Phishing

Phishing je forma podvodu, při které útočník vystupuje jako legitimní instituce (banka, státní úřad, doručovací služba, technická podpora). Komunikace probíhá nejčastěji prostřednictvím e-mailů, SMS zpráv nebo sociálních sítí. Hlavním nástrojem phishingu je vyvolání pocitu naléhavosti (např. „Váš účet byl zablokován“) nebo lákavé nabídky („Vyhráli jste iPhone“).

Jak phishing funguje

Útok obvykle sleduje tento scénář:

```
1. **Návnada:** Útočník rozešle hromadnou zprávu, která vypadá jako oficiální sdělení (např. od České pošty nebo Microsoftu).
2. **Hrozba/Výzva:** Zpráva obsahuje naléhavou výzvu k akci a odkaz na webovou stránku.
3. **Podvržená stránka:** Odkaz vede na falešný web, který je vizuálně k nerozeznání od originálu (včetně log a barev).
4. **Sběr dat:** Uživatel do formuláře na falešném webu zadá své údaje. Ty se okamžitě odešlou útočníkovi.
5. **Zneužití:** Útočník pomocí získaných údajů vybere bankovní účet, ukradne identitu nebo prodá data na černém trhu.
```

Typy phishingu

Název	Popis
Spear Phishing	Cílený útok na konkrétní osobu nebo firmu. Útočník si o oběti předem zjistí informace (jméno, kolegové), aby zpráva působila věrohodně.
Vishing	Phishing prováděný přes telefonní hovor (Voice Phishing). Útočník se vydává například za bankovního úředníka nebo policistu.
Smishing	Podvodné zprávy zasílané prostřednictvím SMS. Často informují o „nedoručeném balíčku“ s odkazem na doplatek cla.
Whaling	Typ spear phishingu zaměřený na „velké ryby“ – vysoce postavené manažery a ředitele firem (CEO fraud).
Angler Phishing	Útočník vytvoří falešný profil na sociálních sítích a reaguje na stížnosti zákazníků jménem oficiální podpory.

Na co si dát pozor (Varovné znaky)

Moderní phishing je velmi sofistikovaný, ale často ho prozradí detaily:

- **Podezřelá URL adresa:** Web vypadá jako pravý, ale v adresním řádku je např. `mojebanka-cz.com` místo `mojebanka.cz`.
- **Naléhavost a nátlak:** Snaha donutit vás k rychlé akci bez přemýšlení („Udělejte to do 10 minut, jinak přijdete o peníze“).
- **Gramatické chyby:** I když se kvalita překladů zlepšuje, stále se objevují nepřirozené obraty nebo strojový překlad.
- **Podezřelý odesílatel:** E-mail se tváří jako od „Podpory Apple“, ale adresa odesílatele je např. `apple-support73@gmail.com`.

Jak se chránit

- **Kontrolujte adresní řádek:** Vždy ověřujte doménu webu, na kterém zadáváte heslo.
- **Dvoufaktorové ověření (2FA):** Nejdůležitější ochrana. I když útočník získá vaše heslo, bez potvrzení v mobilu se k účtu nedostane.
- **Neklikejte na odkazy v e-mailech:** Pokud vám přijde výzva z banky, raději adresu banky sami napište do prohlížeče nebo použijte jejich oficiální aplikaci.
- **Používejte antivir a filtry:** Moderní e-mailové služby a prohlížeče většinu phishingových stránek automaticky blokují.

Související pojmy: Malware, Sociální inženýrství, HTTPS, Browser, DNS Spoofing, 2FA, MitM.