

PHISHINGOVÉ E-MAILY, KTERÉ SE TVÁŘÍ, JAKO BY BYLY ODESLÁNY Z BANKY

Phishing je prováděn prostřednictvím podvodných e-mailů, které od adresátů lákají osobní, finanční nebo bezpečnostních údaje.

JAK TO FUNGUJE?

Tyto e-maily:

mohou **vypadat** shodně jako korespondence zasílaná skutečnou bankou.

kopírovat loga, strukturu a znění skutečných e-mailů.



požadovat od vás, abyste si stáhli připojený dokument nebo klikli na odkaz.

používat jazyk, který vyvolává pocit naléhavosti.



Kyberzločinci se spoléhají na to, že jsou lidé zaneprázdněni; na první pohled vypadají tyto podvodné e-maily jako pravé.



Mějte se na pozoru pokud používáte mobilní zařízení. Z vašeho telefonu nebo tabletu může být obtížnější zjistit pokus o phishing.

CO MŮŽETE DĚLAT?

- **Aktualizujte svůj software**, včetně svého prohlížeče, antivirového a operačního systému.
- **Mějte se obzvláště na pozoru**, pokud jste v e-mailu z „banky“ žádání o citlivé informace (např. heslo k vašemu internetovému bankovníctví).
- **Podívejte se na e-mail pozorně**: porovnejte adresu s předchozími skutečnými zprávami ze své banky. Zkontrolujte, zda e-mail neobsahuje gramatické a pravopisné chyby.
- **Neodpovídejte na podezřelý e-mail**, místo toho jej přepošlete své bance na adresu, kterou sami zadáte.
- **Neklikejte na odkaz a nestahujte přílohu**, místo toho zadejte adresu do svého prohlížeče.
- Pokud máte pochybnosti, **ověřte to** na webových stránkách vaší banky nebo do banky zavolejte.

#CyberScams

