidamente

Chiediti perché qualcuno con risorse dichiarate ha bisogno del tuo aiuto finanziario
Siate scettici nei confronti delle emergenze e delle crisi ripetute

Conclusione

Il caso di Sarah è rappresentativo delle migliaia di truffe sentimentali che si verificano ogni anno. Sebbene abbia perso ingenti somme di denaro, l'impatto emotivo del tradimento si è rivelato ancora più devastante. Attraverso la terapia e i gruppi di supporto, Sarah ha ricostruito la sua vita e ora aiuta gli altri a riconoscere i segnali d'allarme delle truffe sentimentali prima che perdano i propri risparmi o il proprio cuore a causa di abili manipolatori.

Conoscere e crescere: autovalutazione e valutazione.

Co-funded by
the European Union

4 Autovalutazione e valutazione

4.1 Test di autovalutazione sul Capitolo 1: Comprendere le truffe amorose

1. Qual è l'obiettivo principale di una truffa amorosa?
A) Per trovare veri partner romantici
B) Per sfruttare i legami emotivi per ottenere un guadagno finanziario
C) Per promuovere sane relazioni online
D) Per fornire consigli sugli appuntamenti
Risposta corretta: B

2. A quale truffa storica si dice che abbia origine la truffa dell'amore?
A) Schema Ponzi
B) La truffa del “prigioniero spagnolo”
C) Schema piramidale
D) Schema del principe nigeriano
Risposta corretta: B

3. Qual è la fase iniziale nella struttura di Whitty per le fasi di una truffa sentimentale?
A) Fase di preparazione
B) Fase di profilazione
C) Fase di sfruttamento
D) Fase di rivelazione
Risposta corretta: B

4. Nelle truffe sentimentali, la tattica di sommergere la vittima di affetto e attenzione è nota come:
A) Senso di colpa
B) Creazione di crisi
C) Love bombing
D) Sfruttamento finanziario
Risposta corretta: C

5. Quale dei seguenti è un segnale d'allarme comune nelle truffe sentimentali?
A) Richieste di incontro immediato di persona
B) Dettagli personali limitati o vaghi sul profilo del truffatore
C) Storie di vita chiare e coerenti
D) Presenza pubblica sui social media
Risposta corretta: B

6. Secondo gli studi, quale gruppo ha maggiori probabilità di cadere vittima di truffe sentimentali?
A) Giovani adulti di età compresa tra 18 e 25 anni
B) Uomini anziani di età superiore ai 70 anni
C) Donne di mezza età di età compresa tra 40 e 60 anni
D) Adolescenti
Risposta corretta: C

7. Quale tipo di metodo di pagamento viene comunemente richiesto dai truffatori nelle truffe amorose?
A) Assegni personali
B) Criptovaluta o carte regalo
C) Pagamenti con carta di credito
D) Deposito diretto su un conto bancario
Risposta corretta: B

8. In che modo i truffatori cercano spesso di impedire alle vittime di riconoscere la truffa?
A) Incontrando frequentemente le vittime
B) Solo tramite videochiamate
C) Chiedendo alle vittime di evitare di condividere i dettagli della loro relazione con altri
D) Incoraggiando le vittime a denunciarli
Risposta corretta: C

10. Quale delle seguenti è una misura preventiva consigliata contro le truffe sentimentali?
A) Inviare denaro rapidamente per evitare di perdere la relazione
B) Mantenere i dettagli privati ed effettuare controlli dei precedenti sui nuovi contatti
C) Evitare del tutto amicizie e relazioni
D) Ignorare qualsiasi sentimento di sospetto
Risposta corretta: B

9. Qual è spesso l'impatto psicologico sulle vittime di truffe sentimentali, secondo Button et al. (2014)?
A) Sollievo e soddisfazione
B) Solo perdita finanziaria senza impatto emotivo
C) Grave trauma emotivo e perdita finanziaria
D) Sentirsi più sicuri
Risposta corretta: C

4.2 Test di autovalutazione sul Capitolo 2: Buone pratiche per gli educatori

1. Qual è uno dei motivi principali per cui i truffatori prendono di mira gli anziani socialmente isolati?
A) Sono più propensi a investire in azioni rischiose
B) Sono desiderosi di apprendere nuove tecnologie
C) Sono solitamente ricchi
D) Sono emotivamente vulnerabili e cercano connessioni
Risposta corretta: D

2. Quali fattori contribuiscono più spesso alla vulnerabilità di un anziano alle truffe amorose?
A) Reddito elevato e mancanza di esperienza sui social media
B) Fiducia nella natura, declino cognitivo e bisogno emotivo
C) Tempo libero e buon supporto familiare
D) Di solito sono ricchi
Risposta corretta: B

3. Quale tattica usano spesso i truffatori per adescare emotivamente le loro vittime?
A) Linguaggio legale rigoroso
B) Promesse di eredità anticipata C) Love bombing e rinforzo emotivo
D) Presa in giro della loro solitudine
Risposta corretta: C

4. Qual è il doppio trauma che spesso affrontano le vittime di truffe amorose?
A) Tradimento emotivo e perdita finanziaria
B) Problemi legali e declino della salute
C) Conflitti familiari e imbarazzo
D) Uso improprio della tecnologia e perdita del lavoro
Risposta corretta: A

5. Quali conseguenze possono persistere anni dopo la truffa se non è stato offerto loro un supporto adeguato?
A) Miglior giudizio
B) Trauma a lungo termine ed evitamento delle relazioni
C) Migliori abitudini online
D) Migliore autostima
Risposta corretta: A

6. Perché gli anziani spesso evitano di denunciare le truffe?
A) Non capiscono come funziona la segnalazione
B) Non sono emotivamente coinvolti
C) Temono la vergogna, il ridicolo o il giudizio
D) Vogliono proteggere il truffatore
Risposta corretta: C

7. Perché gli educatori sono spesso più efficaci della famiglia nell'individuazione precoce delle truffe?
A) Hanno l'autorità legale per indagare
B) Limitano l'uso online
C) Gli anziani si sentono meno giudicati e più a loro agio a confidarsi con loro
D) Vivono con gli anziani
Risposta corretta: C

8. Quale ruolo possono svolgere gli operatori giovanili nel ridurre la vulnerabilità degli anziani alle truffe?
A) Segnalare le truffe alle banche per conto degli anziani
B) Offrire tutoraggio digitale intergenerazionale ed empatia
C) Rimuovere gli anziani dalle piattaforme online
D) Sostituire gli educatori in tutti i workshop
Risposta corretta: B

9. Qual è il motivo principale per cui l'alfabetizzazione digitale è fondamentale per prevenire le truffe?
A) Per ridurre la suscettibilità alle tattiche di frode online
B) Per far sì che gli anziani trascorrano più tempo online
C) Per insegnare loro a creare blog
D) Per evitare di dover ricorrere all'intervento della polizia
Risposta corretta: A

10. Perché i “buddy systems” sono efficaci nel prevenire le truffe?
A) Riducono i costi di viaggio per gli insegnanti
B) Limitano le telefonate
C) Monitorano l'uso di Internet
D) Offrono agli anziani qualcuno a cui confidarsi in caso di attività sospette
Risposta corretta: D

11. Quali dovrebbero essere le priorità degli educatori quando progettano workshop sulla prevenzione delle truffe?
A) Linguaggio tecnico complesso e sessioni lunghe
B) Racconti ammonitori basati sulla vergogna
C) Metodi accessibili e interattivi sulla consapevolezza emotiva e digitale
D) Dire agli anziani di smettere di usare la tecnologia
Risposta corretta: C

12. Quale comportamento è un segnale precoce di una truffa sentimentale in corso?
A) Fare volontariato più spesso
B) Aumentare le visite dei familiari
C) Frequentare corsi di alfabetizzazione digitale
D) Improvvisa segretezza su una nuova relazione online (Corretto)
Risposta corretta: D

13. Quale NON è un metodo di rilevamento consigliato?
A) Confronto diretto
B) Conversazioni per costruire la fiducia
C) Coinvolgimento emotivo
D) Osservazione del comportamento
Risposta corretta: A

14. Che cosa si intende per “triage” nella strategia di risposta alle truffe?
A) Incolpare la vittima
B) Valutare, accusare, segnalare
C) Ignorare, osservare, analizzare
D) Coinvolgere, educare, valutare
Risposta corretta: D

15. Come dovrebbero comportarsi gli educatori con gli anziani emotivamente coinvolti nelle truffe?
A) Usare tattiche intimidatorie
B) Usare scenari anonimi e domande guidate
C) Insistere affinché segnalino immediatamente la truffa
D) Avvisare la famiglia senza il consenso
Risposta corretta: B

16. In che modo gli educatori possono contribuire a ridurre l'isolamento post-truffa?
A) Incoraggiare la segretezza
B) Riconnettere le vittime con attività sociali sicure e gruppi di supporto
C) Monitorare i loro social media
D) Interrompere l'uso di Internet
Risposta corretta: B

17. Perché gli educatori dovrebbero coinvolgere con sensibilità le famiglie delle vittime?
A) Per incolparli
B) Per aumentare la pressione
C) Per delegare la responsabilità
D) Per creare supporto e ridurre la vergogna della vittima
Risposta corretta: D

18. Perché le collaborazioni con biblioteche, centri sanitari e centri comunitari sono fondamentali per prevenire le truffe?
A) Riducono la burocrazia
B) Sostituiscono il lavoro dell'educatore
C) Aiutano a raggiungere gli anziani e a fornire ambienti di fiducia
D) Possono far rispettare le leggi
Risposta corretta: C

4.3 Test di autovalutazione sul Capitolo 3: Nozioni di base sulla sicurezza informatica per principianti

1: Qual è la caratteristica principale di un attacco di phishing?
a) Installazione di malware tramite dispositivi USB
b) Sfruttamento delle vulnerabilità del software
c) Ingannare gli individui affinché rivelino informazioni sensibili attraverso comunicazioni fraudolente
d) Violazione fisica dei sistemi informatici
Risposta corretta: C

2: In che cosa lo spear phishing differisce dal phishing tradizionale?
a) Utilizza telefonate invece di e-mail
b) Prende di mira individui o organizzazioni specifici con attacchi personalizzati
c) Prende di mira solo le agenzie governative
d) Utilizza la posta cartacea invece della comunicazione elettronica
Risposta corretta: B

3: Che cosa si intende per pretexting nell'ingegneria sociale?
a) Invio di e-mail di massa a destinatari casuali
b) Creazione di uno scenario inventato per coinvolgere le vittime e rubare informazioni
c) Utilizzo di exploit tecnici per ottenere l'accesso al sistema d) Installazione di keylogger sui computer di destinazione
Risposta corretta: B

4: Quale scenario descrive meglio un attacco baiting?
a) Lasciare unità USB infette nei parcheggi affinché i dipendenti le trovino
b) Inviare e-mail minacciose che richiedono il pagamento
c) Effettuare telefonate fingendosi di essere personale di supporto IT
d) Creare falsi profili sui social media
Risposta corretta: A

5: Cos'è il tailgating nel contesto dell'ingegneria sociale?
a) Seguire l'attività online di qualcuno
b) Monitorare il traffico di rete
c) Seguire qualcuno attraverso una porta sicura senza la dovuta autorizzazione
d) Copiare i tasti premuti da qualcuno
Risposta corretta: C

6: A cosa si riferisce il termine "vishing"?
a) Phishing visivo tramite siti web falsi
b) Phishing virale tramite social media
c) Phishing video tramite videochiamate false
d) Phishing vocale tramite chiamate telefoniche
Risposta corretta: D

7: Quale principio psicologico sfruttano comunemente gli ingegneri sociali?
a) Complessità tecnica
b) Protocolli di rete
c) Autorità e fiducia
d) Algoritmi di crittografia
Risposta corretta: C

8: Cos'è un attacco watering hole?
a) Avvelenamento delle riserve idriche effettive
b) Compromissione di siti web visitati frequentemente dalle organizzazioni prese di mira
c) Attacco alle aziende di servizi idrici
d) Utilizzo di e-mail di phishing a tema idrico
Risposta corretta: B

9: Cosa caratterizza un attacco di ingegneria sociale quid pro quo?
a) Offrire qualcosa in cambio di informazioni o accesso
b) Minacciare azioni legali
c) Utilizzare solo metodi tecnici
d) Prendere di mira solo i dirigenti
Risposta corretta: A

10: Che cos'è il reverse social engineering?
a) Progettare i social network al contrario
b) Quando l'aggressore si posiziona come utile e aspetta che la vittima lo contatti
c) Invertire gli effetti dell'ingegneria sociale
d) Utilizzare i social media in ordine cronologico inverso
Risposta corretta: B

11: Quale dei seguenti è un campanello d'allarme che potrebbe indicare un tentativo di ingegneria sociale?
a) Richieste di aggiornamenti software
b) Richieste urgenti di informazioni sensibili con minacce di conseguenze
c) Comunicazioni private regolari
d) Riunioni programmate con persone conosciute
Risposta corretta: B

Sources

AARP. (n.d.). Romance scams. https://www.aarp.org/money/scams-fraud/

AARP. (2021). AARP VOA ReST program: Healing after fraud. AARP Fraud Watch Network. https://www.aarp.org/fraudwatchnetwork

AARP. (n. d.). Emotional Support for Victims of Fraud. https://states.aarp.org/maryland/emotional-support-for-victims-of-fraud#

Against Scams. (2024). The importance of trauma therapy for scam victims. https://againstscams.org/importance-of-trauma-therapy-for-scam-victims-2024

Action Fraud. (n.d.). Romance fraud. https://www.actionfraud.police.uk/

Action Fraud. (2025, January 30). Our research and statistics on romance fraud – Action Fraud claims advice. https://www.actionfraud.org.uk/research-and-statistics-on-romance-scams-fraud/

Ayoobi, N., Shahriar, S., & Mukherjee, A. (2023, September 5). The looming threat of fake and LLM-generated LinkedIn profiles: Challenges and opportunities for detection and prevention. arXiv. https://doi.org/10.1145/3603163.3609064

BBC News. (2024, May 7). How a 'Brad Pitt' scam broke my mum's heart. https://www.bbc.com/news/articles/ckgnz8rw1xgo

Berry, K. (2024, November 24). Scams: 'I was duped by Martin Lewis deepfake advert'. BBC News. https://www.bbc.co.uk/news/articles/clyvj754d9lo

Boulat, P.-A., & Wake, P. (2024, May 15). Can AI-generated deepfakes compromise know your customer (KYC) authentication? techUK. https://www.techuk.org/resource/can-ai-generated-deepfakes-compromise-know-your-customer-kyc-authentication.html

Sources

Brady, S. (2024, February 20). Tinder bolsters ID verification amid surge in AI scams. Verdict. https://www.verdict.co.uk/tinder-bolsters-id-verification-amid-surge-in-ai-scams/?cf-view&cf-closed

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224(Original work published 2014)

Commissariato di P.S. (n.d.). Truffe romantiche - Romance scam. Polizia di Stato. https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/truffe-romantiche-romance-scam/index.html

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020.). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. Clin Pract Epidemiol Ment Health, 16 https://doi.org/10.2174/1745017902016010024

Cross, C. (2014). Love hurts: the costly reality of online romance fraud. The Conversation.

Cross, C., Dragiewicz, M., & Richards, K. (2016). Understanding romance fraud: Insights from domestic violence theory. Cyberpsychology, Behavior, and Social Networking, 19(7), 419-423. https://doi.org/10.1089/cyber.2016.0729

Cross, C., & Layt, R. (2021). “I suspect that the pictures are stolen”: Romance fraud, identity crime, and responding to suspicions of inauthentic identities. Social Science Computer Review, 40(4), 1043–1058. https://doi.org/10.1177/0894439321999311

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: The need to rethink current romance fraud prevention messaging. Crime Prevention and Community Safety, 24(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Sources

Cunha, H. S. (n.d.). Why are romance scams so powerful? https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf

CybSafe. (2023). Romance scams: The stats, and what they mean for your organization. https://www.cybsafe.com/blog/romance-scams-stats-for-organizations/

Daily Mail. (2024, June 1). British grandmother arrested in Brazil for smuggling cocaine. https://www.dailymail.co.uk/news/article-14718249/Grandmother-Veronica-Watson-Brazil-drugs.html

Dellinger, A. J. (2019). Anatomy of a scam: Nigerian romance scammer shares secrets. Forbes. https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/

Dogma. Truffe sentimentali: I segnali e come difendersi. https://www.dogma.it/it/news/truffe-sentimentali--i-segnali-e-come-difendersi

Eberhart, C. (2023, May 26). Who is watching you? AI can stalk unsuspecting victims with 'ease and precision': Experts. Fox News. https://www.foxnews.com/us/who-is-watching-you-ai-can-stalk-unsuspecting-victims-ease-precision-experts

Europol. 13 arrested in Italy for tricking elderly in love. https://www.europol.europa.eu/media-press/newsroom/news/13-arrested-in-italy-for-tricking-elderly-love

Europol. How not to fall for the "lover boy" scam. Europol. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-not-to-fall-for-lover-boy-scam

Sources

Europol. (2023). Spotlight report: Online fraud schemes. https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Europol. (2017). Online sexual coercion and extortion as a crime affecting children. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Federal Bureau of Investigation. (2024, December 3). Criminals use generative artificial intelligence to facilitate financial fraud. https://www.ic3.gov/PSA/2024/PSA241203

Federal Trade Commission. (2023). Romance scammers' favorite lies exposed. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

Federal Trade Commission. Report fraud. https://reportfraud.ftc.gov/

Federal Trade Commission. Avoiding online romance scams. https://www.consumer.ftc.gov

Finney, G. (2023). Project Zero Trust. Cybersecurity Insights. https://www.cybersecurityinsights.com/project-zero-trust

Fintech Global. (2025, February 13). Banks face heightened reputational and financial risks as romance scams surge. https://fintech.global/2025/02/13/banks-face-heightened-reputational-and-financial-risks-as-romance-scams-surge/

Goodwin, L. (2024, December 19). 'AI deepfake romance scam duped me out of £17k'. BBC News. https://www.bbc.co.uk/news/articles/cdr0g1em52go

Sources

Gozzi, L. (2025, January 15). French woman duped by AI Brad Pitt faces mockery online. BBC News. https://www.bbc.co.uk/news/articles/ckgnz8rw1xgo

Howard, R. (2023). Cybersecurity First Principles: A Reboot of Strategy and Tactics. John Wiley & Sons. https://www.wiley.com/en-us/Cybersecurity%2BFirst%2BPrinciples%3A%2BA%2BReboot%2Bof%2BStrategy%2Band%2BTactics-p-9781394173099

Internet Crime Complaint Center (IC3). (n.d.). Romance scams. https://www.ic3.gov/

Interpol. (2022). Interpol report on sextortion trends. International Criminal Police Organization. Retrieved from https://www.interpol.int

Kollmorgen, A. (2025). AI-driven romance scams likely leading to higher losses. Choice. https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/romance-scams-and-how-to-avoid-them

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: prevalence, process, and offender characteristics. Trauma, violence & abuse, 15(2), 126–139. https://doi.org/10.1177/1524838013511543

Lee, Y., & Gelman, B. (2023, November 27). The dark side of AI: Large-scale scam campaigns made possible by generative AI. Sophos News. https://news.sophos.com/en-us/2023/11/27/the-dark-side-of-ai-large-scale-scam-campaigns-made-possible-by-generative-ai/

Magramo, K. (2024, May 17). British engineering giant Arup revealed as $25 million deepfake scam victim. CNN. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

Sources

Mattackal, L. P. (2025, February 14). Crypto scams likely set new record in 2024 helped by AI, Chainalysis says. Reuters. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/

Narang, S. (2024, February 14). Pig butchering scam: How Bitcoin, Ethereum, Litecoin and spot gold (XAUUSD) investments are used in romance scams to steal hundreds of millions. Tenable. https://www.tenable.com/blog/pig-butchering-scam-bitcoin-ethereum-litecoin-spot-gold-xauusd-romance-scam

National Cyber Security Centre. (2024, January 24). The near-term impact of AI on the cyber threat. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

National Crime Agency [NCA]. (2021). Sextortion threat report. NCA Cybercrime Unit. https://www.nationalcrimeagency.gov.uk

Newcastle University. (n.d.). Online dating scam victims: Psychological impact analysis. https://doi.org/10.54097/ehss.v4i.2740

Newman, L. H., & Burgess, M. (2024, September 30). The pig butchering invasion has begun. Wired. https://www.wired.com/story/pig-butchering-scam-invasion/

Newman, L. H., & Burgess, M. (2025, February 13). The loneliness epidemic is a security crisis. Wired. https://www.wired.com/story/loneliness-epidemic-romance-scams-security-crisis/

Nielson, S. J. (2023). Discovering cybersecurity: A technical introduction for the absolute beginner. Apress. https://doi.org/10.1007/978-1-4842-9560-1

Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. Sexual abuse : a journal of research and treatment, 32(1), 30–54. https://doi.org/10.1177/1079063218800469

Sources

Patel, M. (2025). Cybersecurity for beginners: Learn practical skills to defend against cyber threats and prepare for certification exams. Michael Patel. ISBN-13: 9798227516435.

pen University. (2024). The psychology of cybercrime. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

Pietilä, E. & Korhonen, H. (5.06.2024). The harsh realities of romance scams. https://nordicwelfare.org/popnad/en/artiklar/the-harsh-realities-of-romance-scams/

Policija.si. (n.d.). Romance scams. Slovene Police. https://www.policija.si/eng/prevention/internet-security/romance-scams

Rege, A. (2009). Tainted love: A systematic literature review of online romance scam research. Interacting with Computers, 21(5-6), 427–437. https://doi.org/10.1016/j.intcom.2009.06.006

Rogiers, A., et al. (2024, November 11). Persuasion with large language models: A survey. arXiv. https://doi.org/10.48550/arxiv.2411.06837

Sanction Scanner. (2024, September 16). How generative artificial intelligence launders money. https://www.sanctionscanner.com/blog/ais-dark-side-how-generative-artificial-intelligence-launders-money-863

ScamWatch. (2024, August 15). Online dating and romance scams. https://www.scamwatch.gov.au/types-of-scams/online-dating-and-romance-scams

SciSpace. (n.d.). Online romance scams: Relational dynamics and psychological insights. https://scispace.com/papers/online-romance-scams-relational-dynamics-and-psychological-5cckseevfj

Sources

Shea, S., & Krishnan, A. (2024). How AI is making phishing attacks more dangerous. TechTarget. https://www.techtarget.com/searchSecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

Shepardson, D. (2024). Consultant fined $6 million for using AI to fake Biden's voice in robocalls. Reuters. https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/

Statista. (2025,). Number of fake accounts removed by Facebook per quarter worldwide as of Q1 2025. https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hall, J., & Kieran. (2024, November). AI-enabled influence operations: Safeguarding future elections. CETaS Research Reports.

Surrey Police. Romance fraud. Surrey Police. https://www.surrey.police.uk/romancefraud

Tech Report. Romance scam statistics. https://techreport.com/statistics/cybersecurity/romance-scam-statistics/

The Debt Advisor. (2023). Romance scams: A growing threat to both men and women. https://www.thedebtadvisor.co.uk/romance-scams/

The Guardian. (2024). Spanish police arrest five people over fake Brad Pitt scam. https://www.theguardian.com/film/2024/sep/23/spanish-police-arrest-five-people-over-fake-brad-pitt-scam

Sources

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

U.S. Federal Reserve. (2024). Synthetic identity fraud: Generative AI toolkit for payments fraud detection. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

U.S. Immigration and Customs Enforcement. (10.02.2025). Sextortion. https://www.ice.gov/features/sextortion#

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

U.S. Federal Reserve. (2024). Synthetic identity fraud: Generative AI toolkit for payments fraud detection. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

Wang, C. (2022). Online Dating Scam Victims Psychological Impact Analysis. Journal of Education, Humanities and Social Sciences, 4, 149-154. https://doi.org/10.54097/ehss.v4i.2740

Wang, F. (2024). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. International Review of Victimology, 31(1), 91-116. https://doi.org/10.1177/02697580241234331 (Original work published 2025)

Sources

Whitty, M. T., & Buchanan, T. (2016). Do you love me? Psychological characteristics of romance scam victims. Psychological Characteristics of Romance Scam Victims - PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5297105/

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: Causes and consequences of victimhood [PDF]. University of Warwick. https://wrap.warwick.ac.uk/id/eprint/81382/1/WRAP_whitty__buchananpsychological_impact_romance_scam_final_version.pdf

Whitty, M. & Buchanan, T.. (2012). The Online Romance Scam: A Serious Cybercrime. Cyberpsychology, behavior and social networking. 15. 181-3. 10.1089/cyber.2011.0352.

Wrexham.com. (2024, February13). Wrexham man conned out of £25k in romance scam. https://wrexham.com/news/warning-issued-after-wrexham-man-conned-out-of-25k-in-romance-scam-247088.html

Yeung, J. (2024, October 15). Deepfake romance scam raked in $46 million from men across Asia, police say. CNN. https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk/index.html

Zhang, D., et al. (2024, February 9). IP-Adapter inpainting: Controllable inpainting with IP-Adapter. arXiv. https://arxiv.org/html/2502.06593v1

Zvelo. (2023, November 8). The role of AI in social engineering. https://zvelo.com/the-role-of-ai-in-social-engineering

Zvelo. (2023, November 8). The role of AI in social engineering. U

Connect with US!

This manual was developed collaboratively by the FALS project coordinators; EUW (Germany), ECREC (The Netherlands), and IVI (Italy).

To stay connected, and in case of any inquiries, comments, or suggestions, Please feel free to reach out to us through the following channels.

ECREC (The Netherlands)

Phone
+31 70 200 2595

Email
info@ecrec.eu

Website
https://ecrec.eu/

EUW (Germany)

Phone
+49 176 55030502

Email
projects@euthwonders.org

Website
www.euthwonders.org

IVI (Italy)

Phone
+39 329 599 7585

Email
igorvitaleinternational@gmail.com

Website
https://www.igorvitale.org/

Co-funded by the European Union

Connettiti con noi!

Questo manuale è stato sviluppato in collaborazione dai coordinatori del progetto FALS: EUW (Germania), ECREC (Paesi Bassi) e IVI (Italia).

Per rimanere in contatto e per qualsiasi domanda, commento o suggerimento, non esitate a contattarci tramite i seguenti canali.

ECREC (Paesi Bassi)

Telefono
+31 70 200 2595

E-mail
info@ecrec.eu

Sito web
https://ecrec.eu/

EUW (Germania)

Telefono
+49 176 55030502

E-mail
projects@euthwonders.org

Sito web
www.euthwonders.org

IVI (Italia)

Telefono
+39 329 599 7585

E-mail
igorvitaleinternational@gmail.com

Sito web
https://www.igorvitale.org/

Co-funded by the European Union