

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **115** ze dne **12.8.2025**

Nepropadejte panice! Jak se chránit před hrozbou typu scareware

Žijeme v uspěchané době, čehož jsou podvodníci připraveni kdykoli zneužít. Velmi často navíc těží ze špatných zpráv, na které chtě nechtě reagujeme. Strach může být silnou zbraní a podvodníci vědí, jak ho v lidech vyvolat a přimět je k unáhleným krokům. V kyberprostoru k tomu běžně využívají tzv. scareware.

Co je scareware?

Scareware se vás pokusí přesvědčit, že vaše zařízení napadl nějaký malware. Zničehonic se objeví spousta oken nebo notifikací, které se vás snaží vyděsit. Cílem útočníků je zpravidla prodat vám nějaký program, který neexistující malware odstraní, případně z vás vymámit osobní/finanční údaje nebo nainstalovat skutečný malware.

Jak se scareware se šíří?

Automaticky pop up okna: Tato okna se automaticky otevrou po kliknutí na nějaký odkaz, při navštívení webové stránky nebo otevření konkrétní aplikace. Může se v nich uvádět, že váš počítač infikoval nebezpečný malware. A to jediné, jak zachránit situaci, je kliknout na vyskakovací okno a stáhnout neexistující antivirový nástroj.

E-maily a zprávy na sociálních sítích: O stejný trik se mohou útočníci pokusit i prostřednictvím nevyžádaných e-mailů. Text se vás snaží přimět, abyste okamžitě odstranili infekci malwarem zjištěnou ve vašem zařízení. Tyto zprávy mohou dokonce přicházet z legitimně vypadajících, ale falešných e-mailových adres. Příložený odkaz nebo tlačítko vás po kliknutí přesměruje na škodlivou stránku nebo spustí stahování.

Podvodné reklamy: To samé mohou dělat i škodlivé reklamy na legitimních stránkách nebo sociálních sítích, které vyzývají uživatele, aby si stáhli "antivirový software" a odstranili neexistující malware.

Telefonáty s technickou podporou: Někdy podvodné notifikace nebo zprávy obsahují číslo na technickou podporu, které vás přesměruje do podvodného call centra. Tam vás "specialista" ihned informuje o napadení zařízení. Podvodníci vás mohou požádat o stažení softwaru pro vzdálený přístup, aby mohli problém "vyřešit". Ve skutečnosti se budou snažit získat vaše osobní údaje nebo vás přimět zaplatit za služby, které nepotřebujete.

Někdy vám mohou podvodníci z falešné technické podpory zavolat nečekaně a zkusit to s podobnou lží. Tyto podvody se dějí už více než deset let a v roce 2023 byly podle FBI třetím nejvýnosnějším typem počítačové kriminality – podvodníkům vynesly přes 924 milionů dolarů.

Nenechte se scarewarem vyděsit

Scareware využívá klasické techniky sociálního inženýrství. Útočníci se snaží oběť přimět k unáhlenému rozhodnutí a nedávají jí čas na rozmyšlenou. Varování bývá výrazné a má vyvolat pocit naléhavosti – například: "Jednete HNED, jinak mohou být vaše soubory a fotografie NAVŽDY ztraceny."

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **115** ze dne **12.8.2025**

Podvodníci používají blikající červené prvky, velká písmena a falešné snímky obrazovky s údajně infikovanými soubory, případně také zobrazují falešný průběh kontroly počítače. Podvodníci proto napodobují značky známých dodavatelů bezpečnostních řešení a používají názvy jako DriveCleaner, Antivirus360, PC Protector nebo Mac Defender.

Co může scareware způsobit?

V tom lepším případě vyhodíte peníze za zbytečný program. Sice zaplatíte za "nic", ale aspoň tím podvod končí. V horším případě zločinci získají vaše osobní a finanční údaje, které mohou zneužít k dalším podvodům. Případně si kliknutím na odkaz nebo reklamu nevědomky nainstalujete další malware.

Jak se vyhnout scarewaru

Ochrana před scarewarem není nijak složitá. V první řadě nereagujte na taková varování ihned.

- Nikdy neklikejte na vyskakovací okno. Pokud název "antivirového nástroje" nepoznáváte, ověřte si jej ve spolehlivém zdroji, například přes Google.
- Zavřete webový prohlížeč nebo se odpojte od internetu. Ve Windows stiskněte Ctrl+Alt+Delete, otevřete Správce úloh a ukončete úlohu prohlížeče. V macOS stiskněte Command+Option+Escape pro vynucené ukončení. Nebo zařízení jednoduše vypněte.
- Používejte důvěryhodné blokátory reklam/pop-up oken, abyste snížili riziko zobrazení scareware. Mnohé z nich škodlivé prvky zastaví dříve, než vám mohou vyskočit na obrazovce.
- Pravidelně aktualizujte webový prohlížeč. starší verze bývají zranitelnější.
- Nainstalujte si legitimní bezpečnostní software od ověřeného dodavatele a udržujte jej aktuální.

Jak odstranit scareware

Pokud se scareware dostane do vašeho počítače nebo mobilu, jeho odstranění by nemělo být složité. Pamatujte, že nejde o skutečný malware. Stačí spustit důvěryhodný antivir, který scareware rozpozná, a poté se řídit pokyny pro odstranění.

Zdroj: AVcentrum ČR