FNP CISL PENSIONATI Lombardia

ADICONSUM LOMBARDIA Associazione Difesa Consumatori APS dal 1987

FIRST CISL Federazione Italiana Reti dei Servizi del Terziario LOMBARDIA

IL "PHISHING"

Definizione - Il cosiddetto *phishing* è una modalità di truffa *on-line* messa in atto da un operatore informatico, che con l'inganno cerca di indurre la vittima a fornire 'volontariamente' dati personali o finanziari, *password*, codici di accesso e simili.

L'azione truffaldina viene messa in atto attraverso varie forme di comunicazione digitale, in genere con messaggi che sembrano provenire da enti o persone apparentemente affidabili, legittimi ed ufficiali (ad esempio istituti finanziari, società pubbliche o private, aziende, gestori di servizi).

Il termine *phishing* è una parola inglese coniata verso la fine degli anni Ottanta e deriva da *fishing*, che significa 'pescare'; la pronuncia è analoga.

Entità del fenomeno - In termini statistici, vari istituti di ricerca specializzati attestano che gli attacchi di *phishing*, nei primi due decenni degli anni Duemila, sono aumentati in modo vertiginoso. In genere l'obiettivo è carpire i dati d'accesso a conti correnti e carte di credito (in alcuni casi clamorosi le vittime sono state centinaia di milioni) oppure di inserirsi nei sistemi informatici di aziende o di enti statali (nei casi più gravi, forze armate e servizi segreti).

Strumenti - Le tecniche utilizzate per queste azioni illegali sono di vario genere, ma le possiamo riassumere sinteticamente qui di seguito.

- **MAIL** - E' la forma più diffusa, e si concretizza con l'invio massiccio di messaggi ingannevoli attraverso la posta elettronica. L'indirizzo *mail* di provenienza è falsificato per farlo apparire come un mittente ufficiale e affidabile.
- **SMS** - Sono molto utilizzati anche i messaggi dei telefoni, con gli stessi accorgimenti.
- **SITI WEB** - Le richieste di dati o i *link* ingannevoli, trasmessi attraverso le *mail* o gli *sms*, rinviano a siti contraffatti, che presentano l'aspetto, le caratteristiche ed i loghi di siti ufficiali - a volte con una notevole accuratezza.
- **CHIAMATE TELEFONICHE** - In questi casi, il raggiro è perpetrato da persone che richiedono dati direttamente oppure utilizzando registrazioni vocali.
- **SOCIAL MEDIA** - Con l'avvento di *Facebook* e delle tante piattaforme analoghe, la situazione si è ulteriormente complicata. Nel mondo *social* le truffe vengono architettate con messaggi e comunicazioni fasulle, che sembrano provenire dai gestori oppure da amici e persone conosciute.

Modalità delle truffe - L'attacco tramite *phishing* può essere più o meno elaborato, ma si può comunque individuare una serie di fasi dalle caratteristiche standard.

1. Il truffatore invia i messaggi ingannevoli, utilizzando gli strumenti sopra descritti e presentandosi come un mittente noto alle vittime oppure come un ente autorevole (ad esempio, la propria banca oppure un istituto celebre e prestigioso). L'azione di *phishing* viene realizzata simulando le caratteristiche reali dell'ente contraffatto: impostazione grafica, logo, modalità di scrittura, tipologia dei contenuti, colorazione, eccetera. In molti casi la contraffazione è goffa e facilmente smascherabile, ma per disattenzione, o scarsa dimestichezza con gli strumenti informatici, il raggiro potrebbe ugualmente funzionare; il pericolo aumenta, ovviamente, quanto la simulazione è di alta qualità.
2. Il messaggio ingannevole, in genere, viene costruito facendo leva sull'emotività della vittima, facendogli vagheggiare vincite o premi, oppure mettendolo in allarme con false comunicazioni di gravi problemi e situazioni da risolvere in tempi rapidi. Ad esempio, frasi del genere: *la sua carta di credito è stata clonata - è in corso un'azione penale nei suoi confronti - abbiamo ricevuto una nota di addebito sul suo conto corrente di cinquemila euro - deve riconfermare i suoi dati, per non essere cancellato dal registro delle imprese - deve autenticarsi con la massima urgenza …*
3. L'elemento cruciale del *phishing* è quasi sempre la richiesta di cliccare su un *link*, per poter accedere ad un sito od un servizio informatico, il quale "permetterà" alla vittima di ottenere il beneficio promesso o di risolvere il suo problema. Questo *link*, in realtà, rinvia l'ignaro utente ad una copia contraffatta di quello vero.
4. Il truffatore, a questo punto, è in grado di carpire dati, informazioni, *password*, accessi a servizi e quant'altro, e di memorizzarli nei propri strumenti informatici. Tutto ciò gli servirà per effettuare prelievi, bonifici e/o addebiti bancari ai danni delle vittime, frodi finanziarie generalizzate, vendita di dati ad *hacker* o persone ed enti vari, oppure per pianificare altre azioni illegali in rete.

Caratteri tipici del *phishing* - Ovviamente non è facile capire se il messaggio che abbiamo ricevuto possa essere un'azione fraudolenta o meno, ma ci sono alcuni 'segnali' che, ad un'attenta valutazione, risultano sospetti. Alcuni casi tipici sono i seguenti.

- TESTI CON EVIDENTI ERRORI DI ORTOGRAFIA, DI LINGUA E DI GRAMMATICA - Molto spesso i messaggi truffaldini sono creati utilizzando programmi di traduzione automatica, che com'è noto non sono quasi mai perfettamente corretti (sono solo una prima base per procedere ad integrazioni ed adattamenti). Una *mail* sgrammaticata e dal linguaggio contorto, insomma scritta male, deve metterci in allarme.
- INDIRIZZO *MAIL* POCO AFFIDABILE - Osservando l'indirizzo di posta elettronica del mittente, si ha già una prima impressione della sua affidabilità; se poi il messaggio presenta le caratteristiche sopra descritte, il tentativo di *phishing* è certo.
- MESSAGGI GENERICI - Una *mail* indirizzata in modo indistinto al pubblico, senza riferimenti precisi alla persona che lo riceve, in prima battuta è già sospetta. La presenza di altri elementi descritti in questo capitolo dovrebbe indurre alla massima prudenza ed a considerare l'eventualità che si tratti di un messaggio ingannevole.

- TESTI CON RICHIESTE URGENTI E PER SITUAZIONI GRAVI - Come abbiamo già detto nel capitolo precedente, i messaggi ingannevoli, in genere, fanno leva sull'emotività, facendo credere che un grave problema debba essere risolto in tempi rapidi, per indurci a rispondere subito alle richieste avanzate. Questo è probabilmente il caso più tipico di *phishing*.
- COMUNICAZIONI DI VINCITE, PREMI E SOMME DI DENARO - Si tratta della più classica delle tipologie di truffa, non solo con i mezzi informatici… Il sospetto, in questo caso, dovrebbe essere d'obbligo.
- RICHIESTA DI DATI E INFORMAZIONI PERSONALI E IMPORTANTI - Quando un messaggio richiede al destinatario dati privati, informazioni delicate, *password*, PIN telefonici, numeri di conto o di carte di credito, è pressoché certo che sia in corso un tentativo di truffa. Informazioni di questo genere, a mezzo *mail* o strumenti *social* di vario genere, non rientrano nelle modalità operative degli istituti finanziari e/o di enti pubblici e privati. In ogni caso, se una persona avesse effettivamente dei rapporti con il presunto mittente del messaggio, per tranquillizzarsi può fare una verifica chiamando direttamente la banca o l'ente in questione.
- PRESENZA DI LINK - Molti messaggi contengono *link* necessari per dare corso ad azioni effettivamente utili, di provenienza legittima e corretta. Purtroppo l'inserimento di un *link* da cliccare è la trappola più diffusa e pericolosa dei tentativi di *phishing*, e quindi occorre avere la massima attenzione e prudenza. Piuttosto che rischiare, è bene cercare di verificare la bontà del *link:* ad esempio, passando con il cursore del mouse sopra il *link* (attenzione, senza cliccare!), si può visualizzare l'indirizzo reale del sito; oppure, come già detto, si può chiamare direttamente il mittente del messaggio.

Ricordiamo, infine, che uno dei trucchi più generalizzati è il falso avviso della SPEDIZIONE O ARRIVO DI UN PACCO POSTALE, ovviamente corredato del solito *link* (contraffatto) per "verificare" la consegna o lo stato della spedizione.