ADICONSUM
PIEMONTE
Associazione Difesa Consumatori APS
dal 1987

LA TUTELA DEL CONSUMATORE IN PILLOLE

SPAM, PHISHING, SMISHING E VISHING

Ministero dello Sviluppo Economico

Realizzato nell'ambito del Programma generale d'intervento della Regione Piemonte con l'utilizzo dei fondi del Ministero dello Sviluppo Economico. DM 10.08.2020

REGIONE PIEMONTE

COSA SONO

Lo SPAM è l'invio, attraverso indirizzi generici non verificati o sconosciuti, di messaggi pubblicitari indesiderati o non richiesti, generalmente di carattere commerciale. Lo spam è noto anche come posta spazzatura o posta indesiderata. Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale.
Il PHISHING è una truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico. VISHING e SMISHING sono sue varianti, che utilizzano telefonate (VISHING) o SMS (SMISHING). Talvolta i tentativi di truffa avvengono combinando più modalità di contatto.

A COSA PRESTARE ATTENZIONE

Gli attacchi di PHISHING non sempre replicano l'aspetto di quelle di istituti bancari o finanziari, ma anche di siti diversi dove però vengono utilizzati dati di carte di credito o bancari per effettuare i pagamenti oppure cercano di convincere i destinatari che sono i percettori di grosse somme di denaro. Di seguito riportiamo alcuni esempi di mail realmente ricevute da svariate persone:

"Gentile cliente, stiamo avendo problemi con i tuoi dati di fatturazione, per eseguire di nuovo il login occorre aggiornare l'account". Questa E-Mail è stata ricevuta nel 2017 da milioni di abbonati Netflix. Gli autori del phishing hanno chiesto agli utenti di aggiornare le informazioni relative alla modalità di pagamento. Chi ci è cascato ha perso sia i dati personali sia quelli della carta di credito, debito o prepagata associata all'account;

"Gentile utente" o "Salve utente PayPal". In genere iniziano così le E-Mail in cui si annuncia che la compagnia in questione è stata vittima di un attacco hacker e prega gli utenti di cambiare

tutte le proprie credenziali. Ma il messaggio non arriva affatto dalla società che offre servizi di pagamento digitale e di trasferimento di denaro tramite Internet, bensì dai criminali informatici che vogliono rubare i nostri dati. La stessa PayPal, sul proprio sito, afferma che nelle E-Mail indirizzate ai propri fruitori utilizza il nome e il cognome o la ragione sociale registrati sul tuo conto PayPal. Mai fidarsi degli incipit generici. Modalità simili vengono utilizzate nelle E-Mail apparentemente provenienti dalle banche. In questo caso, è necessario prestare un'attenzione maggiore in quanto recentemente ci sono numerose segnalazioni di E-Mail di phishing la cui veridicità viene avvalorata da una telefonata di un sedicente impiegato della banca;

L'elencazione si chiude citando le E-Mail phishing più famose della storia, nonché tra le più diffuse. Arrivano da presunti nobili che affermano di non riuscire a sbloccare il loro conto in banca milionario oppure da notai che comunicano al destinatario di essere eredi di grandi fortune. Propongono uno scambio: a fronte dell'anticipo delle spese legali o notarili per lo sblocco dei soldi offrono una quota del patrimonio o garantiscono che sarà erogata in breve tempo l'eredità. Peccato che non esista alcun nobile, né tantomeno una lauta somma. Ma si tratta, per l'appunto, di un raggiro.

REGOLE DI PRUDENZA

NESSUNO può proteggerci da questo tipo di truffe, se non la nostra prudenza! Per cercare di tutelarsi al meglio, è bene ricordare alcune regole

- Controllare sempre il link e il mittente della mail prima di cliccare qualunque indirizzo, ancora meglio non cliccare sul link, ma copiarlo invece nella barra dove si inserisce l'indirizzo del browser;
- prima di cliccare su un qualunque link, bisogna verificare che l'indirizzo mostrato è davvero lo stesso indirizzo Internet al quale il link condurrà. Un controllo che può essere effettuato in modo semplice, passando il mouse sopra il link stesso;

- usare solo connessioni sicure, in particolar modo quando si accede a siti sensibili. Come precauzione minima, si consiglia di non sfruttare connessioni sconosciute né tantomeno i wi-fi pubblici, senza una password di protezione. Se vogliamo una maggiore sicurezza, abbiamo l'opportunità di installare VPN che possono cifrare il traffico. Perché va ricordato sempre che in caso di utilizzo di una connessione non sicura, i cybercriminali possono reindirizzarci, senza essere visti, a pagine di phishing;
- controllare che la connessione sia HTTPS e verificare il nome del dominio all'apertura di una pagina. Questi fattori sono importanti soprattutto quando si usano siti che contengono informazioni sensibili, come pagine per l'online banking, i negozi online, i social media e via discorrendo
- non condividere mai i propri dati sensibili con una terza parte. Le compagnie ufficiali non chiedono mai informazioni del genere via E-Mail.

E SE SONO CADUTO NELLA TRAPPOLA?

Può capitare di accorgersi di essere caduti in una trappola quando ormai è troppo tardi. In questo caso è bene agire immediatamente per limitare il più possibile i danni. Se il phishing riguarda banche o strumenti finanziari, bisogna segnalare immediatamente l'accaduto ai canali di assistenza della banca o dell'intermediario per bloccare immediatamente i servizi di Home Banking e le carte di pagamento, quindi è consigliabile provvedere al cambio di tutte le proprie password. Gestita la parte di blocco delle utenze, è necessario presentare denuncia alla Forze dell'Ordine.

Per maggiori informazioni, trovate gli indirizzi delle nostre sedi e i contatti sul sito web: www.adiconsumpiemonte.it