VÍTKOVICE
VÍTKOVICE IT SOLUTIONS

Phishing – poučení pro ty, kteří kliknuli…

Co je phishing?

Phishing je snaha počítačových podvodníků získat vaše citlivé osobní informace, jako jsou hesla, údaje o platebních kartách, rodná čísla nebo čísla bankovních účtů. Šíří se podvodnými emailovými zprávami nebo přesměrováním na falešné webové stránky.

Odkud přichází podvodné zprávy zvané phishing?

Phishingové zprávy vypadají jako zprávy od důvěryhodných organizací, jako je PayPal, Česká pošta nebo vaše banka. Nicméně se ve skutečnosti jedná o podvod. Pokud vás tyto instituce žádají o aktualizace, ověření nebo potvrzení informací o vašem účtu, měli byste být velice obezřetní. Po kliknutí na odkaz v podvodném emailu jste přesměrováni na falešné stránky, kde vás útočníci nabádají k zadání citlivých informací o vašem účtu, což může vést ke krádeži identity.

Jak odhalit phishing?

Obdržíte zprávu s žádostí o zadání vašich osobních informací, obvykle prostřednictvím emailu nebo internetových stránek. Věnujte pozornost zejména následujícím znakům:

Pravopisné a gramatické chyby

Zkontrolujte pravopisné a gramatické chyby v předmětu a těle e-mailu. E-mail od legitimní organizace by měl být dobře napsaný.

Škodlivé odkazy

Umístěte kurzor na hypertextové odkazy v e-mailu a před kliknutím je zkontrolujte. Tyto e-maily mohou obsahovat hypertextové odkazy se škodlivými adresami URL, které vás zavedou na falešné webové stránky.

Žádný bezpečnostní certifikát

adresy URL bezpečnostních certifikátů by měly začínat zabezpečeným https:// – nikoli http://. Pokud adresa URL postrádá bezpečnostní certifikát, neklikejte.

Neobvyklý obecný pozdrav

Legitimní společnosti vás obvykle osloví vaším jménem. Dejte si pozor na obecné pozdravy, jako je „Vážený zákazníku online nakupování“

Upozornění, která znějí legitimně

E-mail může znít legitimně a může uvádět „zaznamenali jsme podezřelou aktivitu“ nebo „vyskytl se problém s platebními údaji na vašem účtu“

E-maily s žádostí o „kliknutí“

E-mailové podvody vás téměř vždy požádají, abyste na něco klikli. „Kliknutím sem aktualizujete své platební údaje“ nebo „Kliknutím sem zobrazíte nejnovější informace o Covid-19“

Falešné e-mailové adresy

Phishingové e-maily jsou obvykle odesílány z falešné e-mailové adresy obsahující název společnosti. Ujistěte se, že nebyly provedeny žádné změny (jako jsou další čísla nebo písmena).

Nebezpečné přílohy souborů

E-mail může obsahovat přílohu s falešnou fakturou nebo malwarem, který do vašeho počítače vnese ransomwarové infekce. Autentické instituce vám obvykle neposílají e-maily s přílohami náhodně, ale místo toho vás nasměrují ke stažení dokumentů nebo souborů na jejich vlastních webových stránkách.

Panika

E-mail bude říkat něco, co způsobí paniku, jako je hrozba uzavřením účtu, pokud nebudete okamžitě jednat.

E-mail od ředitele nebo nadřízeného
Hackeři budou mít často tyto e-maily vypadat, jako by přicházely od generálního ředitele zaměstnavatele. Tyto e-maily budou obvykle vyžadovat, aby zaměstnanci převedli peníze na neautorizovaný účet.

Jak se bránit phishingovým útokům?

• Základním pravidlem je obezřetnost. Neklikejte na odkazy v nevyžádané poště nebo na Facebooku
• Pravidelně aktualizujte váš prohlížeč a instalujte bezpečnostní záplaty.
• Neotvírejte přílohy nevyžádaných emailových zpráv.
• Chraňte si svá hesla a nikomu je neprozrazujte.
• Nikomu nesdělujte vaše citlivé informace po telefonu, osobně nebo emailem.
• Kontrolujte správnost URL adresy navštěvovaných stránek. V mnoha případech při phisingovém útoku vypadá webová adresa na první pohled zcela důvěryhodně. Rozdíl naleznete v detailech. Například v chybném písmeně v URL adrese nebo v odlišné doméně (.com namísto .cz).