

8. Důvěřujte, ale ověřujte: Pokud vás kontaktuje online zástupce banky, pojišťovny či jiné instituce s nabídkou služby, tak se nebojte identitu dané osoby ověřit. Lze například zavolat na informační linku dané instituce.

9. Komunikujte s rodinou a přáteli: Pokud jste si něčeho nejisti, zeptejte se svých blízkých nebo důvěryhodné osoby.

10. Zdravý rozum: Jako v reálném světě, i na internetu platí, že pokud se něco zdá příliš dobré na to, aby to byla pravda, pravděpodobně to tak je. Vždy používejte svůj zdravý rozum.



Podnikatelé

1. Bezpečná komunikace: Při komunikaci s klienty nebo zákazníky používejte vždy zabezpečené metody. Nikdy nesdílejte důvěrné informace prostřednictvím nezabezpečených kanálů.

2. Zabezpečení dat: Používejte silná hesla a dvoufázovou autentizaci k ochraně svých účtů a dat. Pravidelně zálohujte svá důležitá data.

3. Ochrana proti kybernetickým hrozbám: Ujistěte se, že vaše zařízení jsou chráněna nejnovějším antivirovým softwarem a firewalllem. Pravidelně provádějte aktualizace softwaru a systému.

4. Pozor na podvody a phishing: Bud'te opatrní na e-maily nebo zprávy, které vypadají podezřele. Tyto mohou být pokusy o phishing, které se snaží získat vaše citlivé informace.

5. Vzdělávání zaměstnanců: Ujistěte se, že vaši zaměstnanci jsou vzdělávání v otázkách kybernetické bezpečnosti. Zaměstnanci by měli vědět, jak rozpoznat a zacházet s potenciálními hrozbami.

6. Používání bezpečných platebních metod: Při provedení transakcí online vždy používejte zabezpečené platební metody. Vyhněte se poskytování citlivých finančních informací, pokud si nejste jisti, že jsou bezpečné.

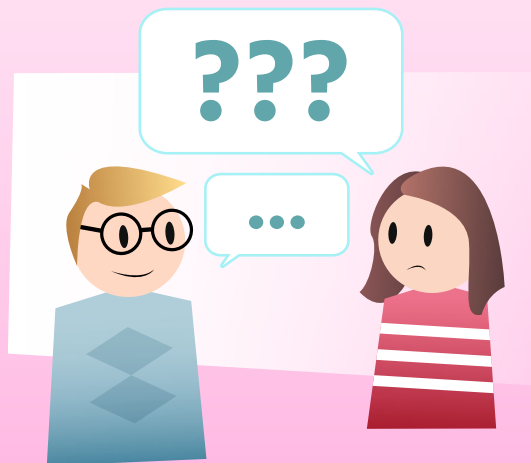
7. Plán pro kybernetickou bezpečnost: Měli byste mít jasný plán pro kybernetickou bezpečnost, který zahrnuje preventivní opatření, postupy pro řešení incidentů a plán obnovy v případě nějakého incidentu.

8. Omezení přístupu k informacím: Ne všichni zaměstnanci potřebují přístup ke všem informacím. Omezte přístup k citlivým datům na minimum potřebných osob.



9. Zabezpečení fyzických prostor: Kromě digitálních hrozeb je důležité chránit také své fyzické prostředky. Ujistěte se, že vaše kanceláře a zařízení jsou bezpečné.

10. Využívání odborného poradenství: Pro řešení otázek týkajících se kybernetické bezpečnosti využijte odborné poradenství. Toto může zahrnovat najmutí interního bezpečnostního týmu nebo spolupráci s externí bezpečnostní firmou.



BEZPEČÍ NA INTERNETU

Rady pro děti a rodiče,
seniory i podnikatele.



DĚTI A JEJICH RODIČE

1. Omezit osobní informace: Nikdy nesdílejte informace, jako je jméno, adresa, telefonní číslo nebo název školy na veřejných internetových fórech nebo sociálních médiích.

2. Hesla: Vždy si zvolte silná hesla a pravidelně je měňte. Nikdy nesdílejte svá hesla s nikým, ani s nejlepšími přáteli.

3. Kontrola online přítomnosti: Rodiče mohou zkontrolovat online obraz svého dítěte. Zkuste napsat jeho jméno do vyhledávače a podívejte se, co se objeví.

🔍 Michal Novák



FRAJER_MIKE_384
(Michal Novák)



4. Pozor na neznámé odkazy a e-mail: Nikdy neklikejte na odkazy od neznámých zdrojů. To může vést k infekci počítače škodlivým softwarem.

5. Omezení času stráveného u počítače: Příliš mnoho času stráveného u počítače může vést k fyzickým problémům, jako je bolest zad nebo očí. Je důležité mít pravidelné přestávky a věnovat se i jiným aktivitám.

6. Respektování ostatních: Stejně jako v reálném životě, i na internetu je důležité zachovávat slušné chování a respektovat ostatní.

Ahoj Michale 😊

Ahoj teto, ...

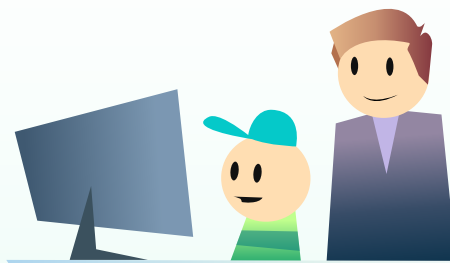
7. Používání aktualizovaného antivirového softwaru:

Měli byste vždy používat aktuální verzi antiviru, aby byl váš počítač co nejvíce chráněn.

8. Více zdrojů: Pokud narazíte na něco, co nechápete nebo co vás znepokojuje, měli byste se obrátit na dospělého. To může být rodič, učitel nebo jiná důvěryhodná osoba.

9. Kyberšikana: Pokud se setkáte s kyberšikanou, je důležité o tom informovat dospělého. Nikdy se nezapojujte do šikany, ani když jste jen svědkem.

10. Rodičovský dohled: Děti by měly používat počítač nebo jiná zařízení s přístupem na internet v přítomnosti dospělé osoby nebo pod jejich dohledem.



SENIORŮ

1. Omezit osobní informace: Stejně jako u dětí, je důležité nezveřejňovat osobní údaje, jako jsou vaše adresa, telefonní číslo nebo bankovní údaje na internetu.

2. Pozor na podvody a phishing: Buďte opatrní při otevírání e-mailů nebo zpráv od neznámých odesílatelů. Nikdy neklikejte na odkazy nebo přílohy v těchto zprávách, mohou obsahovat škodlivý software.

3. Používejte silná hesla: Mějte různá a silná hesla pro různé účty. Heslo by mělo být kombinací písmen, číslic a symbolů.

4. Aktualizujte svůj software: Pravidelně aktualizujte operační systém a aplikace, včetně antivirového softwaru. Tyto aktualizace často obsahují opravy bezpečnostních chyb.

5. Používání aktualizovaného antivirového softwaru: Měli byste vždy používat aktuální verzi antivirového softwaru, aby byl váš počítač co nejvíce chráněn.

6. Vzdělávejte se o internetové bezpečnosti: Je důležité se neustále učit a být informováni o nových hrozbách a nejlepších postupech pro bezpečnost na internetu.

7. Opatrně s online nákupy: Při nakupování online se ujistěte, že stránka je zabezpečená (adresa začíná na "https") a že se jedná o důvěryhodný prodejce.



<https://www.google.cz>



VŠB TECHNICKÁ
UNIVERZITA
OSTRAVA

FAKULTA
ELEKTROTECHNIKY
A INFORMATIKY