

# JAK NA INTERNET

## Veřejné počítače

Pokud používáte počítač, který nemáte pod kontrolou vy, ani nikdo komu důvěřujete, je potřeba vždy dbát zvýšené opatrnosti. Zejména při používání počítačů v hotelech, v knihovně či v internetové kavárně. Pokud se z takového počítače připojujete do nějaké služby vyžadující jméno a heslo, je potřeba se vyvarovat některých akcí:

- Pokud se prohlížeč zeptá na uložení vašeho jména a hesla, nesmíte mu to povolit.
- Dále je potřeba se vyvarovat použití trvalého přihlášení.
- Při ukončení práce s prohlížečem je také potřeba se před jeho uzavřením nezapomenout odhlásit.
- Buďte ostražití, dávejte pozor na lidi, pohybující se okolo vás. Mohou vás sledovat a pokoušet se odpozorovat například vaše přihlašovací údaje.
- Pokud možno nikdy nepracujte na veřejném počítači s důvěrnými informacemi, nezasílejte čísla platebních karet ani se nepřihlašujte do citlivých služeb, jako je například internetové bankovníctví. Riziko zneužití je na těchto počítačích příliš vysoké.
- Používejte také privátní mód prohlížeče, při kterém prohlížeč neukládá žádné údaje o průběhu Vašeho sezení, tedy ani navštívené stránky, či dočasné soubory.

### Opatrně s veřejnou wi-fi

Samostatnou kapitolou jsou veřejně dostupné wi-fi sítě a jejich používání. Na veřejných wi-fi sítích se vyvarujte přihlašování do služeb, které nevyžadují pro přihlášení https. Pokud se přihlásíte na službu pomocí http, existuje velké riziko odchytnutí jména a hesla útočником. Avšak ani při použití https není útok nemožný. Pokud by Vám prohlížeč při připojení přes veřejnou wi-fi začal dávat varovné hlášení o neplatném, či jinak poškozeném certifikátu, okamžitě práci na dané stránce ukončete.

Také si průběžně kontrolujte, že váš prohlížeč nadále používá https. Existuje útok, při kterém se útočník vloží mezi oběť a server a prohlížeč oběti donutí přejít na http. Přijímá nechráněné informace z prohlížeče oběti (například jméno a heslo internetového bankovníctví) a sám pak se serverem banky komunikuje pomocí https. Oběti pak posílá přes http všechny odpovědi od serveru. Ta tak nemá šanci si probíhajícího útoku všimnout, pokud nezaznamená změnu protokolu z https na http. Proto při využívání veřejných wi-fi sítí a to i těch chráněných heslem je potřeba dbát zvýšené pozornosti.

### Rada na závěr

Pokud pro Vás není nezbytně nutné veřejně dostupné počítače používat, raději je nepoužívejte. Nebo je využívejte pouze pro shlédnutí zpráv nebo jako zdroj informací.

