eset | bezpečne na nete

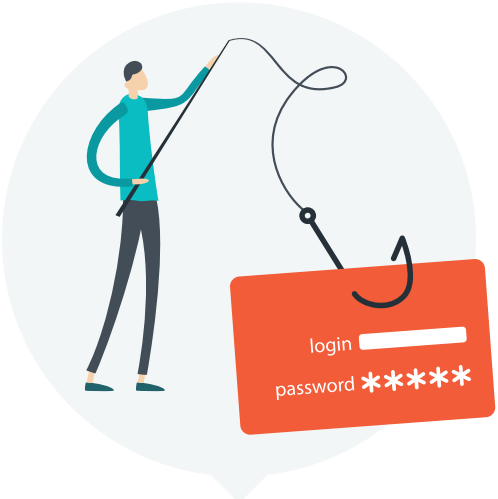
Podvodné praktiky

Techniky, ktoré prostredníctvom psychologickej manipulácie spôsobujú u používateľa alebo skupiny želanú zmenu jeho správania v prospech útočníka. Výsledkom tejto manipulácie je získanie osobných informácií o používateľovi podvodom.

Najčastejšie formy

Spam

Sociálne inžinierstvo



Phishing

Spam

Spam je akákoľvek forma nevyžiadanej komunikácie, môže byť odosielaná aj hromadne. Najčastejšou formou je komerčný e-mail zaslaný na veľké množstvo adries.

Ako minimalizovať spam?

Nezverejňujte váš e-mail na verejných webových stránkach a službách.

Neklikajte na žiaden odkaz ani nesťahujte prílohy, ktoré sa nachádzajú v neoverenom e-maile.

Používajte spoľahlivý bezpečnostný softvér s funkciou antispam.

Sociálne inžinierstvo

Sociálne inžinierstvo je spôsob manipulácie ľudí s cieľom získať od nich dôverné informácie alebo prinútiť ich vykonať požadovanú akciu.

Ako minimalizovať vplyv sociálneho inžinierstva?

Neotvárajte e-maily a prílohy z podozrivých zdrojov.

Používajte viacfaktorové overenie.

Nenaleťte na lákavé ponuky. Ak ponuka znie príliš dobre na to, aby bola pravdivá, kliknutie na ňu si dvakrát premyslite.

Udržujte bezpečnostný softvér vždy aktualizovaný.

Phishing

Phishing je forma útoku s využitím metód sociálneho inžinierstva, pri ktorom sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať od obete citlivé informácie.

Ako zabrániť phishingu?

Neposkytujte osobné údaje hocikomu prostredníctvom elektronickej komunikácie.

Neklikajte na skrátené odkazy v správach ani v statusoch na sociálnych sieťach.

Overte si obsah správy priamo u odosielateľa.

Čo je to phishing?

Phishing je taktika útoku, pri ktorom sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať citlivé informácie. Najčastejšie sa šíri cez klamlivé e-maily, četovacie služby či obyčajný odkaz v príspevku na sociálnej sieti.

Znaky phishingového útoku

Žiadosť o osobné údaje

Obsah správy vás vyzýva na okamžité zaslanie vašich kontaktných údajov, bankového účtu, čísla karty alebo žiada o aktualizáciu prihlasovacích údajov do nejakej služby.

Naliehavosť

Phishingové správy vás svojím obsahom pokúšajú naviesť na to, aby ste konali rýchlo a neuvážene.

Všeobecné a neformálne oslovenia

Obsahuje všeobecné oslovenie, napr. „Milý môj", „Ahoj môj najlepší kamarát". Nie vaše konkrétne meno.

Slabá jazyková úroveň

Správa obsahuje pravopisné chyby, preklepy a nezvyčajné vetné formulácie. Nie je to však podmienka.

Neočakávaná výhra

Často sa objavuje správa obsahujúca ponuku, ktorá sa neodmieta. Ak znie správa až príliš dobre na to, aby bola pravdivá, takmer vždy ide o podvod.

Podozrivá doména

Ak ste presmerovaný na externú webovú adresu, pri phishingovom útoku často stránka neobsahuje **https://** protokol a ikonu bezpečnostného zámku.

Hlavné pravidlo

Nikdy nezasielajte vaše osobné údaje prostredníctvom e-mailu alebo iných dostupných komunikačných platforiem.

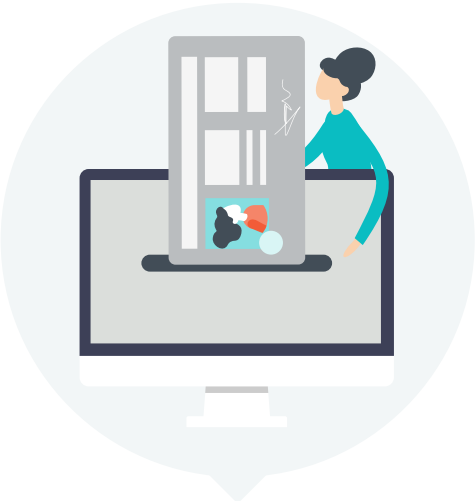
Ako sa chrániť pred phishingom?

Sledujte aktuálne dianie a majte aktuálne informácie zo sveta IT bezpečnosti.

Neotvárajte a nesťahujte prílohy v podozrivých správach vo vašej e-mailovej schránke.

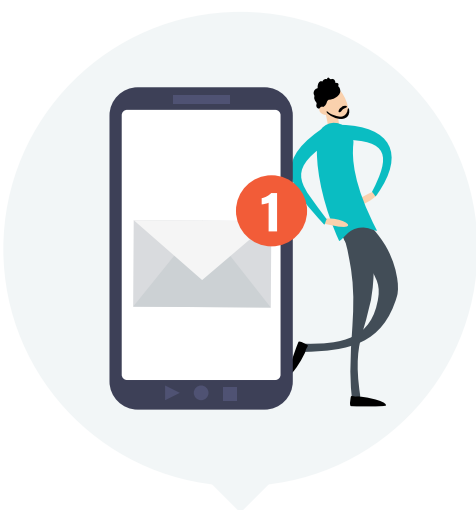
Neklikajte na skrátené odkazy v správach ani v statusoch na sociálnych sieťach.

Pravidelne aktualizujte bezpečnostný softvér a operačný systém vo vašich zariadeniach.



Neposkytujte osobné údaje hocikomu a buďte obozretný pri poskytovaní údajov prostredníctvom elektronickej komunikácie.

Overte si obsah správy priamo u odosielateľa alebo organizácie, ktorú zastupuje. Legitímnosť si viete overiť telefonicky alebo návštevou pobočky.



Nastavte si notifikácie na prevody z účtu. Ak sa náhodou stane niečo podozrivé, ste upozornený a môžete takmer okamžite bez čakania kontaktovať svoju banku.

Ako účinne zabezpečiť váš e-mail

Používajte bezpečnostný softvér. Ideálne s funkciami antiphishing a antispam.

Používajte kvalitné a silné heslo. Zvoľte frázové heslo, unikátne do každého e-mailového účtu.

Zapnite si dvojfaktorovú autentifikáciu. Bezplatne ju poskytujú mnohí veľkí poskytovatelia e-mailových schránok ako Gmail, Yahoo a podobne.

Neotvárajte podozrivé prílohy. Názov takéhoto dokumentu má často odlišnú príponu, napríklad nekončí sa na „doc" alebo „docx", ale inými písmenami.

Neklikajte na skrátené odkazy, na ktoré máte podľa odosielateľa správy kliknúť.

Zbytočne verejne nezdieľajte vašu e-mailovú adresu.