UNITED NETWORKS

INTERNET MOBIL TELEVIZE

JAK SE BEZPEČNĚ CHOVAT V DIGITÁLNÍM PROSTŘEDÍ

Preferujte weby s HTTPS a bezpečné zdroje dat 	Při prohlížení webových stránek se ujistěte, že adresa začíná "https://" a nikoliv jen "http://". To přidané písmenko "s" znamená, že komunikace mezi vámi a webem je šifrovaná a méně náchylná k odposlechu. Zkontrolujte také, zda web, na který se připojujete, je důvěryhodný a má platný certifikát. Nikdy neklikejte na odkazy v nevyžádaných e-mailech nebo podivných zprávách. Často vedou na stránky, kde není zajištěna bezpečná komunikace. Pozorně prozkoumejte zdroj komunikace. Ověřujte si odkazy, než na ně klikněte.
Dnešní routery umí velmi jednoduše zřídit na vaše přání wifi síť pro hosty, která je oddělená od vaší domácí sítě.	**Budte pozorný hostitel, vytvořte svým hostům vlastní wifi síť** 
Zálohujte svá data a chraňte se proti ransomware 	Pravidelně zálohujte svá osobní data (fotky, dokumenty) na externí úložiště nebo do důvěryhodného cloudového prostředí. To je klíčové pro ochranu před ransomwarem, zlým softwarem, který může zašifrovat vaše soubory a hacker pak může požadovat výkupné za jejich odblokování. Mějte vždy aktuální antivirový software, který dokáže detekovat a zastavit pokusy o infekci ransomwarem a dalším internetovým neřádstvem.
Při připojování k internetu mimo domov, třeba na veřejné Wi-Fi sítě, buďte obezřetní. Takové sítě často nejsou šifrované, což znamená, že vaše data mohou být snadno odposlechnuta. Doporučujeme používat prověřenou virtuální privátní síť (VPN), která šifruje vaši komunikaci a zvyšuje bezpečnost. Vyhýbejte se citlivým operacím, jako je přihlášení do bankovnictví nebo zadávání hesel, pokud se pohybujete v nedůvěryhodném prostředí. Buďte opatrní, pokud používáte cizí počítač nebo mobil. Neukládejte si do něj hesla ani jiné citlivé informace.	**Dávejte pozor, kde se připojujete** 

UNITEDNETWORKS
Nepomucká 1232/215, 326 00 Plzeň
IČ: 035 79 051
373 705 705 info@u-n.cz www.u-n.cz

Aktualizujte pravidelně operační systém a aplikace

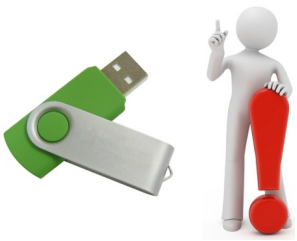
Pravidelně aktualizujte svůj operační systém v počítači a mobilu a nainstalované aplikace. Aktualizace často obsahují opravy bezpečnostních chyb, které by mohly být zneužity hackery. Pokud používáte zařízení, které již nemá podporu aktualizací (například starší verze operačního systému), zvažte jeho výměnu nebo buďte obzvláště opatrní při jeho používání. Ale vězte, že doba od připojení neaktualizovaného operačního systému k internetu do jeho napadení škodlivým softwarem se počítá na minuty. Napadení není riziko, napadení je jistota!

Používejte antivir a systémový firewall

Antivirový software je základem pro ochranu vašeho zařízení před malwarem, viry a jinými škodlivými programy. Ujistěte se, že máte nainstalovaný spolehlivý antivirový program a že je pravidelně aktualizován. V případě, že antivirus detekuje hrozbu, postupujte podle jeho pokynů a nezanedbávejte žádná varování. Pravidelně testujte své zařízení, abyste se ujistili, že je v pořádku.

Většina moderních operačních systémů, jako je Windows (Windows Defender Firewall) nebo macOS (Application Firewall), má svůj vlastní integrovaný firewall, který může uživatel konfigurovat podle svých potřeb. Nikdy nepovolujte instalaci aplikací, kterým nedůvěřujete.

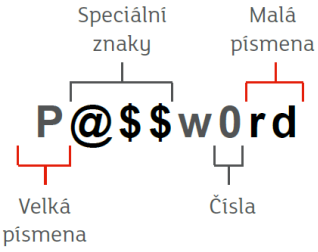
Důvěřuj, ale prověřuj



Nikdy neotvírejte soubory z neznámých paměťových zařízení, která jste nalezli třeba na chodníku, v práci, v hospodě nebo v parku, protože mohou obsahovat škodlivý software. I kdyby se soubor na flash disku jmenoval třeba "Odměny zaměstnanců.xls".

Nakupujte jen u prověřených e-shopů. Pokud máte pochybnosti, zkontrolujte, zda e-shop není v seznamu rizikových obchodů České obchodní inspekce.

Používejte silná hesla a dvoufaktorovou autentizaci



Vytvářejte silná a jedinečná hesla pro každou svou službu. Používejte kombinaci velkých a malých písmen, číslic a speciálních znaků. Pro jednodušší správu a tvorbu hesel můžete používat speciální aplikace – password managery.

Kde je to možné, aktivujte dvoufaktorovou autentizaci (2FA), která přidává další vrstvu zabezpečení, obvykle v podobě kódu zaslaného na váš telefon.

Nikomu svá hesla nesdělujte!