

CO JE TO VISHING?

Kamil KOPECKÝ

Vishing, neboli hlasový phishing, je forma sociálního inženýrství, kdy útočníci využívají telefonní komunikaci k získání citlivých informací od obětí. Tento typ útoku je obdobou phishingu, který se typicky odehrává prostřednictvím emailu, avšak vishing se zaměřuje na telefonické hovory nebo zprávy hlasové pošty.

Útočníci při vishingu často předstírají, že jsou z důvěryhodné organizace, jako jsou banky, pojišťovny, nebo dokonce státní instituce, a snaží se oběť přesvědčit, aby jim poskytla osobní, finanční, nebo jiné citlivé informace. Mohou také nalákat oběť k provedení určitých akcí, jako je převod peněz nebo zadání přihlašovacích údajů na podvodné webové stránky.

Jak se vishingu bránit?

1. **Nedůvěřujte neověřeným telefonním číslům:** Pokud vás kontaktuje osoba tvrdící, že reprezentuje určitou organizaci, a požaduje vaše osobní údaje, buďte opatrní. Ověřte si její totožnost zpětným vyhledáním oficiálního telefonního čísla organizace. Pozor, zobrazení telefonního čísla na mobilním telefonu může být zfalšováno!
2. **Nezadávejte citlivé informace:** Nikdy neposkytujte osobní, finanční nebo jakékoli jiné citlivé informace přes telefon, pokud nemáte absolutní jistotu, že hovor je legitimní.

-
3. **Používejte dvoufaktorovou autentizaci:** Kde je to možné, používejte dvoufaktorovou autentizaci pro vaše online účty, což může pomoci chránit vaše údaje i v případě, že se útočníkům podaří získat některé z vašich přihlašovacích údajů.
 4. **Vzdělávejte se a šířte osvětu:** Udržujte si aktuální informace o nejnovějších metodách sociálního inženýrství a sdílejte je se svými blízkými, aby i oni mohli rozpoznat a předejít možným hrozbám.

Vishing je sofistikovaná forma podvodu, která může mít vážné důsledky pro jednotlivce i organizace. Důležité je být vždy na pozoru, nevyzradit citlivé informace přes telefon a pravidelně se informovat o nových typech podvodů. Tím můžeme výrazně snížit riziko, že se staneme obětí vishingu.