Zadání: školicí video „Jak rozpoznat phishingový e-mail“

Cíl a rozsah

Krátké školicí video pro zaměstnance o tom, jak rozpoznat podvodný e-mail. Do firmy v poslední době chodí zprávy, které se vydávají za Microsoft. Video má na jednom konkrétním příkladu ukázat, na co si dát pozor a jak se zachovat.

- Délka: přibližně 2,5 minuty.
- Průvodce: avatar, který se představí jako Honza a má na starosti bezpečnost.
- Obraz: vedle avatara názorné obrázky ke každému bodu.
- Použití: školení nových zaměstnanců a rozeslání všem kolegům.

Obsah videa

Úvod

Honza se představí a řekne, že ukáže, jak poznat podvodný e-mail, který se vydává za Microsoft.

Příklad podvodného e-mailu

Zaměstnanci přijde e-mail o podezřelé aktivitě na účtu. Pokud do 24 hodin nepotvrdí svou totožnost, účet mu údajně zablokují. Zpráva vypadá jako oficiální upozornění. Má odesílatele Microsoft, předmět o neobvyklé aktivitě při přihlášení, údaje o přihlášení a tlačítko „Ověřit účet“. Video pak krok za krokem projde, podle čeho se dá podvod poznat.

1. Odesílatel

Jméno Microsoft si do zprávy může napsat kdokoli. Adresa na první pohled vypadá správně, ale skrývá jeden důležitý rozdíl. Písmeno „c“ ve slově Microsoft je ve skutečnosti znak z azbuky. Vypadá téměř stejně, ale jde o jiný znak, a tedy i o jinou internetovou adresu. Homografický útok musí být vysvětlený tak, aby ho pochopili i lidé bez technického zázemí. Video nemá tvrdit, že takto vypadá adresa v každé aplikaci, protože každý program ji může zobrazit jinak.

2. Časový tlak

Hrozba zablokování do 24 hodin má lidi přimět jednat ve spěchu a bez ověření. Podvodníci s tím počítají.

3. Odkaz

Tlačítko nabízí ověření účtu, ale může vést úplně jinam. Video ukáže, že na počítači stačí najet myší na odkaz, neklikat a zkontrolovat jeho skutečnou adresu. Na mobilu stačí odkaz podržet prstem. Pro srovnání uvede i pravou přihlašovací adresu Microsoftu 365.

4. Falešné přihlášení

Odkaz může otevřít falešnou přihlašovací stránku Microsoftu 365. Kdo na ní zadá heslo nebo ověřovací kód, může je předat útočníkům. Ani symbol zámku v adresním řádku nezaručuje, že je člověk na správném webu. Znamená jen šifrované spojení.

5. Pravopis

Video vyvrátí představu, že podvodný e-mail poznáte podle pravopisných chyb. Dnes bývají takové zprávy napsané naprosto bezchybně. Důležitější je ověřit odesílatele, odkazy a nečekané požadavky.

Co dělat

- Na podezřelý odkaz neklikat.
- Microsoft 365 otevřít přímo přes známou adresu nebo aplikaci.
- E-mail nahlásit IT oddělení.
- Kdo už své údaje zadal, okamžitě informuje IT a postupuje podle jeho pokynů.

Závěr

Krátké outro s heslem „Neklikejte. Ověřte. Nahlaste.“, které si lidé snadno zapamatují.

Požadavky na ukázky

- Všechny e-maily, adresy a stránky ve videu jsou jen ilustrační a zřetelně označené jako ukázka podvodu.
- Žádné skutečné adresy zaměstnanců.
- Nic, na co by se dalo kliknout.

Podklady

Grafika k jednotlivým bodům není k dispozici. Připraví ji dodavatel.