Základní bezpečnostní opatření při prohlížení internetu

1. Používejte aktualizovaný Antivirový Software:

Co to znamená: Antivirový software je nástroj navržený k detekci, blokování a odstraňování škodlivého softwaru, jako jsou viry, spyware a malware, které mohou poškodit váš počítač nebo odcizit vaše osobní údaje.

Proč je to důležité: Aktualizovaný antivirový software dokáže rozpoznat a chránit váš počítač před nejnovějšími hrozbami, protože bezpečnostní hrozby se neustále vyvíjejí. Pravidelné testování počítače může odhalit skryté nebezpečí.

2. Rozpoznávání falešných webových stránek:

Co to znamená: Falešné webové stránky jsou vytvořeny s cílem podvádět uživatele a získat od nich citlivé informace, jako jsou přihlašovací údaje nebo finanční údaje.

Vždy věnujte pozornost webové adrese, která se skrývá pod odkazem, např. v e-mailu. Jakmile vám přijde adresa podezřelá nebo neodpovídá názvu

Proč je to důležité: Buďte obezřetní při klikání na odkazy v e-mailech nebo na webových stránkách, které vypadají podezřele. Falešné stránky mohou napodobovat ty skutečné a snažit se napáchat podvody.

Škodlivost stránek můžete zjistit i přes speciální stránky určené k validaci URL jako např. https://www.psafe.com/dfndr-lab/

3. Varování před nebezpečnými soubory:

Co to znamená: Nebezpečné soubory mohou obsahovat škodlivý software a představovat riziko pro váš počítač a osobní údaje.

Proč je to důležité: Při stahování souborů z internetu a otevírání e-mailových příloh buďte obezřetní. Neotevírejte soubory z neznámých zdrojů a dejte pozor na varování antivirového softwaru. Pravidelně aktualizujte bezpečnostní software a systém, abyste byli chráněni před nejnovějšími hrozbami.

4. Dodržujte bezpečné návyky při stahování:

Co to znamená: Vyhněte se stahování souborů z neznámých a neověřených zdrojů. Mějte na paměti, že pirátský obsah může být rizikový, protože jsou často zdrojem virů.

Proč je to důležité: Stahování souborů z důvěryhodných zdrojů minimalizuje riziko nákazy počítače škodlivým softwarem. Nepoužívejte nelegální nebo neověřený software, protože může obsahovat skrytý malware.

5. Pravidelně zálohujte data:

Co to znamená: Pravidelně zálohujte důležitá data, abyste minimalizovali ztrátu informací v případě útoku škodlivého softwaru nebo hardwarové poruchy.

Proč je to důležité: Zálohy vám umožní obnovit data v případě potřeby a minimalizovat dopady na vaše osobní nebo pracovní informace.

Tato základní bezpečnostní opatření by měla být součástí vašeho běžného chování při prohlížení internetu, aby byla zajištěna vaše online bezpečnost a ochrana osobních údajů. Více informací o bezpečnosti se dozvíte v lekci: Zabezpečení a ochrana osobních údajů online.