ATTENTI AL LUPO ONLINE

GUIDA PER PREVENIRE FRODI E TRUFFE DIGITALI

GLI STRUMENTI DI PAGAMENTO UTILIZZATI E I CONSIGLI

LE NUOVE MINACCE VIA WHATSAPP E CON INTELLIGENZA ARTIFICIALE

Le frodi digitali rappresentano una minaccia crescente, sono in costante evoluzione e richiedono attenzione e aggiornamenti continui; consistono in attività illecite, che mirano a sottrarre denaro o informazioni sensibili agli utenti. I "ladri digitali" sfruttano tecniche di ingegneria sociale, per manipolare le vittime facendo leva su emozioni come paura, curiosità o fiducia, inducendole a compiere azioni che altrimenti eviterebbero. Inoltre, approfittano di vulnerabilità tecnologiche, individuando falle nei sistemi di sicurezza o software non aggiornati, per ottenere un accesso non autorizzato a dispositivi o reti. Comprendere i diversi tipi di attacchi e frodi, le caratteristiche e le modalità operative è fondamentale per riconoscerle ed evitare i rischi, anche con misure preventive, per proteggere i propri risparmi. Tra le categorie più colpite, le persone anziane e, inaspettatamente, i giovani. Le frodi digitali presentano **alcune caratteristiche** ricorrenti. **Urgenza**: i contatti fraudolenti, in qualsiasi forma giungano, sollecitano azioni immediate, creando uno stato di agitazione e di impellenza per indurre l'utente a prendere decisioni veloci e avventate. **Apparenza legittima**: i frodatori utilizzano loghi, indirizzi, numeri di telefono, e-mail che imitano quelli di istituzioni affidabili per guadagnare la fiducia delle vittime. **Richiesta di informazioni sensibili**: viene spesso richiesto di fornire dati personali, credenziali di accesso o dettagli finanziari. Tuttavia, nel caso delle truffe sentimentali o dei falsi investimenti *online*, la strategia principale è la costruzione graduale, nel medio lungo periodo, di un rapporto di fiducia con la vittima. È, pertanto, essenziale diffidare sempre di richieste di denaro ricevute da contatti mail, numeri di telefono o account social di cui non si conosce l'autenticità. Le banche non chiedono mai, via telefono e via e-mail, i dati personali o le credenziali per l'accesso all'*home banking*.

Sono diversi gli strumenti di pagamento presi di mira. **Carte di credito e di debito**: fra i metodi di pagamento più diffusi per gli acquisti *online* sono spesso bersaglio di frodi come il *phishing* o la clonazione. **Carte prepagate**: sebbene considerate più sicure, poiché limitano l'importo disponibile, possono essere soggette a frodi, specialmente se i dati vengono sottratti o utilizzati senza autorizzazione. **Portafogli digitali**: offrono praticità e sicurezza, ma possono essere

oggetto di frode attraverso tecniche di ingegneria sociale o accessi non autorizzati. **Bonifici bancari**: spesso utilizzati a seguito di raggiri commerciali o disposti direttamente dal frodatore senza autorizzazione. Per sventare eventuali tentativi di frode, occorre analizzare attentamente la comunicazione ricevuta che, anche se sembra autentica, in realtà non lo è.

Quindi, è utile una serie di verifiche preventive. **Controllare** l'indirizzo e-mail, il nome e il numero di telefono del mittente o chiamante per individuare eventuali anomalie o discrepanze. **Analizzare** corpo e contenuto del messaggio, prestando attenzione a errori grammaticali, richieste inusuali, come per esempio scaricare un allegato, cliccare su un *link*, effettuare un *download*. **Verificare** il tipo di linguaggio utilizzato: se urgente, è una truffa. La maggior parte delle frodi si distingue per la modalità con cui la vittima viene contattata. Spesso si tratta di e-mail, sms, telefonate, contatti WhatsApp e *social media*. La trappola può celarsi dietro un *link*, un numero di telefono da richiamare o in un finto operatore della banca o delle forze dell'ordine che contatta la vittima per "mettere in salvo" i suoi i risparmi, mentre con grande abilità li sta rubando. L'introduzione di nuove tecnologie e l'utilizzo dell'intelligenza artificiale stanno diffondendo in modo allarmante nuove minacce molto sofisticate e difficilmente riconoscibili. Ecco alcuni esempi. *Deepfake* video e vocali: i truffatori usano l'intelligenza artificiale per clonare volto e voce di familiari o amici per la richiesta di denaro. Truffe sui *marketplace:* falsi annunci su piattaforme e-commerce per vendere prodotti inesistenti. Attacchi via *social:* creazione di falsi account con foto generate artificialmente per ingannare le vittime. *Chatbot* fraudolenti: capaci di simulare conversazioni intelligenti usati per finti supporti tecnici, truffe romantiche, truffe personalizzate.

LE 8 REGOLE D'ORO PER EVITARE LE TRUFFE

COSA FARE	COSA NON FARE
Utilizzare *password* complesse e modificarle regolarmente	Non cliccare su *link* sospetti
Monitorare regolarmente i conti bancari	Non effettuare trasferimenti di denaro in caso di richieste dubbie o non verificate
Utilizzare l'autenticazione a 2 fattori (2FA), sms, impronta digitale, app di autenticazione	Non fornire informazioni personali
Modificare regolarmente il pin di accesso alla banca *online*	Non fidarsi di offerte economiche troppo vantaggiose
Scaricare e utilizzare applicazioni provenienti solo dagli *store* ufficiali	Non lasciare incustoditi pc, tablet, cellulare
Accedere ai servizi online solo da *link* sicuri o già testati	Non cedere le credenziali dell'internet banking
Aggiornare sempre i propri dispositivi	Non cedere dati delle tessere di pagamento: bancomat, carta di credito, carta prepagata
Installare sul pc antivirus e *firewall*	Non condividere lo schermo del pc o WhatsApp con soggetti sconosciuti

E SE È TROPPO TARDI?

Interrompere qualsiasi ulteriore trasferimento di denaro. Bloccare, se necessario, carte di pagamento e accesso all'home banking o all'app bancaria quindi segnalare l'accaduto. Denunciare la frode alla Polizia di Stato o alle altre forze dell'ordine.

GLI INGANNI SENTIMENTALI SFRUTTANO BISOGNI DI AFFETTO E SOLITUDINE

Gli inganni e le frodi sentimentali rappresentano un fenomeno in crescita, sfruttano il bisogno di affetto e la solitudine delle vittime per trarle in inganno. Questo tipo di raggiri si sviluppa prevalentemente online, dove seduttori senza scrupoli tessono trame di fiducia e vicinanza emotiva con il solo obiettivo di sottrarre denaro alle loro vittime. Il meccanismo è consolidato: un individuo dall'apparenza affascinante e premurosa, creato da un algoritmo, entra in contatto con la vittima attraverso social network, app di incontri o piattaforme digitali. Dopo un'intensa fase di conoscenza virtuale, caratterizzata da attenzioni costanti e dichiarazioni di affetto, sopraggiunge un'emergenza improvvisa – una spesa medica, un investimento irripetibile, un blocco dei fondi inaspettato. A quel punto, la richiesta di denaro diventa inevitabile e, mentre la vittima crede di aiutare una persona ormai cara, il truffatore incassa e scompare. Nessuno è esente da questo rischio: uomini e donne, giovani e anziani, possono cadere nella rete di queste sofisticate manipolazioni. Non si tratta di ingenuità, ma di speranza: un sentimento su cui questa categoria di criminali costruisce il loro inganno. Oltre al danno economico, il peso psicologico è significativo: chi subisce la frode spesso prova vergogna, senso di colpa e difficoltà nel denunciare quanto accaduto. Prevenire è possibile: è fondamentale diffidare di storie che appaiono eccessivamente perfette, richieste di denaro inaspettate o promesse troppo allettanti.

LE NORME DELL'UNIONE EUROPEA

Il 28 giugno 2023 la Commissione europea, al fine di modificare e modernizzare l'attuale quadro normativo in materia dei servizi di pagamento in Europa, ha presentato due proposte: la direttiva sui servizi di pagamento (PSD3) e il regolamento sui servizi di pagamento (PSR). Entrambi gli atti sono stati approvati in prima lettura dal Parlamento europeo il 23 aprile 2024. Il pacchetto normativo, fra le varie iniziative, introduce misure per contrastare e ridurre le frodi, con l'obiettivo di creare un mercato dei pagamenti europeo più sicuro, trasparente e vantaggioso; raccoglie inoltre la sfida posta dall'innovazione tecnologica, proteggendo gli interessi dei consumatori e aumentando la loro fiducia nei pagamenti digitali. Le misure proposte per migliorare l'aspetto della sicurezza sono: ottimizzare l'utilizzo della **Strong customer authentication** (Sca); introdurre in caso di bonifico, l'obbligo di **verifica** della **corrispondenza** tra il **codice IBAN** e l'intestazione del conto del beneficiario; consentire ai prestatori di servizi di pagamento di **condividere** tra loro le **informazioni sulle frodi**; avviare **programmi di sensibilizzazione** per aumentare la consapevolezza degli utenti sui rischi di frode; valutare l'**estensione del diritto di rimborso** per i consumatori truffati, in specifiche situazioni. Le proposte della Commissione europea sono ancora in fase di discussione e potrebbero subire delle modifiche durante l'iter legislativo, prima di entrare effettivamente in vigore.

GLOSSARIO

ACQUISTI ONLINE TRAPPOLA Siti web falsi, di fatto trappole, che vendono prodotti a prezzi incredibilmente bassi ma non consegnano mai gli articoli acquistati

FINTO SUPPORTO TECNICO Truffatori che affermano di essere tecnici di supporto e richiedono accesso remoto al computer della vittima per risolvere problemi inesistenti, rubare informazioni, o autorizzare operazioni

FURTO D'IDENTITÀ Utilizzo non autorizzato di informazioni personali per aprire conti bancari, ottenere prestiti o effettuare acquisti

INVESTIMENTI FASULLI Truffatori promettono rendimenti elevati su investimenti falsi

MALWARE BANCARIO Software dannosi installati sui dispositivi degli utenti per rubare informazioni o monitorare attività *online*

MONEY MULING I truffatori reclutano persone, spesso inconsapevoli, per riciclare denaro proveniente da attività illecite, a fronte di una piccola commissione

PHISHING Truffatori inviano e-mail che sembrano provenire da fonti legittime per rubare informazioni personali

SIM SWAP È una frode informatica in cui un malintenzionato ottiene una nuova scheda SIM con il numero di telefono della vittima, intercettando sms e chiamate a lui destinate e accedendo ai suoi *account*

SMISHING Simile al phishing, ma attraverso sms

SPOOFING Truffatori mascherano il proprio numero di telefono o indirizzo e-mail per sembrare reali

TRUFFE DI DATING ONLINE Truffatori che fingono di essere potenziali partner romantici per ottenere denaro o informazioni personali

VISHING Truffatori utilizzano chiamate telefoniche per ottenere informazioni sensibili