### Jak může útočník získat vaše přihlašovací údaje na veřejné Wi-Fi?

# Jak může útočník získat heslo (vysoká úroveň)

1. **Phishing / falešné přihlašovací stránky (evil twin / captive portal)**
   Útočník postaví veřejnou Wi-Fi s názvem podobným té vaší (evil-twin) nebo nasadí falešný „captive portal“ — stránku, která vypadá jako legitimní přihlášení služby. Uživatel zadá heslo přímo do podvodné stránky a útočník ho získá. Taková stránka může mít i HTTPS (platný certifikát) — viz níže.

2. **Man-in-the-middle s falešným certifikátem / kompromitovaný certifikační úřad**
   HTTPS je bezpečné jen pokud prohlížeč důvěřuje certifikátu. Pokud uživatel ignoruje varování o certifikátu (nebo má v systému nainstalovaný škodlivý kořenový certifikát), útočník může „vidět“ obsah. Kompromitovaný nebo zlovolný CA může vydat certifikát i bez vašeho vědomí (vzácné, ale možné).

3. **Malware nebo keylogger na zařízení**
   Pokud je zařízení kompromitováno (malware, keylogger), útočník získá přihlašovací údaje dříve, než je šifrování použije — HTTPS nic neřeší, když jsou údaje ukradeny přímo na koncovém bodě.

4. **DNS nebo router hijacking — přesměrování na podvodnou stránku**
   Útočník může změnit DNS nebo upravit provoz přes kompromitovaný router tak, aby vás přesměroval na podvodnou stránku, která vypadá jako originál. Pokud stránka není přesně stejná doména, prohlížeč může upozornit na certifikát — ale mnoho lidí si toho nevšimne.

5. **Znovupoužívání hesel a získání údajů z jiného úniku**
   Útočník může získat heslo z úplně jiného úniku a zkusit ho na vaší službě (credential stuffing). HTTPS přenos nebrání tomu, že používáte stejné heslo jinde.

6. **Session hijacking / cookie theft (pokud služba špatně nastaví zabezpečení cookie)**
   I když je obsah šifrovaný, pokud stránka používá nezabezpečené cookies nebo nevlastní atributy Secure / HttpOnly / SameSite, může dojít k odcizení session. To je méně pravděpodobné u moderních dobře navržených služeb, ale může se stát.

# Proč „mám HTTPS, tak jsem v bezpečí“ není vždy pravda

- HTTPS chrání data během přenosu mezi vaším zařízením a serverem, ale nechrání: samotné zařízení, falešné stránky, phishing, uživatelské chyby (přijetí varování), nebo chyby serveru (špatné nastavení cookie, znovupoužívání hesel).

- Pokud zadáte heslo do falešné stránky (i když má zelený symbol zámku — zámek jen říká, že přenos je šifrovaný, ne že stránka je legitimní), útočník ho má.

# Praktická doporučení — co dělat na veřejné Wi-Fi

Krátký checklist, který skutečně snižuje riziko:

1. **Používejte dvoufaktorové ověřování (2FA)** — i když někdo získá heslo, bez druhého faktoru obvykle nic neudělá. Nejlepší volba: hardwarové klíče (FIDO2) nebo autentifikátor (TOTP). SMS je lepší než nic, ale méně bezpečná.

2. **Používejte jedinečná hesla + správce hesel** — zabráníte credential stuffing a phishingu

tím, že správcem hesel se automaticky nedoplňují údaje na jiných doménách.

3. **Nepřihlašujte se přes veřejné Wi-Fi k důležitým účtům, pokud to není nutné** — nebo používejte VPN, která šifruje celý provoz (snižuje riziko MITM a snoopingu na místní síti).

4. **VPN** — spolehlivá placená VPN nebo firemní VPN je silná ochrana v nezabezpečených sítích; ale i VPN může být kompromitována, takže vybírejte důvěryhodného poskytovatele.

5. **Kontrolujte varování o certifikátu** — nikdy nepřeskakujte varování „nezabezpečené připojení / certifikát neplatný“ a nedovolujte instalovat neznámé root certifikáty.

6. **Nenechte zařízení automaticky připojovat k otevřeným sítím** — vypněte automatické připojování a ověřujte SSID.

7. **Aktualizace OS a aplikací** — opravují chyby, které by útočník mohl zneužít.

8. **Používejte správce hesel, který nevyplní přihlašovací údaje na falešné doméně** — to je silná obrana proti phishingu.

9. **Pozor na captive portály** — pokud vás web přesměruje na přihlášení do „Wi-Fi portálu“, pečlivě si přečtěte, co po vás chtějí. Nikdy tam nezadávejte hesla pro jiné služby (Google, banku, apod.).

10. **Preferujte HTTPS stránky s HSTS a moderním nastavením** — většina velkých služeb má HSTS, což znemožňuje SSL-stripping; stále si ale ověřte doménu.

# Co dělat, když máte podezření, že heslo uniklo

- Okamžitě změňte heslo na napadené službě a všude, kde jste heslo znovu použil/a.
- Zaveďte 2FA na dotčeném účtu.
- Zkontrolujte zařízení na malware a spusťte antivirovou kontrolu.
- Pokud šlo o bankovní/platební údaje, kontaktujte banku.

---

Shrnutí: HTTPS je zásadní, ale není jediná obrana. Útočník často cílí na člověka (phishing), na zařízení (malware), nebo na důvěřující chování (ignorování varování). Nejlepší obrana: MFA (ideálně hardwarová), jedinečná hesla + správce hesel, VPN na veřejných sítích, nepřihlašovat se na veřejných Wi-Fi bez potřeby, a neignorovat varování prohlížeče.

Unique solution ID: #1174
Author: n/a
Last update: 2025-09-15 11:08