SANFELICE 1893 BANCA POPOLARE

Newsletter

Ciao,

siamo qui oggi per parlare di alcune minacce sempre crescenti nel mondo digitale: il **phishing**, lo **smishing** e il **vishing**. Queste forme di truffa online stanno diventando sempre più sofisticate e diffuse, mettendo a rischio la sicurezza e la privacy dei nostri dati personali. È importante essere consapevoli di queste minacce e conoscere i modi per proteggerci. In questa newsletter, esploreremo cosa sono, come funzionano e cosa possiamo fare per difenderci.

Phishing
Il phishing è una truffa online in cui i truffatori cercano di ingannare le persone per ottenere informazioni personali come password, dati finanziari e numeri di carte di credito. Questo avviene spesso attraverso e-mail contraffatte che sembrano provenire da istituzioni legittime come banche, società di carte di credito o siti di social media. Le e-mail di phishing possono contenere link malevoli che portano a siti web contraffatti dove le vittime vengono indotte a inserire le proprie informazioni sensibili.

Smishing
Lo smishing è simile al phishing, ma anziché avvenire tramite e-mail, avviene attraverso messaggi di testo o SMS. I truffatori inviano messaggi contraffatti che sembrano provenire da banche, istituzioni finanziarie o altre aziende rispettabili, chiedendo alle vittime di fornire informazioni personali o di cliccare su link dannosi.

Vishing
Il vishing è una forma di phishing che avviene attraverso chiamate telefoniche. I truffatori chiamano le vittime fingendo di essere rappresentanti di istituzioni finanziarie o aziende legittime e cercano di ottenere informazioni sensibili o di convincere le persone a compiere azioni dannose come trasferimenti di denaro.

Come proteggersi

- **Sii vigile**: fai attenzione alle comunicazioni non richieste, sia che arrivino via e-mail, messaggi di testo o telefonate. Se qualcosa sembra sospetto non agire mai d'impulso comunicando dati personali e/o effettuando operazioni (saranno i truffatori a mettervi "fretta"). Chiamate di vostra iniziativa (controllando il numero sui documenti in vostro possesso o sul sito internet ufficiale) l'azienda o l'istituzione coinvolta.
- **Verifica l'autenticità**: prima di fornire informazioni personali o fare clic su link, verifica l'autenticità dell'e-mail, del messaggio di testo o della chiamata. Controlla l'indirizzo e-mail del mittente, cerca errori di ortografia o grammatica e confronta i numeri di telefono con quelli ufficiali dell'azienda.
- **Utilizza l'autenticazione a due fattori**: attiva l'autenticazione a due fattori (2FA) ovunque sia possibile. Questo aggiunge un ulteriore livello di sicurezza richiedendo un secondo metodo di verifica, come un codice inviato al telefono, oltre alla password per accedere ai tuoi dati personali.
- **Mantieni aggiornati i software**: assicurati di tenere aggiornati i tuoi software antivirus e anti-malware per proteggerti dalle ultime minacce online.
- **Educazione**: educa te stesso e gli altri sulle minacce del phishing, smishing e vishing. Più le persone sono consapevoli, meno probabile è che cadano nelle trappole dei truffatori.

La sicurezza online è una responsabilità condivisa e proteggersi da queste minacce richiede una combinazione di vigilanza, educazione e utilizzo delle migliori pratiche di sicurezza informatica. Speriamo che questa newsletter ti abbia fornito informazioni utili su come difenderti da phishing, smishing e vishing.

Rimani vigile e sicuro online!

SANFELICE 1893 Banca Popolare