

Jak být bezpečně online >>>



Používat silná hesla

Heslo by mělo mít alespoň 12 znaků a obsahovat kombinaci písmen, číslic a symbolů. Každý účet by měl mít své vlastní heslo.

Neotvírat podezřelé e-maily a odkazy

Přílohy a odkazy z neznámých nebo nedůvěryhodných zdrojů představují riziko. Odesílatele je vhodné vždy ověřit.

Zálohovat důležitá data

Důležité soubory je vhodné pravidelně zálohovat a ukládat na bezpečné místo, například do cloudu nebo na externí disk.

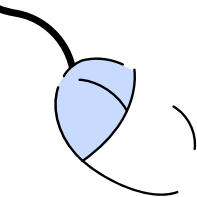
Zapnout dvoufázové ověření

Dvoufázové ověření (2FA) zvyšuje bezpečnost přístupu a chrání účet i v případě úniku hesla.

Aktualizovat zařízení a software

Pravidelné aktualizace opravují bezpečnostní chyby a zajišťují ochranu zařízení před aktuálními hrozbami.

Bezpečí začíná u Vás.



Jak rozpoznat podezřelý email >>>

Nedůvěryhodná adresa odesílatele

Adresa často napodobuje
oficiální domény, ale
obsahuje drobné odchylky v
názvu či příponě.

Naléhavý tón

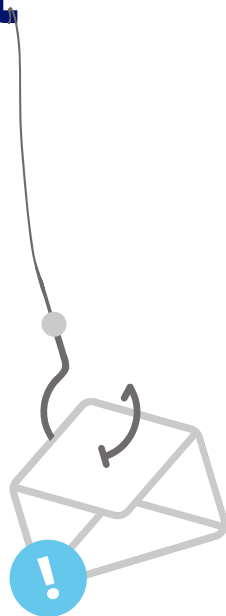
Zpráva vytváří tlak na rychlou
reakci a vyvolává obavy z
blokace účtu či ztráty dat.

Nedůvěryhodné odkazy či přílohy

Podezřelé e-maily často
obsahují odkazy nebo přílohy,
které mohou vést na podvodné
stránky nebo nainstalovat
škodlivý software.

Jazykové a formální nedostatky

Text často obsahuje jazykové
chyby, nepřírozené formulace a
bývá stylisticky nekonzistentní.



Zastavit.

Zkontrolovat.

OVĚŘIT.