PHISHING

AKO FUNGUJE, AKO HO ROZPOZNAŤ A AKO SA CHRÁNIŤ

Predvianočný čas je ideálnym obdobím pre podvodníkov. Ľudia viac nakupujú online, sledujú zásielky, čakajú upozornenia od kuriérov a častejšie reagujú na e-maily či SMS s informáciami o platbách, doručení balíkov alebo potvrdení objednávok. V hektickej atmosfére sviatkov, keď sa kombinuje časový tlak, stres a množstvo digitálnej komunikácie, je oveľa jednoduchšie prehliadnuť varovné signály.

Podvodníci to dobre vedia a práve v tomto období masovo šíria phishingové kampane, ktoré napodobňujú správy od e-shopov, bánk či kuriérskych služieb. Stačí jedno unáhlené kliknutie na falošný odkaz – a môže dôjsť k odcudzeniu peňazí, osobných údajov či kompromitácii celého účtu.

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 nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Phishing patrí medzi najčastejšie a najnebezpečnejšie formy internetových podvodov, pri ktorých útočníci cielia na získanie citlivých údajov – najmä prihlasovacích údajov do internetového bankovníctva, údajov z platobných kariet či osobných informácií. Ide o techniku sociálneho inžinierstva, ktorá zneužíva dôverčivosť používateľov a ich prirodzenú reakciu na naliehavé správy. V dôsledku phishingu môže dôjsť k odcudzeniu financií, zneužitiu osobných údajov alebo k prevzatiu kontroly nad online účtami.

Mechanizmus podvodu

Phishingový útok zvyčajne začína zaslaním e-mailu alebo SMS, ktorá sa tvári ako dôležité upozornenie od banky, kuriérskej spoločnosti, štátnej inštitúcie či známej online služby. Tieto správy sú často formulované tak, aby v príjemcovi vyvolali pocit naliehavosti. Podvodníci používajú tvrdenia ako:

- Váš účet bol zablokovaný.
- Je potrebné uhradiť clo za balík.
- Overte svoju identitu, inak bude služba deaktivovaná.

Súčasťou správy býva odkaz, ktorý smeruje na webovú stránku napodobňujúcu originál – či už ide o internetové bankovníctvo, portál kuriérskej spoločnosti alebo inú službu. Grafika aj rozloženie stránok bývajú často veľmi presvedčivé, čo zvyšuje pravdepodobnosť, že si používateľ podvod nevšimne.

Po kliknutí na odkaz je obeť presmerovaná na falošnú prihlasovaciu stránku, kde je vyzvaná zadať citlivé informácie: prihlasovacie meno, heslo, číslo platobnej karty, CVV kód či dokonca rodné číslo. Ak používateľ údaje vyplní, okamžite sa dostanú do rúk podvodníkov. Tí ich následne použijú na prihlásenie do reálneho účtu obete alebo na zadanie neoprávnených platieb. Niektoré útoky pokračujú aj žiadosťou o SMS kód či push notifikáciu, aby mohli dokončiť platbu aj v prípade aktívneho viacfaktorového overenia.

Indikátory podvodu – ako phishing rozpoznať

Hoci phishingové správy môžu pôsobiť vierohodne, väčšinou obsahujú signály, ktoré poukazujú na podvod. Medzi najčastejšie patria:

- **Neočakávaná správa** od neznámeho odosielateľa – banka, či úrad vás bežne nekontaktujú z náhodných e-mailových adries, alebo telefónnych čísel.
- **Naliehavé a zastrašujúce formulácie** – požiadavky typu „okamžite konajte", „inak bude účet zrušený" či „posledná výzva".
- **Podivné odkazy** – doména v odkaze nezhoduje s oficiálnou stránkou, je pozmenená, obsahuje preklepy alebo neobvyklé koncovky.
- **Požiadavka na zadanie citlivých údajov mimo oficiálnych kanálov** – legitímne spoločnosti nikdy nežiadajú zadávať heslá, alebo údaje z platobnej karty cez odkazy zaslané v správach.
- **Gramatické chyby a nesúrodá grafika** – nie všetky podvody sú profesionálne spracované a môžu obsahovať chyby či nelogické texty.

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 nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ako sa chrániť pred phishingom

Prevencia je najúčinnejšia forma ochrany pred phishingom. Nasledujúce zásady výrazne znižujú riziko, že sa stanete obeťou:

- Nikdy **neklikajte na odkazy v podozrivých správach**. Ak máte pochybnosti, navštívte stránku cez vlastnoručne napísanú adresu v prehliadači.
- **Overte odosielateľa**. Všímajte si doménu e-mailu a telefónne číslo. V prípade pochybností kontaktujte banku či spoločnosť cez ich oficiálny kontakt.
- Nikomu **neposielajte vaše bezpečnostné, prihlasovacie** údaje ako sú: heslá, PIN kódy ani SMS overovacie kódy. Žiadna banka ani úrad od vás nikdy nebude tieto informácie žiadať.
- **Aktivujte si viacfaktorové overenie** a používajte silné, jedinečné heslá.
- **Pravidelne aktualizujte** zariadenia a používajte kvalitný antivírus, ktorý môže zachytiť niektoré typy škodlivých odkazov.
- **Dôsledne kontrolujte** webovú adresu pri prihlasovaní do internetového bankovníctva.
- **Buďte obozretní** pri neočakávaných výzvach na platbu alebo údajne nezaplatené zásielky.

Phishing je sofistikovaný, no pri správnej opatrnosti rozpoznateľný podvod. Útočníci sa neustále zdokonaľujú, preto je dôležité mať aktuálne informácie a dodržiavať zásady bezpečného správania na internete. Najúčinnejšou ochranou ostáva zdravá miera nedôvery – ak niečo vyzerá podozrivo alebo nečakane, radšej to skontrolujte dvakrát, než by ste útočníkom poskytli prístup k svojim financiám či osobným údajom.

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 nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti