

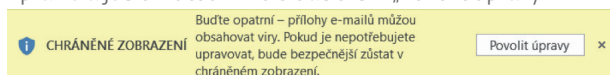
JAK SE BRÁNIT PHISHINGU

Manuál pro uživatele

01.

NEPOVOLUJTE MAKRA V PROGRAMECH

S makry se setkáte zejména v programech Microsoft Office. Zpravidla jde o žlutou linku s tlačítkem „Povolit úpravy“.



Pokud se jedná o škodlivou přílohu, povolením spustíte skript, který například může stáhnout další malware. Pokud dokument použití makra vyžaduje, pečlivě ověřte důvěryhodnost odesílatele.

03.

KONTROLUJTE E-MAIL ODESÍLATELE

Pokud obdržíte urgentní nebo neobvyklý požadavek e-mailem, dobře se podívejte na e-mailovou adresu odesílatele. Zkontrolujte část před i za @. Je doména přesná? Skutečně váš dodavatel používá tento formát jména? Neváhejte si urgentní požadavek ověřit po telefonu.

05.

NESDÍLEJTE SLUŽEBNÍ INFORMACE

Útočníci pro spearphishingové kampaně často sledují sociální sítě zaměstnanců konkrétní firmy. Hledají údaje o interním fungování, aby byl jejich podvod skutečně věrohodný. Proto nedoporučujeme veřejně sdílet informace o hierarchii společnosti a interních bezpečnostních a administrativních procesech.

02.

NEOTEVÍREJTE KAŽDOU PŘÍLOHU ČI ODKAZ V E-MAILU

Pokud zpráva vykazuje podezřelé znaky (je příliš urgentní nebo vám nabízí příliš dobrou nabídku), neotevírejte přílohu, ani neklikejte na řádné odkazy v e-mailu.

04.

KOMUNIKUJTE S IT

Máte z nějaké zprávy špatný dojem? Přepošlete ji na IT oddělení. Vaši administrátoři si s případnou hrozbou poradí.

06.

NEZADÁVEJTE CITLIVÉ INFORMACE

Pokud obdržíte e-mailem požadavek na aktualizaci přístupů do banky, nějakého programu nebo informací z platební karty, zbystřete. Renomované instituce podobné požadavky e-mailem nepošílají, vždy si tyto údaje nastavujte po přihlášení přímo v programu či bankovníctví. Přihlašujte se prostřednictvím oficiálních stránek, nikoli proklikem z e-mailu či vyhledávače.

Zdroj: ESET a Národní úřad pro kybernetickou a informační bezpečnost