
SICUREZZA IN RETE
Riconoscere le minacce e come proteggersi

Phishing:Una delle truffe più diffuse in rete

Che cos’è ?

Cosa fare per non cadere in trappola?

Che cosa fare dopo un attacco phishing e come sporgere denuncia alla Polizia Postale?

PHISHING: di cosa si tratta?

Il phishing è un tipo di truffa effettuata su internet dove un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

La più comune forma di phishing viene fatta attraverso l'invio di un'e-mail o altra comunicazione fraudolenta. Il messaggio è strutturato in modo da ingannare l'utente circa l'affidabilità del mittente. Spesso l'e-mail, che presenta un logo contraffatto di un istituto di credito, invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di sicurezza o di ordine tecnico (soprattutto per i servizi bancari).

Questo tipo di truffa non avviene solo via email. Attualmente si sta diffondendo anche via sms (Smishing), via social e anche tramite chiamate (Vishing).

Phishing:Una delle truffe più diffuse in rete

Si esplica:

📧 Nelle e-mail (Phishing)

✉️ Negli SMS (Smishing)

📞 Nei chiamate (Vishing)

📱 Nei QR Code (Qrishing)

🛜 Nei Wi-Fi (Wiphishing)

Possono essere combinate tra loro!

PHISHING: di cosa si tratta?

www.NewsBIELLA.it
QUOTIDIANO ONLINE GRATUITO di BIELLA e del biellese
BIELLA CITTÀ CREATIVA UNESCO

CRONACA | 26 gennaio 2024, 11:20

"Il figlio è in difficoltà, deve fare bonifico di 3mila euro": ma è una truffa. A sventarla l'impiegata di banca

La dipendente della banca, moglie di un Carabiniere e ben informata delle diverse modalità di truffe che avvengono ogni giorno, ha chiesto ulteriori informazioni e, dopo aver verificato che il conto corrente (su cui doveva avvenire il versamento) era straniero, ha consigliato alla pensionata di mettersi in contatto con il figlio telefonicamente per capire se il messaggio fosse autentico.

Alla fine, il figlio ha risposto tranquillamente alla chiamata del genitore e

il Biellese

Fa un bonifico di 3mila euro per il figlio. Era una truffa

I carabinieri invitano alla massima attenzione. Solo la scorsa settimana un altro caso era stato sventato grazie all'intervento di un'impiegata di banca

Sulla nota chat di messaggistica, il 75enne, aveva ricevuto un messaggio da un uno sconosciuto. Chi scriveva diceva di essere il figlio e che aveva avuto un problema. Gli si era guastato il telefono e quindi si era fatto prestare un apparecchio da un conoscente. Ma se fosse stato solo quello il problema... Ahimè, si trovava molto in imbarazzo, ma doveva saldare un debito d 3 mila euro, e anche in fretta.

Il pensionato, abile nella gestione dei suo affari attraverso i servizi bancari online, non ci ha pensato due volte e ha subito disposto il versamento della cifra richiesta facendola accreditare sul conto corrente indicato da chi si spacciava per essere suo figlio.

Solo dopo, a versamento fatto, si è interrogato se chi gli aveva scritto fosse

PHISHING: di cosa si tratta?

CRONACHE

A- A+

Sabato, 10 febbraio 2024

"Il suo conto corrente è sotto attacco", 80enne perde 240 mila euro con un sms

Dopo aver ricevuto il messaggio, la vittima è stata contattata da un individuo che si è spacciato per un operatore del servizio antifrode della sua banca

Di Redazione Cronache

Cosa fare per non cadere in trappola?

Controllare sempre il link e il mittente della email prima di cliccare qualunque indirizzo. Sarebbe ancora meglio non cliccare sul link, ma copiarlo invece nella barra dove si inserisce l'indirizzo del browser.

Controllare sempre l'ortografia. Bisogna fare anche molta attenzione alla struttura e al contenuto del messaggio. Inoltre, le e-mail sono indirizzate ad un destinatario specifico e avanzano richieste ben precise. Perciò, un primo campanello d'allarme consiste nella presenza di messaggi vaghi, rivolti ad un soggetto qualunque.

Usare solo connessioni sicure, in particolar modo quando si accede a siti sensibili (sono tutti quelli dove viene svolto un lavoro per il pubblico interesse e che richiedono misure di sicurezza più elevato). Come precauzione minima, si consiglia di non sfruttare **connessioni sconosciute né tantomeno i wi-fi pubblici, senza una password di protezione**.

Ogni volta che visitiamo un sito bisogna 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 email.

Cosa fare per non cadere in trappola?

https://haveibeenpwned.com/

Che cosa fare dopo un attacco e come sporgere denuncia alla Polizia Postale

Nel caso fossimo stati raggirati si possono presentare **2 casi:**

- abbiamo inserito i nostri dati su un sito fake
- i criminali sono riusciti ad estorcerci la copia digitale di un nostro documento d'identità.

Nel primo caso, va contattato l'amministratore del portale originale per avvertirlo di quanto accaduto, cambiare la password, e poi sporgere denuncia. Nel secondo, **dobbiamo necessariamente denunciare.**

Attualmente c'è l'opportunità di fare tutto comodamente a casa tramite sito della Polizia Postale**(https://www.commissariatodips.it/)**. All'interno dell'homepage dedicata alle segnalazioni, troviamo diversi riquadri da compilare. Una volta effettuata la denuncia, la Pubblica Sicurezza aprirà un regolare fascicolo che verrà trasmesso alla Procura della Repubblica per ottenere le necessarie autorizzazioni a procedere.

Inoltre, sul sito della polizia postale è possibile inviare e avere/ricercare informazioni sui reati informatici di cui veniamo a conoscenza, come phishing, hacking, il furto di codici bancomat e carte di credito, truffe e-commerce, spamming, pedofilia online, violazioni del diritto d'autore online e telefonia.

Cos’è lo Spamming? Alcuni consigli per evitarlo

Lo spamming è l’invio indiscriminato, senza il consenso del destinatario, di messaggi di posta elettronica e/o newsletter. In concreto la casella di posta elettronica viene inondata da decine di e-mail pubblicitarie capaci di porre a rischio il funzionamento del servizio di posta elettronica della vittima.

Alcuni consigli per evitarlo:

- Evitare di fornire sul web il proprio indirizzo e-mail, se non strettamente necessario per attivare dei "servizi";
- Non rispondere ad eventuali e-mail di spam, è quasi sempre un espediente utilizzato dal mittente per avere la conferma che l’indirizzo è attivo;
- Creare un indirizzo apposito, da dare nei newsgroup e nei siti web, che, nel caso colpito in maniera massiccia da spam, si possa abbandonare senza troppi problemi;
- Leggere attentamente, quando si compilano e firmano moduli che richiedono l'immissione dei propri dati personali, quale tipo di autorizzazione si concede al trattamento dei propri dati, e fare attenzione, in modo particolare, a chi può avere accesso a tali dati, per quali fini e a che titolo.


GRAZIE PER
L'ATTENZIONE!