



5 TIPŮ, JAK ROZPOZNAT PODVODNÝ E-MAIL

1.

BUĎTE OPATRNÍ, KDYŽ VÁM PŘIJDE E-MAIL OD NEZNÁMÉHO ODESÍLATELE

A to zejména tehdy, pokud po vás odesílatel vyžaduje rychlou nebo neobvyklou akci, kterou byste za normálních okolností neučinili. Autoři phishingových e-mailů se často vydávají za nějakou autoritu – bankéře, lékaře, právního zástupce nebo státního úředníka – aby donutili příjemce udělat, co chtějí.

2.

POZOR NA FALEŠNÉ E-MAILOVÉ ADRESY

Najeďte si na adresu odesílatele v horní části e-mailu a dobře si ji prohlédněte. Obsahuje náhodná čísla, kombinaci malých a velkých písmen nebo chybně napsaných slov? Pak může jít o podvod. Takové adresy se většinou podobají tradičnímu formátu adres vašich kolegů a spolupracovníků, ale jsou trochu rozdílné. To samé platí i u zpráv cloudových služeb.

3.

PŘEMÝŠLEJTE NAD ŽÁDOSTÍ V E-MAILU

Jde o obvyklý požadavek, nebo se vám doručená zpráva zdá něčím podezřelá? Podvodné e-maily v sobě mívají naléhavost a snaží se příjemce přesvědčit o závažnosti situace. Třeba po vás chtějí odpověď v omezeném čase (do 24 hodin či dokonce hned) nebo vám hrozí pokutami.

4.

VŠÍMEJTE SI TÓNU DORUČENÉ ZPRÁVY

Phishingové e-maily útočí na lidské emoce. Cítíte po přečtení příchozí zprávy paniku, strach, zvědavost či naději? Zpomalte. Autoři podvodných e-mailů často vyhrožují, žádají vás o podporu nebo naopak nabízejí něco, co vám chybí a vy byste o to mohli mít zájem. Třeba lék, peníze nebo lístky na koncert. Varovat by vás měly také pravopisné chyby v textu.

5.

POZOR NA STAHOVÁNÍ PŘÍLOH, ODKAZY NA CIZÍ STRÁNKY A ŽÁDOSTI O ZMĚNU HESLA

U podezřelých e-mailů, které obsahují odkaz na webové stránky nějaké společnosti, raději napřed zkontrolujte, zda URL adresa této společnosti neobsahuje nějakou chybu. Neznámé přílohy v mailech nestahujte, zbytečně neklikejte na odkazy v textu a nenechte se automaticky zlákat do sdílení svých osobních údajů.

A CO DĚLAT, JESTLIŽE JSTE UŽ KLIKLI?

- Pokud používáte pracovní notebook nebo telefon, zkontaktujte oddělení IT.
- Pokud jste někomu poskytli bankovní údaje, ihned o tom informujte svou banku.
- Pakliže máte antivirový software, spusťte v něm úplnou kontrolu a nechte ho odstranit zjištěné problémy.
- Prolomené heslo změňte na všech účtech, na kterých ho používáte.
- Spojte se s kontakty ze svého účtu a dejte jim vědět, že jste byli napadeni.