

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **141** ze dne **21.4.2026**

Jak se bránit sociálnímu inženýrství?

Když mluvíme o kybernetických útocích, máme tendenci soustředit se hlavně na jejich technologickou stránku a tu lidskou odsouvat tak trochu na pozadí. A to je chyba. Technologie jsou v tomto případě totiž jen prostředek, ne cíl. Tím jsme my, konkrétně naše osobní data a finanční údaje.

A jedním z nejsnadnějších způsobů, jak je z nás dostat, je sociální inženýrství.

Co je sociální inženýrství?

Sociální inženýrství je soubor technik, které útočníci využívají k psychologické manipulaci svých obětí. Cílem je většinou nasdílení přihlašovacích údajů, potvrzovacích kódů nebo nevědomá instalace malwaru.

Proč je sociální inženýrství tak úspěšné (a tím pádem nebezpečné)? Protože my, lidé, jsme nejen omylní, ale hlavně sociální bytosti naprogramované věřit ostatním lidem a příběhům, které nám vyprávějí. Zvláště, když je považujeme za autority.

"Sociální inženýrství funguje, protože zneužívá rozporu, který v nás vytváří vrozené sociální instinkty a naučené zásady kybernetické bezpečnosti," vysvětluje globální bezpečnostní poradce ESETu Jake Moore. "Řečeno jednoduše, sociální inženýři využívají naší důvěřivosti a dělají to hodně dobře."

Sociální inženýrství často nevyžaduje ani malware, ani sofistikované využívání zranitelností našich zařízení. To znamená, že útoky postavené na něm jsou hůř detekovatelné a hlavně levnější. Obě tyto výhody navíc ještě podpořil nástup generativní AI, která umožňuje snadno vytvářet např. bezchybné phishingové e-maily či přesvědčivé deepfaky.

Jak přesně funguje sociální inženýrství?

Moderní útok na bázi sociálního inženýrství většinou probíhá takto:

- **Průzkum.** Sociální inženýři si své oběti "šacují" podobně jako zloději nebo klasičtí podvodníci. Jako zdroje informací jim slouží naše sociální sítě, balíčky kradených dat z dark webu nebo (v případě útoků na firmy) zpravodajství z otevřených zdrojů (OSINT).
- **Plánování.** Na základě získaných informací si útočníci zvolí nejdůvěryhodnější kanál (např. e-mail, soukromou zprávu na sociálních sítích, QR kód nebo i osobní setkání), kterým útok uskuteční, a uvěřitelnou "návnadu".
- **Útok.** Útočník nahodí návnadu (např. urgentní žádost, příslib odměny, vzbuzení strachu či odvolání se na autoritu), oběť se chytí a provede požadovanou akci (např. klikne na podvodný odkaz, otevře škodlivou přílohu, převede peníze nebo prozradí své přihlašovací údaje).
- **Únik.** Útočník ukradne přihlašovací údaje, inkasuje poslané peníze nebo spustí nainstalovaný malware a užívá si plody své práce.
- **Reakce.** Poškozená strana si uvědomí, co se stalo, a ideálně začne podnikat kroky

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **141** ze dne **21.4.2026**

k nápravě.

Sociální inženýrství z pohledu psychologie

Sociální inženýrství a na něm založené kybernetické útoky nejsou v jádru ničím jiným než útokem člověka na člověka. Hlavní zbraní je v tomto případě manipulace, která je podle amerického psychologa Roberta Cialdiniho založená na následujících principech:

- **Autorita:** Lidé mají tendenci plnit pokyny těch, které vnímají jako vůdce, což je přesně důvod, proč se podvodníci často vydávají za pracovníky bank, státní úředníky, policisty apod.
- **Urgence/FOMO:** Pokud je na nás vyvíjen nátlak, že když nebudeme hned jednat, stane se něco špatného nebo nám něco vzácného uteče, zvyšuje se šance, že poslechneme. Tento typ manipulace hojně využívá phishing, např. výhružkou, že nám někdo do 24 hodin deaktivuje účet, nebo příslibem výhry, kterou je nutné vybrat včas.
- **Vzájemnost (reciprocita):** Lidé nemají rádi pocit, že jsou někomu něco dlužní, a mají často potřebu se revanšovat. Toho zneužívají třeba phishingové e-maily, které slibují dárek nebo produkt zdarma výměnou za to, že se někam přihlásíme, na něco klikneme apod.
- **Závazek:** Většina z nás se snaží zůstat v názorech a jednáních důsledná, což se projevuje například i tak, že pokud na nějaké podmínky přistoupíme jednou, nejspíš to uděláme znovu, i když se po nás tentokrát chce víc. Proto mají sociální inženýři tendence útoky opakovat.
- **Sociální schválení:** Lidé mají sklony jít s davem, takže pokud v nás někdo vzbudí dojem, že většina lidí udělala, co se po nás chce, existuje vyšší šance, že to uděláme taky. Toho se využívá např. při phishingových útocích na firmy, při kterých se zaměstnancům tvrdí, že kolegové už "potvrdili údaje".
- **Oblíbenost:** Většina lidí se rozhoduje na základě sympatií. To znamená, že pokud nám žádost předkládá někdo, kdo se nám líbí, spíš řekneme ano. Proto se sociální inženýři snaží vybudovat co nejpevnější vztah s obětí.

Sociální inženýrství není jen phishing

O tom, že podvody či krádeže dat založené na sociálním inženýrství často nejsou zvlášť technologicky vyspělé, už jsme mluvili. A co je to phishing nejspíš také znovu vysvětlovat nemusíme. Pojdme se tedy podívat na jeho možná méně známé formy:

- **Push bombing** je bombardování notifikacemi z aplikace pro vícefaktorové ověření. Cílem je příjemce zmást nebo doslova "uhnout", aby aspoň jedno z nich potvrdil.
- **Quishing** je phishing pomocí QR kódu, který bývá vyvěšený na veřejných místech nebo zaslaný e-mailem. Stejně jako v případě klasického phishingu vede uživatele na podvodné stránky nebo ke stažení malwaru.
- **ClickFix** je poměrně nový způsob, jak do zařízení oběti dostat malware. V první fázi jde

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **141** ze dne **21.4.2026**

o klasický phishing, ale jakmile oběť dorazí do cíle (např. na falešnou stránku), vyskočí jí upozornění, že došlo k dočasné chybě, kterou může opravit jen tak, že zkopíruje a vloží kód do příkazového řádku. Tím nainstaluje malware.

Mezi metody sociálního inženýrství, které se neopírají o phishing, patří třeba milostné podvody, podvody na (pra)rodiče nebo sextorze. Tyto typy podvodů hojně využívají deepfaky vytvořené pomocí generativní umělé inteligence, které útočníkům usnadňují vydávat se za někoho jiného nebo vytvořit falešný pornografický materiál pomocí fotek ze sociálních sítí.

Jak se bránit sociálnímu inženýrství?

Metody sociálního inženýrství a způsoby, jak je na nás uplatnit, jsou různé, ale jedno mají většinou společné: žádost o peníze a/nebo přihlašovací či jiné důvěrné údaje. Pokud na takovou žádost narazíme, je naprosto zásadní nechat si ji pořádně projít hlavou.

"Pokud v nás někdo vyvolává urgenci nebo strach, je potřeba zpomalit a všechno si ověřit," radí Jake Moore. "Většina útoků sociálního inženýrství se totiž zhroutí ve chvíli, když se odpojíme od platformy, kterou sociální inženýři k útoku používají, a tím narušíme příběh, který nám vyprávějí. To je přesně důvod, proč se nás snaží např. udržet na telefonu, dokud neuděláme, co chtějí."

Odolnost proti sociálnímu inženýrství můžete podpořit následujícími kroky:

- Zvyšujte si povědomí o tom, jaké typy podvodů existují a jaké metody a technologie používají.
- Aktivujte si všechny bezpečnostní prvky, které vám technologie a platformy umožňují (např. vícefaktorové ověření), a pořiďte si dobrý antivir s ochranou proti phishingu nebo blokadě pochybných telefonních čísel.
- Mluvte o hrozbách sociálního inženýrství otevřeně, a to hlavně doma s dětmi a seniory, na které podvodníci cílí také.

AV centrum ČR