Polizia di Stato

Rotary
Gruppo Terre Padane
Distretto 2050

Internet per i “Diversamente Giovani”

Truffe online: Conoscerle per evitarle

INDICE

Prefazione

Dr. Michele Davide SINIGAGLIA
Questore di Cremona

È davvero pregevole l'iniziativa della Sezione Operativa per la Sicurezza Cibernetica – Polizia Postale di Cremona che, con la collaborazione del Gruppo Terre Padane del Rotary, ha realizzato questo pratico manuale che aiuta a difendersi dalle truffe online.

Un tema di stretta attualità, e di sicuro interesse, se si considera che nel 2022 la Polizia di Stato ha svolto indagini su 15.699 segnalazioni di truffe online, arrivando a denunciare all'Autorità Giudiziaria ben 3.570 persone. Cifre, credo, che consentono di inquadrare in modo chiaro la dimensione del fenomeno.

D'altro canto, ad oltre trent'anni di distanza dalla nascita del *World Wide Web* è innegabile che le potenzialità di questo formidabile strumento di connessione e comunicazione planetaria abbiano completamente modificato le abitudini di vita della generalità delle persone ed anche di coloro che, come me, non sono "nativi digitali".

Alle grandi opportunità rappresentate dalla rete telematica mondiale, accessibile oramai da un'ampia gamma di dispositivi elettronici, alcuni dei quali, penso in particolare agli *smartphone*, ci accompagnano in ogni momento della giornata, hanno ben presto corrisposto nuove potenziali fonti di rischio e di vulnerabilità che la criminalità ha saputo rapidamente sfruttare per trarne profitto.

Non starò qui a dilungarmi sulle tante tecniche ideate dai truffatori per carpire la buona fede delle vittime, puntualmente descritte nelle pagine che

seguono. C'è però un elemento che le accomuna tutte: la capacità criminale di sfruttare un particolare fattore di debolezza della vittima che la porta a cadere nei cosiddetti "artifici e raggiri" che costituisco l'elemento fondante del reato di truffa.

Come difendersi allora?

Lo spiega in modo chiaro ed efficace questo manualetto che invito a leggere con attenzione, facendone poi magari argomento di conversazione ed approfondimento con coloro che ci sono vicini, perché si diffonda sempre più la consapevolezza che da questi crimini ci si può difendere informandosi ed acquisendo una maggiore conoscenza dei pericoli che si possono incontrare quando *si naviga* in rete.

Da tempo, infatti, la Polizia di Stato promuove con regolarità su tutto il territorio nazionale campagne di comunicazione volte a diffondere la cultura della legalità e della sicurezza, anche tra gli utenti di internet.

Questa della Polizia Postale di Cremona, simpaticamente rivolta a tutti coloro che sono *diversamente giovani*, ma non solo, si inserisce pienamente in questo solco e, ne sono convinto, con la collaborazione dei Club Rotary del territorio saprà raggiungere una platea sempre più ampia di persone.

Sicurezza Cibernetica - Polizia Postale

Da giugno 2022 la Polizia Postale e delle Comunicazioni ha cambiato denominazione in ***Sicurezza Cibernetica – Polizia Postale***, proprio per rimarcare lo specifico campo operativo, ovvero quello della sicurezza informatica.

La Sicurezza Cibernetica - Polizia Postale è una delle specialità della Polizia di Stato, i cui compiti sono il contrasto ai crimini informatici, quali truffe, frodi informatiche, reati di pedopornografia, terrorismo online, cyberbullismo, ecc.; è inoltre deputata alla protezione delle infrastrutture critiche del Paese.

E' articolata da un Servizio Centrale presso il Dipartimento della Pubblica Sicurezza che coordina le attività a livello nazionale e funge da punto di contattato con gli altri Paesi. Sul territorio, a livello regionale, sono presenti i Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.), da cui dipendono, a livello provinciale, le Sezioni Operative per la sicurezza Cibernetica (S.O.S.C.).

Oltre alla repressione dei reati online, la Polizia Postale svolge attività di prossimità con la cittadinanza, promuovendo incontri per sensibilizzare l'attenzione e alzare l'allerta sui possibili pericoli di Internet, aiutando le fasce più deboli a districarsi nel mondo digitale.

Importanti sono gli incontri che ogni anno vengono svolti nelle scuole di tutto il territorio con gli studenti delle scuole secondarie di primo e secondo grado per informare i più giovani sull'uso consapevole dei social media, al fine di evitare che comportamenti online definiti "scherzi" possano trasformarsi in atti di cyberbullismo verso i ragazzi più sensibili.

Nei più giovani, oltre al rischio cyberbullismo, non vanno dimenticati i pericoli derivanti dagli adescamenti e da tutti gli aspetti legati al mondo della pedopornografia.

Questa guida, però, è dedicata alla Terza Età, proiettata nel mondo virtuale a volte forzatamente (la pandemia, purtroppo, ha fatto la sua parte) e conseguentemente impreparata davanti ai rischi connessi all'uso di Internet; e poi, perché no? a volte smarrita nei termini tecnici o "moderni" spesso usati da chi Internet lo frequenta quotidianamente.

La guida si compone di due parti: una vuole essere un piccolo aiuto a capire le dinamiche che si nascondono dietro comportamenti truffaldini, l'altra è un piccolo glossario sui termini tecnici più comunemente usati, comprensivi di vocaboli e inglesismi spesso usati dai più giovani e meno noti agli adulti che possono apparire strani e oscuri a chi non ha dimestichezza con il mondo dei social.

Il consiglio ultimo, comunque, è che in qualsiasi situazione dubbiosa o pericolosa in cui il lettore possa imbattersi nell'uso dello strumento informatico o nell'interazione con altri utenti della rete, prima di agire, può sempre contattare il personale esperto e qualificato della Polizia Postale o comunque delle Forze dell'Ordine: loro sapranno sicuramente analizzare il problema e consigliare sul da farsi.

La Sezione Operativa per la Sicurezza Cibernetica
Polizia Postale di Cremona

Inquadra con lo smartphone per accedere al sito ufficiale della Polizia Postale, dove poter restare aggiornati sui pericoli del Web

Gruppo Terre Padane del Rotary

Il Service Rotariano alla base del progetto

§

Fabrizio Bragantini, Presidente Rotary Club Cremona 2022-2023

Il Rotary è una rete globale di 1,4 milioni di donne e uomini intraprendenti, amici, conoscenti, professionisti e imprenditori che credono in un mondo dove tutti i popoli, insieme, promuovono cambiamenti positivi e duraturi nelle comunità. Per farlo danno priorità a 7 Aree d'intervento, tra le quali troviamo l'Alfabetizzazione ed educazione di base e lo Sviluppo comunitario.

La crisi pandemica prima e la mutata "normalità" che la pandemia ci ha lasciato in eredità hanno spinto, in un relativamente breve lasso di tempo, verso la dematerializzazione di gran parte dei processi burocratici, dei rapporti con le Istituzioni e, ancora più importante, hanno spostato on-line attività quotidiane, gli acquisti e, molti rapporti interpersonali trasferiti, anche per necessità, sui social network. Questo rapido "cambio di passo", imposto in parte dalla situazione contingente ed in parte dal naturale progresso della tecnica, ha esposto a nuovi e precedentemente sconosciuti rischi alcune fasce generazionali delle nostre comunità (soprattutto quelle "diversamente giovani"), a cui è stata forzata la mano nel passaggio obbligato all'uso di tecnologie, strumenti e termini di cui non erano (e, per la gran parte dei casi ancora non sono) padroni né, tantomeno, idoneamente informati e preparati.

Questo spunto di riflessione, legato a doppio filo alle due Aree di intervento rotariane citate in precedenza, è stato così alla base del service dedicato al miglioramento e al consolidamento delle conoscenze informatiche e tecniche per le persone over 60 ed ideato, nella sua versione iniziale, dal Rotary Club Cremona, che ho l'onore di rappresentare per questo anno rotariano ma che ha avuto una importante evoluzione ed un affinamento grazie all'impegno ed alla fattiva, operosa collaborazione della Sezione Operativa per la Sicurezza Cibernetica - Polizia Postale di Cremona della Polizia di Stato e

di tutto il suo personale, a cui va il mio caloroso ringraziamento. Ringraziamento che devo anche agli amici Presidenti dei Club afferenti al Gruppo "Terre Padane" del Distretto 2050 (RC Cremona Po, RC Cremona Monteverdi, RC Soresina e RC Piadena Oglio Chiese) che hanno deciso di condividere il cammino di questo service ed il suo sforzo economico ed organizzativo, esportandone il modello sui territori di loro competenza.

Il presente volumetto, volutamente ideato per essere snello e di facile lettura, vuole essere un naturale complemento agli incontri che saranno svolti nelle nostre comunità a cura dei Club Rotary del territorio con l'insostituibile supporto, partecipazione e coordinamento della Polizia di Stato e costituisce un manabile sempre disponibile per dipanare i dubbi e sciogliere gli interrogativi che, durante la navigazione della rete e l'uso delle sue risorse, possono sorgere; un modo, insomma per non incappare, anche inconsapevolmente, in errori a volte pagati, come potrete leggere, davvero a caro prezzo.

Buona lettura e buona navigazione.

Rotary
Gruppo Terre Padane
Distretto 2050

Truffe online: conoscerle per evitarle

L'articolo 640 del Codice Penale recita:
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1) ***se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare;***
2) ***se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;***
2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.

Si definisce **ARTIFIZIO** la modificazione della realtà attraverso simulazioni di circostanze inesistenti o nascondendo situazioni esistenti.

Il **RAGGIRO**, invece, può definirsi come insieme di parole fuorvianti e capaci di indurre la vittima a decisioni diverse da quelle che avrebbe normalmente preso se non le fosse stata rappresentata una realtà diversa.

Artifizi o raggiri sono quindi gli elementi alla base della truffa. Elementi che prima dell'avvento di Internet erano per forza adottati di persona: il truffatore doveva interagire personalmente con la vittima, cercando di convincerla con le parole e distorcendo la realtà con abilità.

Come non ricordare il famoso film "Totòtruffa 62", dove un bravissimo Totò vendeva nientedimeno che la Fontana di Trevi allo sprovveduto turista? E' solo un film, potremmo dire, oppure potremmo rimanere stupiti davanti alle abilità dialettiche del truffatore e alla capacità di mistificare la realtà.

Inquadra con lo smartphone e guarda il video di Tototruffa62

Se questo è difficile nel mondo reale e richiede abilità non comuni, nel mondo virtuale la mistificazione è molto più semplice e alla portata di molti. Software in grado di modificare le immagini possono mostrarci ciò che in realtà non c'è. Quando acquistiamo qualcosa in internet lo acquistiamo sempre e soltanto guardando una immagine: ma l'immagine non certifica la reale esistenza di quell'oggetto! Trappole linguistiche a corredo di immagini di oggetti di un certo valore, quali "vincere", "regalo gratuito", "offerta esclusiva", "approfittane subito" devono farci riflettere ed alzare l'attenzione perché i passaggi successivi che ci inducono a compiere potrebbero essere pericolosi.

E lo stesso discorso deve essere fatto con le persone con cui stiamo interagendo: persone che non vediamo, ma con cui chattiamo e da cui stiamo acquistando, a cui daremo denaro. Non lasciamoci ingannare da documenti d'identità trasmessi dai nostri interlocutori, perché potrebbero essere falsi, creati digitalmente in modo artefatto, oppure appartenere ad altre persone che incautamente li hanno trasmessi a chissà quale truffatore che aveva prospettato loro, a suo tempo, affari vantaggiosi.

Infine, facciamo sempre attenzione ai link che arrivano per messaggio (mail o SMS): sono quelli che tecnicamente si chiamano phishing e sono il preambolo alla sottrazione di informazioni delicate che saranno poi usate per danneggiarci (codici bancari, carte di credito, password, documenti d'identità).

La truffa nel commercio elettronico

E' la più classica e diffusa delle truffe online e consiste nel frodare chi compra o addirittura chi vende merce attraverso internet. Tecnicamente possiamo distinguerle in due tipologie: l'una che si basa sulla creazione e sulla gestione di falsi siti di commercio elettronico, a volte cloni di quelli reali, l'altra che sfrutta i portali di vendite online (subito.it, bakeca, e.bay, marketplace di Facebook, Instagram, ecc,) per entrare in contatto con potenziali acquirenti. In tutti i casi, una volta pagata la merce, il venditore sparisce e si rende irreperibile.

COME SI SVILUPPA

1 **La truffa dei falsi siti di e-commerce**:

- Presenza di un sito che apparentemente mette in vendita una moltitudine di oggetti. Solitamente hanno prezzi molto convenienti e competitivi, proprio per catalizzare l'interesse della vittima. In realtà molte volte si tratta di cloni di siti reali.
- La procedura per l'acquisto è uguale a quella dei siti veri, ovvero creazione di un account, scelta dell'oggetto e messa nel carrello virtuale, pagamento (può avvenire con bonifico o carta di credito)
- Dopo il pagamento la merce non arriva e non è possibile contattare il venditore perché l'unico strumento disponibile è un falso form presente sul falso sito
- Può accadere che la spedizione della merce avvenga anche in **contrassegno**: in questo caso il compratore è rassicurato dal fatto che pagherà solo al ricevimento della merce. Al ricevimento del pacco il compratore paga

e solo all'apertura scoprirà che il pacco contiene oggetti inutili del valore di pochi euro.

2 La truffa delle false inserzioni di vendita sui portali che offrono il servizio di vendita / aste online tra privati:

- Il truffatore crea una falsa inserzione di vendita su un portale di aste online o sui marketplace dei social quali Facebook o Instagram;
- La vittima entra in contatto e per farla sentire più tranquilla, il venditore / truffatore fornisce anche un recapito telefonico con cui intercorrono messaggi via Whatsapp;
- Concordata la compravendita il truffatore chiede il pagamento con bonifico o ricarica su carta prepagata. Attenzione: il bonifico non dà alcuna certezza in più rispetto alla ricarica di una prepagata, perché attualmente molte carte prepagate sono gestite anche tramite un IBAN.
- Ricevuto il pagamento si rende irreperibile.

3 La truffa dei falsi acquirenti sui portali di vendita / aste online tra privati:

- Il venditore crea una inserzione di vendita per un suo oggetto.
- **1^ ipotesi**: il venditore viene contattato da un falso acquirente che si trova all'estero (solitamente paesi dell'africa occidentale) che con artifizi e raggiri lo induce a fare un versamento che sarà rimborsato con il bonifico che promette di effettuare. Per ottenere del denaro dal venditore, il falso acquirente adduce scuse quali pagamenti di tasse per acquisti all'estero. Per rendere credibile la cosa fa giungere alla casella di posta elettronica del venditore false mail da sedicenti istituti di credito con allegate false fidejussioni fatte dal falso acquirente
- **2^ ipotesi**: il venditore viene contattato da un falso acquirente che si dice disposto al pagamento tramite ricarica da effettuarsi presso uno sportello postamat. Il falso acquirente (truffatore) con una parlantina fluida non indifferente induce la vittima (venditore) a recarsi presso un postamat, a inserire un bancomat e, anziche ricevere il denaro come prospettato dal truffatore effettua delle ricariche a carte prepagate in uso al falso acquirente (chiamata anche truffa del postamat)

COME DIFENDERSI

1. Innanzitutto, diffidare sempre da prezzi troppo bassi: Sono il primo segnale di una possibile truffa

2. Sui siti d'aste controllate sempre i feedback del venditore: feedback negativi indicano un alto rischio di truffa.

3. Prima di avviare la trattativa ricercate tramite Google il numero del telefono del venditore oppure il suo nickname: spesse volte è già stato segnalato o indicato come truffatore.

4. Diffidate dall'invio da parte del venditore di documenti personali a garanzia della sua persona: questi documenti potrebbero essere stati acquisiti in modo fraudolento da altre vittime.

5. Quindi, mai trasmettere copie dei propri documenti a sconosciuti che non hanno esigenze reali di trattare i nostri dati

6. Se siamo noi i venditori rifiutiamo sempre la richiesta da parte del presunto acquirente di invio di denaro: ricordiamoci che siamo noi a vendere l'oggetto e siamo noi a dover ricevere il denaro. Non mandiamo mai la merce finché non abbiamo ricevuto il denaro.

7. Se il compratore ci chiede di recarci a uno sportello postamat per poter ricevere il denaro pattuito, rifiutiamoci. Il denaro può essere trasmesso in tanti modi e non è mai possibile riceverlo attraverso l'inserimento della propria carta in un bancomat o postamat. Se sono interessati all'acquisto possiamo chiedere che sia fatto un bonifico, oppure una ricarica su una carta prepagata di cui forniremo gli estremi.

8. Se acquistiamo su siti di commercio elettronico cerchiamo sempre sul sito la presenza di contatti, quali un numero di telefono, una mail, e un indirizzo. L'assenza di questi elementi rende altamente probabile che si tratta di siti truffa o comunque di siti che non spediranno la merce scelta. Di certo avremo difficolta di contatto qualora avessimo problemi con l'acquisto.

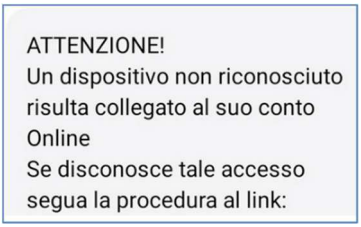
9 Se vogliamo acquistare merce su siti di commercio elettronico facciamo sempre riferimento a siti conosciuti che abbiano numerose recensioni / feedback positivi. Nei casi di siti cloni o falsi. non troveremo mai alcuna recensione. Anche nel caso di siti di commercio elettronico possiamo effettuare una ricerca tramite Google: potremmo scoprire che il sito ha già truffato altre persone oppure che il sito è un clone.

La truffa del phishing

Il phishing è una particolare tecnica che serve a carpire / rubare informazioni delicate e personali della vittima.
Possono essere informazioni relative a un profilo social, ma anche, e soprattutto, informazioni bancarie / finanziarie.

Nel phishing bancario, il malintenzionato cerca di indurre in errore la vittima fingendosi un istituto di credito (banche o società emittenti di carte di credito), con il fine di carpire i dati di accesso al servizio offerto (home banking). Una volta entrato in possesso dei dati bancari porta a termine, molte volte con l'ignara complicità della vittima, operazioni finanziarie tramite l'home banking del malcapitato.

I messaggi di phishing hanno sempre alcune caratteristiche comuni: **una connotazione di urgenza e la richiesta di inserimento di credenziali o informazioni sensibili**. Esattamente le cose che un istituto di credito NON chiederà mai tramite messaggio o tramite mail!!



COME SI SVILUPPA

1 **Il truffatore invia un falso messaggio di allarme alla vittima** (SMS o mail) che sembra provenire dal proprio istituto di credito e che segnala problemi al servizio offerto, rappresentato solitamente da un avviso di blocco del profilo / conto, oppure da un'operazione in sospeso da confermare. Il messaggio è corredato di link che, solo apparentemente, rimanda alla pagina

web dell'istituto di credito o del servizio a cui fa riferimento. La pagina web, clone di quella originale, chiede l'inserimento delle credenziali di accesso (userid e password) oppure di altri dati sensibili, quali utenza telefonica, numero della carta di credito ecc.. In questo passaggio stiamo fornendo al truffatore dati che dovrebbero rimanere riservati perché consento l'accesso al nostro conto corrente o alla nostra carta di credito.

2 **Quando si tratta di servizi bancari e c'è necessità di interagire con** il telefono della vittima perché certificato per le operazioni con l'home banking, le vittime sono contattate telefonicamente dal truffatore che si identifica come un operatore del nostro istituto di credito: egli è perfettamente a conoscenza di ciò che sta accadendo e conosce ogni dettaglio del nostro conto e dei nostri dati. In realtà, e già nell'home banking della vittima e gli risulta semplice interagire; e la vittima, proprio perché il truffatore gli sta fornendo informazioni che solo un operatore della banca dovrebbe sapere, è indotta a credere a quello che le viene detto.

3 **Il truffatore, perché ha bisogno dell'interazione con il telefono** certificato della vittima, chiede la sua collaborazione: in questo passaggio possono essere chiesti il relativo codice di sicurezza della carta di credito (CVV2), oppure le password temporanee (OTP) che giungono all'utenza, oppure l'interazione con l'impronta digitale per confermare l'operazione in atto con il sistema di home banking. Con i codici forniti al truffatore vengono autorizzati i trasferimenti di denaro, a volte anche di decine di migliaia di euro.

4 **Al termine delle operazioni, In alcuni casi, la vittima è invitata a** rimuovere l'app di home banking con la scusa di un aggiornamento e di reinstallarla dopo 24 ore: in questo lasso di tempo la vittima non è pertanto in grado di controllare i movimenti del conto e non può ricevere via app le notifiche di eventuali operazioni / anomalie sul proprio conto corrente.

COME DIFENDERSI

1 MAI cliccare su un link contenuto in un messaggio che sembra provenire dal nostro istituto di credito!

2 Diffidare dalle chiamate con toni ultimativi o intimidatori che sembrano provenire da operatori del nostro istituto di credito che ci prospettano la chiusura del conto bancario, il blocco della carta di credito o eventuali sanzioni se non si dovessero compiere subito certa azione. Possono essere subdole strategie per spingere il malcapitato a fornire informazioni e dati personali senza rifletterci troppo. Gli operatori telefonici hanno normalmente un atteggiamento cortese nei confronti dei clienti e sono disponibili. Invitiamo chi ci sta contattando a riagganciare dicendo che chiameremo noi direttamente la nostra banca per avere informazioni più dettagliate. A quel punto si può decidere di chiamare il proprio istituto di credito all'utenza affidabile e avere certezza della reale situazione.

3 Non fornire mai a nessuno dati e informazioni personali, codici di accesso, PIN, OTP, dati bancari e della carta di credito. È importante tenere presente che le banche e le aziende fornitrici di carte di credito conoscono già determinate informazioni sensibili sul nostro conto e risulta anomalo che ci chiedano proprio quelle informazioni che, di solito, esse stesse ci invitano a mantenere riservate.

4 Se si ricevono mail o messaggi che chiedono di richiamare determinati numeri di aziende o banche, controllare sempre prima se tali numeri corrispondono a quelli ufficiali (ad esempio consultando i siti web ufficiali). Per sicurezza, invece di chiamare i numeri indicati nel messaggio, ci si può rivolgere al centralino o all'URP dell'azienda o della banca per farsi mettere in contatto con l'ufficio che dovrebbe aver inviato il messaggio.

La truffa del trading online

E' la più pericolosa delle truffe, che può portare alla perdita totale del proprio denaro. Negli ultimi anni, anche a seguito della pandemia, si è diffusa sempre più. Le ignare vittime si lasciano convincere da sedicenti consulenti finanziari a tentare un piccolissimo investimento nel trading online delle criptovalute. Con una capacità persuasiva non comune e con false piattaforme di trading inducono la vittima a investire ingenti quantità di denaro (anche centinaia di migliaia di euro) in società inesistenti per poi sparire allorquando l'investitore truffato decide di disinvestire anche solo parte del capitale.

COME SI SVILUPPA

1 **Il truffatore inserisce pubblicità e/o post promozionali solitamente su Facebook e Instagram,** riguardanti il trading online, investimenti di Bitcoin o di azioni di aziende molto conosciute (es. Amazon). Tali scritti sono corredati da un link che riconduce a una pagina web di una fantomatica società di investimenti, dove la persona interessata lascia i propri dati di contatto.

2 **Il truffatore contatta la potenziale vittima,** chiamandola al telefono (solitamente sono numeri con prefisso inglese + 44) spiegando in modo accurato e professionale come funziona il trading online, elogiandone i benefici economici superiori ai normali investimenti proposti dalle banche tradizionali, quali meno tasse da pagare, meno spese di intermediazione e un guadagno facile nell'immediato. La vittima, persuasa dal falso consulente, di fronte al piccolo investimento richiesto (solitamente 250 euro) decide di

provare: le viene aperto un falso conto di trading su una falsa piattaforma, dove può seguire in ogni momento l'andamento degli investimenti e del mercato.

3 **Il truffatore a questo punto inizia a intrattenere con la vittima** una sorta di filo diretto che lo porta a contatti anche quotidiani, di svariate decine di minuti, dove, oltre a parlare e illustrare l'andamento dei mercati, cerca di intessere una falsa amicizia, abbandonandosi a confidenze e cercando confidenze nella vittima, che a quel punto inizia a vederlo sempre più come una persona di cui fidarsi, quasi un amico.

4 **Dopo qualche settimana, e dopo aver manipolato la falsa piattaforma di trading** in modo da far apparire alla vittima un forte ritorno di guadagno negli investimenti, il sedicente trader convince il malcapitato investitore che con un investimento maggiore i ritorni sarebbero ben più proficui. Questo è la fase più delicata e pericolosa: se la vittima cede alle richieste del trader, si innescherà un meccanismo che potrebbe portare la vittima ad avere perdite ingentissime. Se invece rifiuterà di alzare la soglia dell'investimento, il truffatore lascerà perdere e si renderà irreperibile (ma le perdite, almeno, saranno limitatissime).

5 **Se la vittima cede alle prospettive di facili guadagni**, il truffatore inizierà col far aprire a nome dell'investitore un conto / portafoglio (wallet) su piattaforme di compravendita di criptovalute (CoinBase, Binance, per fare alcuni esempi), sul quale saranno depositate le somme da investire. A tale scopo spesso fa installare sul device un software di controllo remoto come AnyDesk per "aiutare" l'investitore meno pratico nella compravendita della criptovaluta. In realtà guiderà la vittima a spostare il proprio denaro sul wallet aperto e da lì sposterà il denaro verso wallet anonimi, facendo apparire alla vittima che sono confluiti sul conto di trading (falso e manipolato)

6 **Il truffatore effettua false operazioni di trading**, mostrando la valenza degli investimenti effettuati che in brevissimo tempo avranno permesso di moltiplicare il capitale e sollecita il "cliente" a investire altro denaro. La vittima, visto il buon andamento delle operazioni, versa ulteriore denaro cadendo ulteriormente nella truffa.

7 **Quando la vittima chiede di ritirare o totalmente o parte dell'investimento** il truffatore mette in atto diverse strategie:

- Può invertire l'andamento dell'investimento mostrando una perdita, colmabile con ulteriore immissione di denaro e spingere la vittima a ulteriori esborsi;
- Oppure informa l'investitore che per disinvestire, deve prima pagare il capital gain (tasse sui guadagni).

8 **Quando il truffatore capisce che la vittima non investirà più nulla,** blocca ogni comunicazione e si rende irreperibile. **E' a questo punto che molte volte scatta una seconda truffa**: la vittima è contattata da sedicenti studi legali, oppure da sedicenti autorità monetarie che informano il malcapitato di essere in grado di far recuperare l'investimento dietro pagamento di una percentuale della somma investita. La vittima, ormai disperata per l'ingente perdita, si aggrappa a qualsiasi cosa che le possa dare la speranza di riavere il proprio capitale e purtroppo, a volte, versa altro denaro ai truffatori senza recuperare nulla.

COME DIFENDERSI

1 Diffidiamo delle pubblicità di investimenti che garantiscono guadagni immediati e sicuri: telefonate da prefissi esteri e da numeri sconosciuti che ci contattano per proporci investimenti vanno chiuse immediatamente senza lasciare alcuna possibilità all'interlocutore.

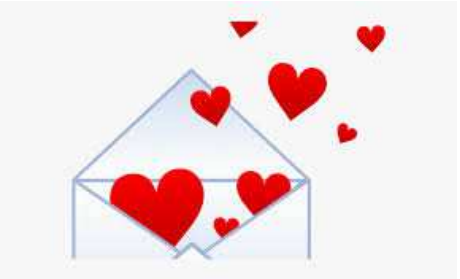
2 Gli investimenti vanno fatti tramite canali e piattaforme ufficiali: tutti gli istituti di credito hanno piattaforme di trading e i loro consulenti sono disponibili a seguirci qualora volessimo provare la strada del trading online. Prima di iniziare un investimento è bene consultarsi con persone competenti e preparate, che possiamo incontrare di persona. Questi truffatori non accetteranno mai di incontravi di persona. Anzi! Molte volte inviano falsi documenti di identità a testimonianza della loro esistenza: **non dimentichiamo mai che qualsiasi documento digitale può essere alterato, modificato, falsificato.**

3 Verificare sul sito della CONSOB (Autorità italiana per la vigilanza dei mercati finanziari) se la società che ci ha contattato è tra quelle che sono autorizzate ad operare in Italia.

4 Versamenti / bonifici su IBAN stranieri e investimenti all'estero "fai da te" dovrebbero metterci in allarme: a chi stiamo dando realmente il nostro denrao? A chi possiamo rivolgerci qualora volessimo ritirare quel denaro o far valere le nostre ragioni?

5 Non permettere a terze persone di poter utilizzare da remoto i nostri dispositivi attraverso programmi che ci viene chiesto di installare (es. AnyDesk). Questi programmi consentono a terze persone di "frugare" nei nostri dispositivi: potrebbero sottrarci altre informazioni delicate e usarle in modo illecito

La truffa sentimentale



Nota anche come **"Romance Scam",** è una forma di cyber-truffa che consiste nell'ottenere denaro dalla vittima facendo leva sul sentimento amoroso. Le vittime sono nella quasi totalità di sesso femminile. Le azioni del truffatore non si discostano molto da quelle adottate nella prima fase di relazione vera e sincera. A causa della grande distanza tra il truffatore e la vittima, la relazione sarà però portata avanti in modo virtuale, anche per molto tempo. Lo scopo è quello di ottenere la fiducia totale della vittima, la quale, per le attenzioni che riceve, si sente euforica e totalmente catturata e soggiogata dall'innamoramento e sente la necessità di quella relazione che, seppur virtuale, spera possa diventare reale

COME SI SVILUPPA

1 **Il truffatore crea un profilo falso solitamente su Facebook**, usando foto recuperate da un profilo reale il cui titolare è ignaro di tutto. In questo profilo crea una sua "trama" che solitamente si nutre di alcune caratteristiche particolari: è sempre straniero, di bella presenza, lavora per importanti enti governativi e non governativi (Esercito degli U.S.A, ONU, Medici Senza Frontiere….) e si trova in territori al alto rischio o teatri di guerra, in modo da far percepire alla vittima la necessità del suo aiuto e supporto per il costante pericolo che incorre la sua vita. Questo gli servirà per suscitare curiosità, fascino e apprensione nella vittima. Solitamente dice di essere vedovo e di avere figli che ha lasciato al suo Paese d'origine, facendo leva sul sentimento umano e materno della vittima.

2 **Il truffatore entra in contatto con la potenziale vittima,** studiandone il profilo. A quel punto cerca il primo contatto sempre tramite Facebook, per poi arrivare a scambiarsi il numero di telefono e proseguire le conversazioni con Whatsapp. Lo scambio del numero di telefono fa percepire

alla vittima una certa confidenza fino a ritenere più veritiera la relazione che si sviluppa sia tramite Whatsapp sia tramite Facebook. Le conversazioni si fanno sempre più fitte e possono andare avanti per settimane, a volte per mesi: il truffatore si lascia andare a false confidenze sulla sua vita, sul suo lavoro, sui figli. Invia foto, poesie, usa parole dolci e suadenti, fino a far nascere nella vittima un sentimento amoroso.

3 **Il truffatore a questo punto porta a termine la truffa** facendo leva sul lato più sensibile che ha manifestato la vittima. Si possono avere diversi scenari, ma i più riscontrati sono la leva sul sentimento materno della vittima e la leva sul desiderio di incontrarsi. La richiesta di denaro diventa via via sempre più ingente, fino all'esborso di parecchie migliaia di euro. Il denaro è sempre richiesto tramite bonifici all'estero, oppure tramite Money transfer quali MoneyGram o Western Union.

4 A volte il truffatore chiede l'invio di carte prepagate per facilitare l'accredito ed il prelievo del denaro, invitando la vittima a intestarsi tali titoli di credito e a trasmetterli a indirizzi solitamente dell'Africa. Questo è molto rischioso perchè su quella carta di credito potrebbero essere veicolati proventi da altri reati, con conseguenze anche penali per il titolare / intestatario.

COME DIFENDERSI

1 Le richieste di amicizia possono nascondere insidie perché non sappiamo chi realmente c'è dall'altro lato dello schermo. Diffidiamo dalle richieste di amicizie di persone che dichiarano di essere residenti all'estero: è difficile capire o verificare quanto ci stanno dicendo.

2 Diffidiamo dalle richieste di amicizia che provengono da profili di persone che sembrano perfette: di bell'aspetto, con un lavoro di prestigio, in giro per il mondo, vedovo o comunque single: sono tutte caratteristiche che ci possono piacere e potrebbero rendere più interessante una persona e il truffatore lo sa!

3 Se decidiamo di accettare l'amicizia il rapporto deve rimanere quello che può esserci tra due semplici conoscenti virtuali: si parla, si dialoga, **ma non si forniscono mai informazioni personali.**

4 Non dobbiamo credere / cedere alle lusinghe o ai complimenti: possono avere sempre un secondo fine, che purtroppo non sapremo mai fino a quando sarà troppo tardi: meglio non rischiare con qualcuno che neppure sappiamo chi sia e mantenere sempre alta la soglia della diffidenza e del sospetto.

5 Non cediamo alle richieste di foto o video intimi!! Potrebbero essere divulgati e usati impropriamente a scopi ricattatori

La truffa immobiliare

Sarà capitato a tutti di organizzare le vacanze e magari cercare un appartamento in affitto. Oppure avere la necessità di prendere in affitto un appartamento perché i figli stanno frequentando l'università in una città lontana da casa. Ma con la popolarità delle piattaforme che offrono il servizio di locazione di immobili, è aumentato notevolmente anche il rischio di imbattersi in truffe che prendono di mira gli utenti che per la prima volta si cimentano con la prenotazione fai da te della vacanza. La Polizia Postale, tra l'altro, in collaborazione con Airbnb, ormai da alcuni anni ha avviato una campagna di sensibilizzazione per questa tipologia di truffe.

COME SI SVILUPPA

1 **Il truffatore crea cerca online una inserizione di una casa in affitto**, preleva le foto dell'abitazione pubblicate dal reale proprietario e crea una falsa inserzione di affitto. L'inserzione può essere fatta su portali dedicati, quali Airbnb, oppure su portali di compravendita, quale "subito.it", per esempio.

2 **Il truffatore attende la potenziale vittima,** e una volta entrato in contatto fornisce il suo recapito telefonico per portare la conversazione su Whatsapp. La trattativa prevede sempre una caparra e il saldo alla consegna delle chiavi. (Attenzione ai numeri esteri, perché sono uno dei segnali della potenziale truffa!)

3 **Il truffatore porta a termine la truffa,** fornendo l'IBAN per il bonifico (spesso si tratta di IBAN stranieri) oppure una carta ricaricabile sulla quale effettuare il versamento concordato. Quando il locatario si reca sul posto per ricevere le chiavi dell'abitazione si rende conto che l'abitazione non è in affitto, oppure che l'abitazione non esiste proprio!!.

COME DIFENDERSI

1 Controllate le foto dell'abitazione e cercatele tramite Google con l'apposito applicativo alla pagina **https://www.google.com/imghp?hl=it_it**: questo vi consentirà di vedere se quelle immagini sono state pubblicate da qualche parte, facendo scattare in voi un campanello d'allarme.

2 Controllate su Google Maps la posizione della casa offerta in affitto: poterete verificare con l'applicativo Google Street View l'esistenza o meno dell'abitazione. Molte volte, nelle nostre indagini, abbiamo verificato l'inesistenza addirittura della casa all'indirizzo indicato dal truffatore!

3 Se avrete a che fare con un annuncio su Airbnb, attenzione alle pagine dove compare l'annuncio: tutte le pagine di Airbnb hanno l'indirizzo che inizia con **www.airbnb.it** o **.com**, e un numero dopo la parola 'rooms', come nell'esempio: **www.airbnb.it/rooms/30728582**. Indirizzi più complicati o con una struttura diversa devono insospettirvi.

4 Diffidate dai numeri di telefono esteri: la scusa che il truffatore adotta è che si trova all'estero e quindi affitta la sua abitazione in Italia. Diffidate anche dalla richiesta di bonifico verso IBAN esteri se state affittando un'abitazione in Italia. Piuttosto cercate un'altra offerta.

5 Non fidatevi se il locatore vi manda dei documenti d'identità a testimonianza della sua reale identità : molte volte sono risultati falsi, modificati digitalmente. Altre volte appartenevano ad altre vittime che a loro volta li avevano mandati per concludere le pratiche del falso affitto.

La truffa del "telefono rotto"

E' l'ultima delle truffe e consiste nel simularsi un famigliare della vittima, facendole credere di avere difficoltà col telefono, spingendola a fare una ricarica su una carta prepagata o un bonifico adducendo varie scuse.

COME SI SVILUPPA

1 Il truffatore invia un messaggio tramite WhatsApp alla vittima, dicendo di essere XXX (potrebbe essere un figlio, un nipote, un coniuge, un congiunto), di avere il telefono rotto, di avere cambiato SIM, ma ha problemi con le chiamate

2 A quel punto per rendere più credibile la situazione manda alcuni messaggi vocali, sempre tramite WhatsApp, il cui contenuto riproduce solo rumori e suoni fastidiosi, tali da indurre la vittima a credere che effettivamente ci siano problemi col telefono.

3 Dopo aver convinto la vittima, il truffatore dice di avere una urgenza: effettuare un pagamento a favore di una carta ricaricabile o di un IBAN per svariati motivi (scadenza di un prestito, finanziamento, tasse, ecc.) e di non potervi provvedere proprio perché il suo telefono è guasto ed è impossibilitato a usare i servizi di home banking. Chiede quindi alla vittima se può provvedere al pagamento in fretta, fornendo le coordinate verso cui fare il versamento. La vittima farà un pagamento verso il truffatore, scoprendo solo dopo di essere stata ingannata.

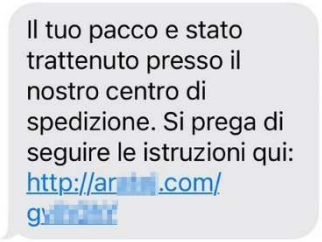
COME DIFENDERSI

1 La cosa più semplice da fare è chiamare telefonicamente il vero numero del famigliare "simulato" dal truffatore. Se risponde abbiamo smascherato il tentativo di truffa.

2 Se per qualsiasi ragione non rispondesse, non facciamoci prendere dalla fretta o dal panico: con calma contattiamo qualcuno che possa avere informazioni maggiori (potrebbe essere la nuora o il genero in caso di figlio/figlia o nipoti), ma non facciamo mai quello che ci chiede tramite Whatsapp. Piuttosto basta fare una telefonata anche alle Forze dell'Ordine per capire se la situazione in atto sia una potenziale truffa.

La truffa del falso pacco

E' una truffa che conta una recrudescenza soprattutto nei periodi prenatalizi, proprio per i numerosi acquisti che si fanno online.
Consiste nel ricevere un messaggio che sembra provenire da un corriere e che ci informa di problemi nella consegna del pacco a noi destinato



COME SI SVILUPPA

1 Riceviamo un messaggio che sembra provenire da un corriere che ci invita a cliccare sul link per risolvere un problema con il pacco a noi diretto.

2 Le frasi più usate in questo tipo di truffa sono le seguenti

- Il tuo pacco è stato trattenuto presso il nostro centro di spedizione. Si prega di seguire le istruzioni qui: *(viene indicato un link)*
- Salve, purtroppo non siamo riusciti a consegnare il suo pacco, la preghiamo di controllare qui: *(viene indicato un link)*
- Il tuo pacco potrebbe essere in ritardo, conferma la consegna qui: *(viene indicato un link)*
- Ciao, il tuo pacco e in attesa di impostare le preferenze di consegna. Clicca qui: *(viene indicato un link)*
- Abbiamo un pacco per lei. Per programmare la consegna clicchi qui: *(viene indicato un link)*

3 Cliccando sul link si apre una pagina che rispecchia fedelmente quella del corriere, ma in realtà è falsa; nella pagina ci viene detto che è necessario pagare 2 euro (o comunque una piccolissima cifra) per procedere nella consegna e ci chiede il pagamento tramite carta di credito.

4 Inseriti i codici della carta di credito verranno decurtati i due euro, ma si attiveranno abbonamenti a servizi di siti esteri, non richiesti, che porteranno addebiti mensili anche di 50 euro.

5 Ogni tentativo di bloccare l'abbonamento risulta sempre vano e l'unica soluzione, oltre a fare denuncia, è quella di bloccare la carta di credito e attivarne un'altra

COME DIFENDERSI

1 Un primo controllo può riguardare il link: il collegamento solitamente non ha la certificazione SSL (non inizia con "https", ma con "http"). E' un primo segnale di una potenziale truffa.

2 Se attendiamo un pacco e abbiamo il codice tracking controlliamo direttamente sul sito del corriere dov'è il pacco. Nel dubbio, prima di aprire il link chiamiamo telefonicamente il corriere per avere delucidazioni.

3 **Ma soprattutto: non cliccare mai sul link!**

Il furto d'identità

Uno dei rischi derivanti dall'uso di internet è la possibilità di vedersi sottrarre la propria identità digitale, che possiamo definire come l'insieme di informazioni che identificano nel mondo virtuale una persona. Possono essere informazioni certificate a cui è attribuibile con certezza una identità fisica (per esempio SPID, PEC, firma digitale) oppure informazioni fornite dalla persona all'atto della creazione di un account / profilo.
Sottrazione di profili social, quali Whatsapp, Instagram, Facebook sono all'ordine del giorno, per non parlare della creazione di falsi profili usando nostre informazioni che abbiamo affidato alla rete, quali il nostro nome e cognome, numero di telefono, indirizzo mail, foto, video ecc.
In molti casi di furto d'identità intervengono tecniche ingannevoli di phishing.

COME SI SVILUPPA

1 **SOTTRAZIONE DI UN PROFILO SOCIAL**: il più delle volte si riceve un messaggio che proviene da una persona che abbiamo nelle nostre amicizie o nella rubrica, a sua volta vittima di un furto d'identità. Il messaggio ci invita a cliccare sul link per vari motivi (partecipazione a un sondaggio, per esempio). In realtà il link inviato è un link di convalida trasmesso dal social sotto attacco: qualcuno sta già tentando di violare il profilo e sta cambiando la password. Cliccare sul link vuol dire confermare al social che siete voi a richiedere il cambio password e conseguentemente state dando accesso all'hacker. L'hacker, una volta all'interno del profilo, cambia la password, la mail e imposta un'autenticazione a doppio fattore inserendo il suo numero di telefono. A quel punto per voi è impossibile accedere. Una volta all'interno usa il profilo nei modi più disparati: manda messaggi ai vostri

contatti, usa il profilo per veicolare messaggi d'odio, lo usa per accrescere i follower di influencer, e ultimamente si è rilevata anche la divulgazione di materiale pedopornografico

2 **CREAZIONE DI UN FALSO PROFILO SOCIAL**: se le impostazioni riguardo alla privacy dei nostri profili non sono configurate correttamente, è possibile per chiunque guardarne i contenuti (foto, video, post, commenti) e da qui acquisire informazioni e immagini da utilizzare per la creazione di profili falsi il più verosimili possibili. Ma attenzione: a volte succede che anche chi abbiamo nelle amicizie possa agire scorrettamente, prendere informazioni e creare un profilo falso. Ma a quale scopo creare un profilo falso? Per invidia verso la vittima, per denigrarla, offenderla, diffamarla…i motivi sono molti, ma mai piacevoli.

3 **ACQUISIZIONE FRAUDOLENTA DI DATI PERSONALI**: frequentemente accade che giungano messaggi SMS o mail che sembrano provenire da pubbliche amministrazioni, quali l'INPS per esempio. Nel caso dell'INPS, il contenuto del messaggio è vario e riporta a erogazione di assegni famigliari, a verifiche di posizioni previdenziali, ad aggiornamento dell'importo della pensione. Al solito, nel messaggio, è presente un link che, se cliccato, apre una pagina identica a quella dell'INPS e invita a inviare copia della carta d'identità, del codice fiscale e di un selfie in cui si esibisce la carta d'identità a riprova dell'identità. Nessuna pubblica amministrazione avanza richieste di documenti in quel modo, ma bisogna pensare che quella tipologia di documenti è richiesta per l'apertura di conti correnti online

4 **APERTURA DI CONTI CORRENTI ONLINE**: se inopportunamente abbiamo fornito copia della carta d'identità, del codice fiscale e di un selfie in cui si esibisce la carta d'identità a riprova dell'identità, è probabile che ci potremmo trovare con dei conti correnti aperti online e usati in modo illecito. Se ciò accadrà dovrà essere presenta immediatamente una denuncia di disconoscimento. E' opportuno che si formalizzi una denuncia anche quando siamo ingannati da falsi siti della Pubblica Amministrazione: questo consente alla Polizia Postale di intervenire immediatamente per far rimuovere il falso sito e tutelare il malcapitato da futuri situazioni illegali.

COME DIFENDERSI

1 Attenti ai messaggi che contengono link, anche se provengono da persone che conosciamo: mai cliccare distrattamente. Se abbiamo cliccato, l'unica possibilità per rientrare in possesso del profilo è seguire la procedura messa a disposizione dal social e per esperienza, la maggior parte delle volte non va a buon fine.

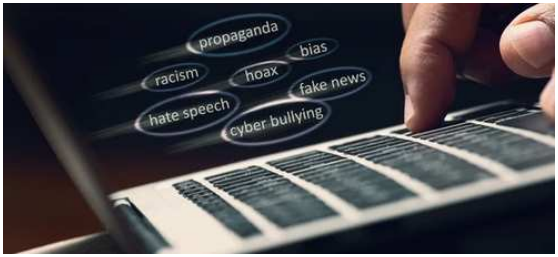
2 Evitare di pubblicare immagini che possano fornire informazioni dettagliate sulla nostra abitazione, residenza, abitudini di vita. Attenzione anche alla geolocalizzazione allorquando scattiamo foto.

3 Mai consegnare / caricare su portali o siti documenti d'identità se non siamo certi che ce ne sia effettivamente bisogno. Le Pubbliche amministrazioni non chiedono di inserire documenti di identità sui loro portali, perché loro hanno già i nostri dati identificativi.

4 Se è un privato che non conosciamo a chiederci i documenti di identità, soprattutto nel corso di una trattativa commerciale, rifiutiamo: stiamo consegnando dei documenti che potrebbero essere usati a nostro discapito.

Diffamazione e crimini d'odio

La diffamazione è un reato previsto e punito dall'articolo 595 del codice penale, che recita:



Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro.
Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro.
Se l'offesa è recata col mezzo della stampa con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro.
Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate.

La diffamazione, quindi, consiste nell'offendere la reputazione altrui o l'attribuire un fatto determinato tale da lederne la reputazione. E' un reato che con l'avvento dei social ha avuto un notevole incremento, perché spesso le persone si lasciano coinvolgere emotivamente nelle discussione nate sotto i post e perdono il lume della ragione, arrivando a offendere, denigrare e attaccare gli altri che manifestano idee o punti di vista diversi.

La commissione di questo reato attraverso l'uso dei social è considerata quasi sempre come un'aggravante perché le dichiarazioni / post / commenti che ledono la reputazione e l'onore della persona presa di mira è vista e letta da un numero elevato di persone, a volte anche migliaia.

Quello che sovente definiamo o giustifichiamo come una "opinione" in realtà configura vere e proprie diffamazioni, passibili di querela.

Analogo discorso va fatto per gli **haters** e per gli **hate speech**.

Mentre i primi sono fomentatori di discussioni accese, rivolgendo offese e denigrazioni alla persona presa di mira, con gli hate speech ci troviamo di fronte a veri e propri **"incitamenti all'odio" o "discorsi d'odio", che rischiano di provocare reazioni violente, a catena.**

Le incitazioni all'odio sono severamente punite dalla legge (articolo 604 bis c.p. - Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa) e sono state oggetto di raccomandazione anche da parte della Unione Europea con la "**Raccomandazione n. 15/2015 della commissione contro il razzismo e l'intolleranza (Ecri) del consiglio d'Europa"**, che dice:
"Si intende per discorso dell'odio il fatto di fomentare, promuovere o incoraggiare, sotto qualsiasi forma, la denigrazione, l'odio o la diffamazione nei confronti di una persona o di un gruppo, nonché il fatto di sottoporre a soprusi, insulti, stereotipi negativi, stigmatizzazione o minacce una persona o un gruppo e la giustificazione di tutte queste forme o espressioni di odio testé citate, sulla base della "razza", del colore della pelle, dell'ascendenza, dell'origine nazionale o etnica, dell'età, dell'handicap, della lingua, della religione o delle convinzioni, del sesso, del genere, dell'identità di genere, dell'orientamento sessuale e di altre caratteristiche o stato personale".

La partecipazione a discussioni sui social, nei forum, nei blog dovrebbe sempre essere ponderata e dettata dall'educazione e dal buon senso, elementi che non perdiamo mai di vista nella vita reale.

Ma l'anonimato che a volte offre la rete, concepita un po' come "terra di nessuno" da parte di molti utenti, la sensazione di essere intoccabili e non identificabili dovuta alla percezione di distanza temporale e spaziale, spesso lascia emergere il peggio di noi, inducendoci in quella disinibizione del comportamento online che ci trasforma in un troll, o peggio in un hater, portandoci alla commissione di reati (in psicologia moderna è definito "effetto Gige", mutuato dal mito di Gige di Platone.), a volta senza nemmeno rendercene conto.

GLOSSARIO

Le pagine che seguono vogliono essere una piccola guida, sicuramente non esaustiva, sulla terminologia e sugli strumenti attualmente più comuni nel mondo digitale.

ACCOUNT / PROFILO

Possiamo definirlo come uno spazio virtuale riservato, creato da un utente previa registrazione e inserimento di dati personali più o meno dettagliati (nome, cognome, luogo e data di nascita, mail, numero di telefono) su una piattaforma che offre servizi, il cui successivo accesso è subordinato alla conoscenza delle credenziali. Abbiamo, per esempio, account di posta elettronica, di home banking oppure profili di Instagram o di Facebook.

AUTENTICAZIONE A DOPPIO FATTORE SICUREZZA DI UN ACCOUNT / PROFILO

La sicurezza di un account o di un profilo (profilo social, account di Home Banking, casella di posta elettronica, account su siti della pubblica amministrazione, ecc.) dipende sempre dall'utente. La regola base è quella di utilizzare password complesse, diverse per ogni account / profilo.
Considerata però l'evoluzione delle tecniche criminali per impossessarsi delle password, si è giunti a utilizzare quella che è tecnicamente chiamata autenticazione a doppio fattore (2FA Two-factor authentication).
Alla base di questa tecnica ci sono tre fattori: il fattore "conoscenza", il fattore "possesso"; il fattore "intrinseco".

- **Il fattore "conoscenza"** è un qualcosa che solo l'utente dovrebbe conoscere (per esempio la password, oppure il PIN della carta di credito o del telefono).
- **Il fattore "possesso"** è qualcosa di fisico che solo l'utente possiede (per esempio la SIM dell'utenza telefonica, oppure la carta di credito, oppure la Carta d'Identità Elettronica).
- **Il fattore "intrinseco"**, infine, è qualcosa che rende unico l'utente. In questo fattore rientrano tutti i dati biometrici, quali il riconoscimento del viso, l'iride dell'occhio, l'impronta digitale.

L'autenticazione a doppio fattore, quindi, utilizza e richiede, per l'accesso a un account digitale (profilo social, home banking, pubblica amministrazione, ecc.) due dei fattori da fornire contemporaneamente, garantendo in tal modo un grado di sicurezza elevato rispetto alla tradizionale password. Per esempio, per accedere ai moderni smartphone, può esser impostato il PIN (fattore di "conoscenza") e una volta convalidato potrebbe essere richiesta l'impronta

digitale (fattore "intrinseco"). Ulteriore esempio è l'uso delle carte di credito con PIN: il PIN, abbiamo visto, è un fattore di "conoscenza", mentre la carta di credito diventa il fattore di "possesso" (diverso da quando bastava "strisciare" la carta di credito per convalidare il pagamento). E ancora: per accedere all'home banking può essere richiesta la password (fattore di "conoscenza") e la digitazione di un codice OTP che giunge sulla vostra utenza che avrete certificato in banca (fattore di "possesso"), oppure potrete certificare il telefono (fattore di "possesso") e autenticarvi con l'impronta digitale (fattore "intrinseco).

BACKUP

Il backup è la copia di sicurezza delle informazioni memorizzate su un dispositivo che ci consente, in caso di perdita di dati o malfunzionamento del sistema, di ripristinarli. Logicamente saranno ripristinati solo i dati sottoposti a backup. Ecco, quindi, la necessità di impostare un backup automatico giornaliero, proprio per non perdere alcun dato. Si consigliano sempre backup di dati importanti. Anche le nostre foto dovrebbero essere sottoposte a backup, anche direttamente al cloud: questo eviterà di perdere i ricordi in caso di guasto irreparabile dello smartphone.

BITCOIN

Una delle criptovalute più note e diffuse nel mondo, creata / inventata nel 2019.

Maggiori informazioni sul sito:
https://www.borsaitaliana.it/notizie/sotto-la-lente/bitcoin-172.htm

CARTA PREPAGATA

La carta prepagata è una carta di credito a tutti gli effetti, che si utilizza allo stesso modo, ma che non ha una disponibilità permanente di denaro.

Il denaro, infatti, biosogna accreditarlo di volta in volta, mediante le cosiddette ricariche.
E' lo strumento consigliato per effettuare acquisti in Internet perché, se clonata, impedirà ingenti perdite. Oggi tutti gli istituti di credito hanno a disposizione carte prepagate e il loro costo è irrisorio. Tra le più conosciute vi sono le Postepay.

C.I.E.

(Carta d'Identità Elettronica). Consente, come lo SPID, di autenticarsi digitalmente con l'uso dell'App CieID sui siti della pubblica amministrazione. Inoltre, può essere utilizzata come firma digitale per autenticare documenti digitali tramite l'App Cie Sign

Maggiori informazioni sul sito:
https://www.cartaidentita.interno.gov.it

CLOUD

Il cloud è un servizio che consente agli utenti di memorizzare propri file su server remoti e potervi accedere in qualsiasi momento da qualsiasi device purchè in possesso di nome utente e password.
Tra i cloud più comuni citiamo Google Drive, iCloud, Dropbox.
Anche Facebook o Instagram possono essere considerati dei cloud perché l'accesso da dispositivi diversi ci consente di avere sempre le stesse identiche informazioni da noi pubblicate / condivise, quali foto, video, commenti…

COOKIE

Significa "biscotto" e mutua il suo nome dai biscotti della fortuna orientali, al cui interno è nascosto un biglietto con frasi.
Analogamente, i cookie sono piccoli file memorizzati sul device durante la nostra navigazione nei vari siti, al cui interno sono salvati dati utili alla sessione di navigazione (come le preferenze sull'aspetto grafico o la lingua del sito).
Permettono, però, anche di tracciare la navigazione per veicolare pubblicità mirata in base alle preferenze dell'utente. Sono molto delicati per quanto riguarda la nostra privacy, tanto è vero che ogni sito è obbligato a chiedere il consenso dell'utente prima di poter salvare, tramite browser, cookie sul device.

CREDENZIALI

Sono i dati che consento l'accesso a un account.
Di solito si identificano nel nome utente e nella password, che possono / devono essere scelti dall'utente

CRIPTOVALUTA

Le criptovalute sono le cosiddette "valute virtuali", tra le quali la più famosa è il Bitcoin (BTC). Esistono anche altre criptovalute, quali per esempio Bitcoin l'Ethereum (ETH), la Tether (USDT), la Binance Coin (BNB).
Il termine si compone di due parole: cripto (nascosto) e valuta, ovvero valuta 'nascosta', cioè che è visibile/utilizzabile solo conoscendo un determinato codice informatico.
Le criptovalute non esistono fisicamente (per questo viene definita 'virtuale'), ma si genera e si scambia esclusivamente per via telematica. Non è possibile trovare in circolazione criptovaluta in formato cartaceo o metallico.
Si tenga però presente che:

- le monete virtuali **NON HANNO** corso legale nella quasi totalità dei Paesi del mondo
- l'accettazione come mezzo di pagamento è su base volontaria

- non sono regolate da enti centrali governativi
- solitamente sono emesse e controllate dall'ente emittente secondo regole proprie a cui i membri della comunità di riferimento accettano di aderire;

Maggiori informazioni sul sito
https://www.consob.it/web/investor-education/criptovalute

DARK WEB

Definito anche come la parte oscura di Internet, per essere fruito necessita di appositi software. Balza spesso alla cronaca perché molti utenti lo usano per commettere fatti / azioni illegali.

DEEPFAKE

I deepfake sono foto, video e audio che partendo da contenuti digitali originali, tramite appositi software, vengono creati artificiosamente in modo realistico. Tramite questi software è possibile modificare volti, movimenti, parole. Si può, per esempio, dare movimento e voce a una semplice foto. Il pericolo riguardo alla privacy è notevole, tanto è vero che anche il Garante della Privacy è intervenuto sull'argomento.

Per scaricare il PDF del vademecum del Garante della Privacy inquadrare con lo smartphone

DEVICE

Dispositivo. Possiamo ricomprendere, in questo termine, il PC, lo smartphone, il tablet….

FAKENEWS

Notizie false e fuorvianti divulgate soprattutto tramite i media digitali per i motivi più disparati, ma con notevole peso quando si tratta di argomenti che coinvolgono aspetti politici o economici. Sono finalizzate a gettare discredito su un determinato argomento suscitando nel lettore sdegno e clamore e spingendo la parte coinvolta alla dimostrazione del contrario.

FEEDBACK

I feedback sono commenti, opinioni usati soprattutto a seguito della fruizione di servizi in internet. Possiamo trovare feedback, oltre nei siti che offrono qualsiasi tipo di servizio, anche sui siti di vendite online verso utenti che hanno pubblicato inserzioni di vendita. E' importante, prima di effettuare un acquisto, leggere e cercare i feedback, perché spesso possono rivelare la natura truffaldina del sito o del singolo venditore.

FIRMA DIGITALE

E' il sistema che, previa identificazione e autenticazione di una persona, consente a quest'ultima di autenticare un documento digitale attraverso alcuni strumenti che sono:

- smart card o dispositivo usb con certificato digitale di sottoscrizione rilasciato da un certificatore accreditato previa identificazione del richiedente;
- lettore di smart card;
- software di firma digitale messo a disposizione gratuitamente dal certificatore.

FOLLOWER

Usato soprattutto nell'ambito dei social, indica un utente che decide di seguire un altro iscritto e di riceverne, quindi, contenuti e aggiornamenti. Di rilevanza nei social è il numero dei follower, soprattutto per gli influencer, in quanto maggiore è loro numero, maggiori sono i ritorni economici a seguito della visione degli inserti pubblicitari nei video e nelle storie create.

GEOLOCALIZZAZIONE

Gli smartphone sono dotati di GPS che consente l'identificazione della posizione geografica nel mondo reale mediante diverse applicazioni. Molte app, per funzionare, richiedono che il servizio di geolocalizzazione sia attivo e questo lo si può fare autonomamente nelle impostazioni del telefono. La geolocalizzazione è sfruttata anche per veicolare pubblicità mirata della zona in cui ci si trova. Può essere anche registrata durante gli scatti fotografici, consentendo a chi ha conoscenze informatiche di stabilire con precisione l'ubicazione dello scatto. E' pertanto importante prestare attenzione che la geolocalizzazione sia disattivata e che non sia stato dato il consenso alla sua registrazione quando si scattano foto soprattutto in abitazioni private, perché rivelerebbe la posizione esatta.

G.D.P.R.

Frequentemente ci saremo imbattuti in questa sigla. E' l'acronimo di General Data Protection Regulation (Regolamento per la protezione dei dati personali) ed è il regolamento europeo che tutela la nostra privacy. In Italia la privacy è

tutelata dal Decreto legislativo 30 giugno 2003, n. 196 e la sua applicazione è affidata al Garante per la Privacy.

Maggiori informazioni sul sito
https://www.garanteprivacy.it

HATER

Detti anche leoni da tastiera possono essere definiti come persone che usano la rete, e in particolare i social network, per esprimere odio (hate in inglese) o per incitare all'odio verso qualcuno o qualcosa o per denigrare, disprezzare, diffamare e scatenare discussioni distruttive. A volte è indicato anche come acronimo di Having Anger Towards Everyone Reaching Success (avere rabbia verso chiunque raggiunge il successo)

HATE SPEECH

Termine inglese che indica un'offesa rivolta a una persona o a un gruppo di persone basata su una discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, ecc.)

HOME BANKING

E' il sistema adottato da tutti gli istituti di credito (Poste Italiane comprese) che consente, ai titolari di conto corrente o di carta di credito, di fruire virtualmente, da un device e tramite apposite APP, della quasi totalità dei servizi offerti tramite sportello bancario.
Per fruire dell'home banking bisogna dapprima abilitarsi di persona presso il proprio istituto di credito, che provvederà a creare le credenziali necessarie all'accesso, e poi installare l'APP indicata dalla banca.

ATTENZIONE: **nessun istituto di credito invia messaggi con LINK su cui cliccare**. Se dovesse giungere un messaggio con un link, che si incasella nelle chat della vostra banca / carta di credito, allora siete in presenza di un tentativo

di phishing, ovvero di un tentativo di truffa!!!! L'importante è non cliccare sul link ed eliminare il messaggio!!! Il vostro device non è compromesso solo per avere ricevuto il messaggio!!!

INFLUENCER

Personaggio popolare, anche e soprattutto nei social network, in generale molto seguito dai media, in grado di influenzare i comportamenti e le scelte di un determinato pubblico. Sono utilizzati, dietro compenso, da qualunque azienda intenzionata a promuove i propri prodotti proprio per la capacità dell'influencer di raggiungere un determinato target di pubblico.

OTP

(One Time Password). E' una password usa e getta (o temporanea) valida solo per una singola sessione di accesso o una transazione. E' usata soprattutto nei sistemi di home banking e serve per autenticare una transazione o un accesso all'account di home banking (nell'autenticazione a doppio fattore è un fattore di "possesso" perché l'OTP è inviata a un numero di telefono precedentemente verificato dall'istituto di credito).

PASSWORD

E' il codice d'accesso a un account / profilo. Alcune regole per rendere sicura una password:

1) Deve avere più di 8 caratteri e contenere almeno un numero, una lettera maiuscola, una lettera minuscola e un carattere speciale.
2) Dovrebbe essere cambiate con una cadenza di circa 60-90 giorni massimo
3) Una password usata non dovrebbe essere riutilizzata
4) Ogni account / profilo deve avere una sua password: usare una password uguale per più account / profili ci espone a maggiori violazioni

5) La password non dovrebbe essere rivelata a nessuno estraneo all'ambito famigliare.

PEC

(Posta Elettronica Certificata). E' una particolare tipologia di posta elettronica che fornisce agli utenti la certezza a valore legale dell'invio e della consegna (o mancata consegna) delle email al destinatario.
Le comunicazioni che avvengo tra due caselle PEC hanno lo stesso valore legale della raccomandata con ricevuta di ritorno.

PHISHING

E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica o SMS ingannevoli.
Con il phishing il malintenzionato, nascondendosi dietro a un falso mittente affidabile, cerca di convincere la vittima a fornire informazioni riservate, quali password, codici di accesso a home banking, numeri di carta di credito ecc. La tecnica è usata per violare account in tutti gli ambiti: home banking, caselle di posta elettronica, profili social, profili Whatsapp ecc..

Queste le tecniche di phishing più comuni:

1) **Spear phishing**: prende di mira un gruppo o una tipologia specifica di individui. La vittima è studiata sui social al fine di inviare false comunicazioni molto personalizzate. E' usato soprattutto per penetrare realizzare attacchi mirati, soprattutto verso aziende.
2) **Whaling**: sempre una tecnica rivolta al singolo individuo, ma in questo caso il bersaglio è sempre qualcuno di molto rilevante per l'azienda (l'Amministratore, il titolare, ecc.)
3) **Pharming:** Con questa tecnica la vittima è rimandata, spesso anche senza cliccare su nessun link, verso un sito web falso che riproduce esattamente quello vero (per esempio il sito della nostra banca o il sito del gestore della nostra casella di posta elettronica). Questa tecnica prende di mira o il computer dell'utente o i server DNS degli operatori.

4) **Deceptive phishing** (phishing ingannevole): è il phishing più comune. In questo caso il criminale invia a pioggia migliaia di mail o messaggi a elenchi di contatti ottenuti in modo fraudolento. I messaggi sembrano provenire da un istituto di credito e non importa se molti dei destinatari non hanno rapporti con quell'istituto di credito: sicuramente qualcuno sarà cliente e tra questi qualcuno, purtroppo, cadrà nell'inganno.
5) **Smishing**: è un attacco che utilizza i messaggi di testo o SMS. Una tecnica di smishing consiste nell'inviare a un telefono cellulare un SMS che sembra provenire dalla propria banca, contenente un collegamento cliccabile. Il messaggio cerca di creare allarme nella vittima affermando che il conto è compromesso e che è necessario rispondere immediatamente, inserendo dati specifici. Ottenute le informazioni, acquisisce il controllo del conto bancario.
6) **Vishing**: analogo allo smishing, solo che in questo caso il phisdhing è portato a termine con una chiamata vocale. Le persone sembrano effettivamente operatori dell'istituto di credito perché sono preparati e sanno praticamente tutto.

QR CODE

E' una specie di codice a barre, composto da moduli neri disposti all'interno di uno schema bianco di forma quadrata, usato per memorizzare informazioni destinate a essere lette tramite un apposito lettore ottico o anche smartphone

Inquadrare con lo Smartphone per leggere i contatti della Polizia Postale di Cremona

RAMSOWARE VIRUS

E' un tipo di malware che, dopo aver infettato il device, cripta i file dell'utente (foto, video, documenti) rendendoli inaccessibili e richiedendo un riscatto (*ransom* in inglese) per rimuovere la codifica. Bisogna sempre evitare di cliccare su allegati provenienti da mail sconosciute, perché spesso è lì che si nascondono i virus informatici.

SPID

(Sistema Pubblico di Identità Digitale). Consente di accedere ai servizi online della Pubblica Amministrazione (INPS, CATASTO, AGENZIA DELLE ENTRATE, FASCICOLO SANITARIO PERSONALE, ECC.) e dei privati aderenti. Per attivarlo è necessario avere a disposizione:

1) un documento italiano in corso di validità (carta di identità, patente, passaporto);
2) la tessera sanitaria (o tesserino codice fiscale, o il certificato di attribuzione di uno dei due);
3) un indirizzo e-mail e un numero di cellulare.

La sua attivazione può avvenire online oppure presso gli uffici di uno degli operatori autorizzati (per esempio Poste Italiane)

Maggiori informazioni sul sito:
https://www.spid.gov.it

SPOOFING

In informatica, manipolazione dei dati trasmessi in una rete telematica, consistente nella falsificazione del dato visibile (indirizzo IP, user name, account, numero telefonico, ecc.) per rendere irriconoscibile la sorgente.

WALLET

Il wallet è un portafoglio elettronico / digitale usato obbligatoriamente per la custodia delle criptovalute. Per accedere al wallet è necessaria la digitazione di una password e siccome per molti di questi wallet non c'è un'assistenza clienti, la perdita della password equivale alla perdita della criptovaluta là custodita.

TROJAN

Un "trojan" è un tipo di malware, che, alla stregua del famoso cavallo di Troia, è nascosto all'interno di altro applicativo. L'utente, eseguendo o installando l'applicativo, attiva inconsapevolmente anche il codice del trojan con conseguente compromissione del device. I trojan sono in grado di catturare codici di carte di credito, password oppure consentire da remoto il controllo del device.

TROLL

Nel gergo di Internet è colui che all'interno di una discussione virtuale invia messaggi di disturbo e fuori tema, irritando i partecipanti.

CONTATTI

S.O.S.C.

Sezione Operativa per la Sicurezza Cibernetica
Polizia Postale

Cremona, Via Verdi 1
Tel. 0372 593 588
Mail: sez.poliziapostale.cr@poliziadistato.it
PEC: dipps502.0400@pecps.poliziadistato.it

Link Istituzionali

www.poliziadistato.it
www.commissariatodips.it
https://it-it.facebook.com/AgenteLisa
https://www.facebook.com/unavitadasocial

Polizia di Stato
Sezione Operativa per la Sicurezza Cibernetica – Polizia Postale
Cremona Via Verdi 1

Stampato da:
Tipolitografia FANTIGRAFICA – Via delle Industrie 38 – 26100 Cremona

Polizia di Stato

Rotary
Gruppo Terre Padane
Distretto 2050

Progetto ideato dalla Polizia di Stato – Sezione Operativa Sicurezza Cibernetica della Polizia Postale di Cremona in collaborazione con il Gruppo Terre Padane del Rotary.