LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

Le 5 truffe più pericolose in rete

Autore: Redazione | 11/01/2021

Le nuove frontiere del crimine cibernetico: le frodi più frequenti e pericolose del web. Phishing, virus, truffe creditizie ed estorsioni.

Con l'avvento del Web 2.0 dovremmo ripensare ad alcuni luoghi comuni. Così, per esempio, il pericolo non starebbe più dietro l'angolo, ma dietro il motore di ricerca o il social network. Secondo recenti stime, a livello globale, avverrebbe una truffa online ogni 5 ore. Un dato sconcertante che non risparmia nemmeno l'Italia, con le

sue 16 milioni di vittime.

Gli imperativi per far fronte al trend in costante aumento del crimine in rete sono due: fare attenzione e conoscere come funzionano le frodi online. Serve, quindi, l'impegno di tutti per porre fine a quella che è ormai nota come cyberinsicurezza.

Pertanto, abbiamo pensato a un articolo nel quale ti spieghiamo quali sono **le 5 truffe più pericolose in rete**. Si tratta di una cernita molto rigorosa, basata su un criterio essenziale: il pericolo delle frodi di cui parleremo consiste soprattutto nei circuiti estorsivi viziosi che sono in grado di generare. In altri termini, i criminali non si accontentano di essere pagati una sola volta, ma torneranno sempre a chiedere altri soldi.

Cybercrime: cos'è e perché si è diffuso?

Le innovazioni tecnologiche hanno inciso significativamente su ogni aspetto della vita quotidiana. Si può effettuare un bonifico con un semplice click senza fare code in banca, oppure seguire le serie tv preferite in streaming su qualsiasi dispositivo mobile.

Questo, quando si parla di persone comuni. Quando invece si tratta di tecnofili, è possibile imbattersi anche nell'**Internet delle cose** (Idc). Nato nel 2000, l'*Internet of things* permette di connettere gli elettrodomestici al proprio smartphone, dal quale possono essere gestiti in modo pratico e sicuro.

Tutto ciò ha indotto i fruitori delle telecomunicazioni ad affidarsi all'informatica per risolvere problemi pratici, traendone non pochi benefici.

Tuttavia, per ogni yang esiste uno yin. E qual è il risvolto negativo derivante da tanto benessere? Purtroppo, a fronte di un massiccio uso della rete, non corrisponde altrettanta consapevolezza dei rischi ad esso connessi.

Così è all'interno di questa forbice che si inserisce il **crimine informatico**. I cybercriminali approfittano della scarsa percezione del pericolo per perpetrare reati ai danni dei navigatori del web.

Negli ultimi due decenni, i crimini informatici più commessi e pericolosi sono stati 5:

1. phishing;
2. furto d’identità;
3. cryptolocker;
4. truffe amorose;
5. estorsioni a sfondo sessuale.

Cos’è il phishing?

Il **phishing** è, senza ombra di dubbio, il principe dei crimini online. Il termine allude alla “pesca” e, quindi, a un sistema di adescamento, inteso come attrazione e allettamento. Ciascun mezzo di telecomunicazione ha una forma di phishing e, limitandoci alla rete, la forma più diffusa sfrutta le mail.

I malintenzionati strutturano **e-mail** in modo da ingannare i destinatari che vengono indotti a rilasciare preziose informazioni personali. In che modo? Per cominciare, i criminali colpevoli di phishing creano dei **domini** specifici in grado di ingannare il lettore e invogliarli ad aprire la **posta elettronica**.

> *Un indirizzo mail a cui prestare molta attenzione può essere organizzato in questo modo: info@posteitaliane?.com.*

La prima parte dell’indirizzo allude a un comparto o un ufficio che può risultare familiare al destinatario. Ciò che importa, però, è che il lettore viene subito colpito dal dominio, molto vicino a un ente noto a tutti.

Ovviamente, i malintenzionati non possono utilizzare il nome esatto dell’ente, il cui dominio risulta già acquistato e impegnato. Pertanto, aggirano il problema corredando il nome dell’azienda con caratteri speciali come punti interrogativi, cancelletti o asterischi.

Anche l’oggetto della posta non è inserito a caso, essendo parzialmente visibile come anteprima nelle notifiche. L’**oggetto di una mail di phishing** può essere: «Abbiamo riscontrato problemi sul suo conto. Acceda per verificare».

Facendo leva sulla paura, il destinatario può facilmente cadere in trappola. Se dovesse aprire il messaggio, probabilmente il lettore si troverebbe di fronte a una richiesta del genere: «Al fine di verificare la sua identità, la invitiamo a fornire il numero della carta e il codice segreto riportato sul retro della sua carta».

Ricordiamo che questi due dati non vanno mai forniti a terzi, perché il possessore del **numero di carta di pagamento** e del **codice segreto** a esso associato è abilitato al suo utilizzo. Entrato in possesso di queste informazioni, il cybercriminale potrà disporre completamente delle finanze dell'utente vessato.

Il furto d'identità: quando accade?

Il **furto d'identità** rientra tra le frodi creditizie più commesse ma, a differenza del phishing, necessita di più attori.

Per cominciare, gli **haker**. Queste figure attive nel **cybercrimine** attaccano i database di società, organizzazioni ed enti al solo fine di rubare informazioni personali.

Il caso più celebre di un attacco haker del genere è stato commesso ai danni del gruppo alberghiero Marriot, che si è visto defraudato dei dati di 320 milioni di clienti: nomi, cognomi, date di nascita, numeri di carte di credito, identificativi dei passaporti, etc.

Questi dati ottenuti in modo illecito finiscono nel **darkweb,** ossia la parte più nascosta della rete, a cui si può accedere con sistemi di navigazione avanzati e non con i tipici motori di ricerca. Una volta caricati nel web oscuro, i dati sono liberamente consultabili.

Al malintenzionato che voglia **rubare l'identità** di un individuo basterà scorrere le liste di nominativi presenti nel darkweb.

Generalmente, il furto d'identità vero e proprio è preceduto da un **attacco di phishing**, mediante il quale il criminale vuole tentare di accedere ai conti del malcapitato. Perché accade questo?

Tra i motivi che possono indurre a mettere in atto un furto d'identità c'è la volontà di **ottenere un prestito o un finanziamento** fingendosi un'altra persona. È chiaro che, avendo libertà di movimento sul conto corrente della persona a cui è stata rubata l'identità, il criminale potrà disporre tranquillamente della somma ottenuta.

Non è raro imbattersi in **vittime di furto di identità** che si accorgono dell'illecito solo quando l'istituto finanziario che ha erogato il prestito chiede la riscossione

delle rate e degli interessi.

Cryptolocker: in cosa consiste e perché è pericoloso?

Il **cryptolocker** sfrutta le potenzialità del phishing e le integra con la dannosità dei virus. Il suo funzionamento è molto semplice: arriva una mail, generalmente da parte di uno pseudo istituto finanziario, che serve ad adescare l'utente, invogliato ad aprirla.

Nel corpo della mail è inserito un link che permette di leggere certi aggiornamenti, magari relativi alla privacy dell'utente, oppure all'informativa. Sta di fatto che il link in questione, in realtà, scarica sul pc dell'utente un **virus** (malware) in grado di criptare tutte le informazioni.

In pratica, il **pc risulta bloccato** e sul display appare un messaggio minatorio: per ottenere il codice di sblocco occorrerà pagare una certa cifra. In caso contrario, tutti i file contenuti nel pc saranno distrutti.

La cifra iniziale che viene richiesta è, all'inizio, abbastanza accessibile. Il problema è che, una volta scaricato il **cryptovirus** sul pc, i criminali che lo hanno creato possono attivarlo in qualsiasi momento. In questo modo, si minaccia continuamente la vittima che, ignara della presenza infettante, continua a versare somme di denaro.

Cosa sono le truffe amorose?

Le **truffe amorose** sono nate in Nigeria e, pertanto, sono anche dette **nigeriane**. Per mettere in piedi una truffa amorosa sono indispensabili due elementi:

- un **profilo falso** su un social network;
- un Money Transfer.

Questo tipo di truffa colpisce soprattutto le persone anziane perché più fragili nel confronto con le nuove tecnologie.

Da recenti indagini è stato scoperto che le truffe amorose sono organizzate da veri e propri **clan criminali** che approntano postazioni di chat con l'obiettivo di trovare

le vittime ideali, generalmente uomini vedovi over 60.

Una volta individuata, la vittima riceve dei semplici messaggi privati sul social network utilizzato. S'innesca, così, una comunicazione che spesso tende a diventare molto intima e sentimentale.

La caratteristica di questo tipo di truffa è la tempistica: spesso, la chat tra il criminale e la vittima può durare anche svariati mesi o anni.

A un certo punto, facendo leva sul clima di fiducia che si instaura e su un fasullo clima amoroso, dal **profilo fake** viene avanzata una richiesta di denaro, necessario per scopi impellenti: un'importante operazione che potrebbe cambiare lo stile di vita, oppure pagare il volo e i documenti necessari per raggiungere l'amato in patria. Si chiede, quindi, di mandare una somma di denaro attraverso il **Money Tranfer**, ossia quel circuito internazionale mediante il quale è possibile trasferire soldi in modo sicuro e veloce.

Nel caso in cui la truffa andasse a buon fine, i criminali non avranno alcuno scrupolo a chiedere ulteriori somme di denaro.

Sex Extortion: in cosa consiste?

Il fenomeno delle **sex extortion** è il gemello virtuale delle **estorsioni a sfondo sessuale** già praticate nella vita reale. Statisticamente, le vittime di sex extortion sono perlopiù uomini.

I luoghi della rete dove si consuma questo tipo di reato sono soprattutto **portali dedicati agli incontri erotici**, ma anche i social network più diffusi possono essere teatro di estorsione sessuale.

L'utente, in genere, viene contattato da un profilo e, in brevi istanti, la conversazione viene dirottata su tematiche piccanti. A quel punto, il criminale invita l'interlocutore ad avviare la **webcam** per una sessione di cyber-autoerotismo.

Il malcapitato, però, non sa che, dall'altra parte del display, c'è qualcuno che sta registrando il tutto mediante software dedicati. Al termine della **videochat**, la vittima si vede recapitare il file contenente la registrazione con l'invito a pagare una certa somma di denaro, pena la pubblicazione del video su canali esterni, tra

cui YouTube e simili.

Come nel caso del cryptolocker, cedere a questi ricatti non serve a far placare le future richieste estorsive.