PHISHINGOVÉ ÚTOKY

NENECHAJTE SA NACHYTAŤ

AKO PREBIEHA PHISHINGOVÝ ÚTOK?

Útočníci sa v elektronickej komunikácii snažia presvedčiť potenciálnu obeť, aby prezradila citlivé informácie ako sú prihlasovacie údaje, bankové údaje alebo údaje z kreditnej karty – vydávaním sa za dôveryhodné osoby, či inštitúcie. Kombinujú sociálne inžinierstvo a klamstvá.
Zdroj: Slovník ENISA

ČO ZNAMENÁ POJEM „SOCIÁLNE INŽINIERSTVO“?

Všetky metódy, ktorými možno presvedčiť obeť, aby odhalila konkrétne informácie alebo vykonala konkrétny úkon z nelegitímnych dôvodov.
Zdroj: Slovník ENISA

ČO ROBIŤ, KEĎ SA DOMNIEVATE, ŽE STE DOSTALI PHISHINGOVÝ EMAIL?

Neklikajte na odkazy, nevolajte na telefónne čísla uvedené v tele emailu, neodpovedajte na mail ani neotvárajte prílohy – označte ho ako SPAM a vymažte ho. Prípadne kontaktujte svojho administrátora. Vždy je lepšie nejaký email ignorovať, než sa nechať nachytať na phishing. Vznikne tým menej škody.

1 POZOR NA URGENCIE

Naliehavo znejúce emaily, ktoré vyžadujú zvláštnu okamžitú reakciu – napríklad neodôvodnenú zmenu hesla, rovnako tak neodôvodnené zadanie vášho telefónneho čísla pre overenie prístupu, výzva na prevod financií alebo požiadavka na zadanie vašich osobných údajov.

2 POZERAJTE SA, ALE NEKLIKAJTE

Skôr, ako v emaili kliknete na odkaz, prejdite na neho kurzorom, aby ste videli URL adresu – z názvu uvidíte, či zodpovedá popisu, alebo môže ísť o podvrh. Podozrivé sú akékoľvek nesúvisiace, či nezrozumiteľné texty v URL adrese.

3 SKONTROLUJTE ODOSIELATEĽA MAILU

Nepozdáva sa vám meno odosielateľa? Kliknite na meno, aby ste videli celú mailovú adresu. Názov banky, či inej organizácie je možné sfalšovať jednoducho – emailovú adresu už nie.

4 POZOR NA PRAVOPISNÉ CHYBY A SKOMOLENINY

Pokiaľ v texte emailu nájdete gramatické chyby, nesprávne skloňovanie, či nelogicky vyskladané vety – pravdepodobne ide o phishing. Útočníci často používajú automatizovaný preklad. Chyby často nastávajú už pri oslovení adresáta.

5 VÝHRY, NOMINÁCIE, OCENENIA

Najpriehľadnejším phishingovým emailom je informácia o výhre v súťaži. Rovnako tak sa však môžete stať obeťou cieleného phishingu, kedy vám príde email s informáciou o nominácii, či ocenení v odvetví v ktorom pracujete alebo študujete – ibaže z neznámej adresy a na konci emailu sa možno dočítate, že je potrebné zaplatiť 1 500€, aby ste svoju nomináciu potvrdili.

Najlepšou ochranou pred phishingom je ostražitosť a neustále zvyšovanie bezpečnostného povedomia.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-24-3
Verzia V.1

www.cybercompetence.sk