

Médiím na kloub

K internetu si dejte
Selský rozum

Čtení
pro seniory
o zdravé
konzumaci
médií



**Dobrý
sluha,
zlý pán**

Pohyb na internetu přináší celou řadu výhod a příležitostí. Je například skvělé, že se můžete spojit se svou vzdálenou rodinou nebo s přáteli z mládí, kteří žijí v zahraničí. Snadno na něm vyhledáte informace, a máte tak neustálý přehled, co se děje. Bez dodržování základních zásad bezpečného chování a kritického odstupu nad množstvím informací, které se po síti šíří, se však internet může stát i nebezpečným místem. Jak praví jedno staré úsloví. Je to dobrý sluha, ale zlý pán.

Na následujících stránkách vám proto přinášíme rady a tipy, které vám pomohou případné nebezpečí včas odhalit a předejít nejrůznějším problémům. Internetu ani množství informací, které nabízí, se nemusíte obávat. Je ale důležité pohybovat se na něm s rozumem a vědět, na co je potřeba si dávat pozor.

**Jak přijít médiím
na kloub?**

**Stačí
jen dál
číst**



Ověřujte a prověřujte

Internet je zdrojem nepřehledného množství informací a zpráv, které se k příjemci dostanou přímo bleskově. Je skvělý v tom, že na něm najdete cokoli, co potřebujete, co vás zajímá nebo co nevíte. Recepty, návody, zápisky z cest a mnoho dalšího. V podstatě o všem už někdo něco na internetu napsal. To s sebou však nese i nevýhody – právě z toho důvodu, že na internetu může psát a šířit informace v podstatě každý. Je tak nezbytné informace a zprávy ověřovat a nevěřit všemu, co čtete nebo vidíte.

Můžete totiž narazit i na záměrně zkreslené informace, úmyslně lživé články, které mají jediný cíl: ovlivňovat a manipulovat – říká se jim dezinformace či fake news.



Takové zprávy pojednávají například o citlivých tématech, která se dotýkají otázek národní bezpečnosti, třeba migrace, a tvoří pak rozpory a špatnou náladu ve společnosti.

Ve skutečnosti jsou plné polopravd. Na téma se totiž dívají jednostranně a sledují jen zájmy autora. Český internet takto například obletěla falešná zpráva, že rozdělení ČSFR v roce 1992 je neplatné. Klamat ale může i obraz – počítačově upravená fotografie či manipulativně sestříhané video.



Jiné zprávy mohou být jen šikovně **skrytou reklamou**, která se tváří třeba jako seriózní vědecká studie. Čtete o zázračném léku, krému či přípravku na hubnutí? **Podívejte se, jestli u textu není malými písmeny napsáno**

„inzerce“ či „komerční sdělení“. A neplatí to jen pro internet. Na podobné triky narazíte i v novinách, časopisech nebo v televizi.

Snadná dostupnost informací svádí k principu nejmenšího úsilí. Jakmile člověk získá odpověď na určitou otázku, opadá jeho pozornost a potřeba informaci si ověřit. Právě to mějte vždy na mysli – být obezřetní a snažit se na informace dívat kriticky. Ptát se: Je to pravda? Nebo je to celá pravda? Novináři se učí ověřovat získané informace minimálně ze dvou na sobě nezávislých zdrojů. Zkuste si na ně při hledání informací zahrát.

Pokud se jedná například o zpravodajství, v žádném případě nečtěte jen nadpisy – titulky. Často mohou být zavádějící a nikdy se do nich nevejde všechno. I titulky už nás ale mohou varovat. Pod slovy „Šok!“, „Skandál!“ a podobně se seriózní zpráva většinou neskrývá, mají jen čtenáře nalákat, aby si dané noviny na stánku koupil nebo na internetu kliknul na příslušný článek.

Dál se vyplatí sledovat, kdo je autorem zprávy – můžete se podívat i na jeho jiné texty a jejich charakter. Občas se autoři skrývají

za zkratkami, jedna z nejčastějších „čtk“ patří České tiskové kanceláři, tuzemské veřejnoprávní zpravodajské agentuře.



Pokud autor není u článku uvedený a nemá další texty, je to podezřelé. Důležitým vodítkem je také to, z jakých zdrojů autor čerpá. Pokud zdroje neuvádí a neodkazuje se dále, rapidně tím důvěryhodnost zprávy klesá.

V neposlední řadě se zkuste zamyslet také nad tím, komu médium, ve kterém zpráva vychází, patří. Nemohou být jeho zprávy zaujaté vůči konkurenci? Znáte to: Koho chleba jíš, toho píseň zpívej.

Pět otázek k zamyšlení

Kdo je autorem zprávy? Kdo ji šíří?

Co je hlavním sdělením zprávy? Co v textu chybí? Co se dá ověřit?

Jak se zpráva šíří? Jaké emoce má vyvolat?

Proč zpráva vznikla? Proč se snaží vyvolat určité pocity?

Komu je zpráva určena? Komu může prospět a komu uškodit?

Heslo je jako klíč od bytu

Pokud se chcete bezpečně pohybovat na internetu, naprostým základem je mít nastavená dostatečně silná a bezpečná hesla u každé služby, kterou používáte – tedy například u e-mailu, účtu na facebooku a podobně.

Ší mít vlastní nápad. Výhodou takového hesla také je, že je i lépe zapamatovatelné.

Nepoužívejte stejná hesla všude, ani si je nepište na kousek papíru, i to je totiž nebezpečné – stáváte se tím snadnou obětí. Nikdy nikomu heslo nesdělujte. Zámek od bytu či domu přece také chcete mít co nejlepší a klíč nikomu na potkání nedáváte.

12345 je začátek dětské říkanky, ne dobré heslo

Na veřejné síti nejste nikdy sami

Nemáte-li doma svůj vlastní počítač a připojení k internetu, můžete se k síti připojit například z prostředí knihovny nebo kavárny. V takovém případě však buďte obezřetní a sledujte například i to, jestli se na vás někdo nedívá. Možná to zní komicky, ale i to je způsob, jak získat něčí heslo. Vždyť, kdo z nás se nedíval někdy někomu do knížky nebo časopisu přes rameno?

Základní zásadou je pak neukládat hesla do veřejných počítačů a vždy se odhlašovat. Pokud jen zavřete okno prohlížeče nebo vypnete počítač, některé služby vás po chvíli automaticky odhlásí, ale není to pravidlem a nejedná se o doporučený postup.

Ta nejhorší a nejslabší hesla vypadají například jako 123456, ABCDE, 123ABC anebo se jedná hesla, která vycházejí ze jména či adresy. Ta nejlepší a **nejsilnější hesla mají vždy alespoň dvanáct znaků, speciální znak (třeba lomítko), obsahují malá i velká písmena a také čísla**. Další tip pro silné heslo je například část oblíbené písničky nebo upravená oblíbená filmová hláška. Například fráze „Jak/Utop1t/Doktor4/Mráčk4? je jen velmi obtížně prolomitelná. To ale neznamená, že je moudré ji od teď začít používat, vždy je lep-

Dále například ve vlaku nebo v obchodních centrech bývá možnost připojení k internetu bez potřeby hesla do takzvané veřejné sítě. Nemusí to být vždy nebezpečné, jsou ale zneužitelné. Proto pokud se připojíme na

takovou síť, nepracujeme s internetovým bankovníctvím ani jinými citlivými službami. Tyto veřejné sítě jsou ideální například pro zjišťování dopravních spojů, otevírací doby a podobných informací.



- **Nepoužívejte stejná hesla všude**
- **Nepište si hesla na papírek a nikomu je nesdělujte**
- **Mějte hesla, která neodrážejí vaše jméno, bydliště či záliby**
- **Mějte hesla, která jsou alespoň 12 znaků dlouhá**
- **Mějte hesla, která obsahují malá a velká písmena, čísla a speciální znaky**
- **Silná a dobře zapamatovatelná hesla jsou například upravené filmové hlášky**
- **Čas od času hesla preventivně změňte**



Chodí vám
nevyžádané maily?

Odhlaste
se z jejich
odběru

Elektronická pošta pod palcem

Internet umožňuje rychlou komunikaci. Základním způsobem takové komunikace je e-mail, tedy elektronická pošta. E-mail, zjednodušeně řečeno, funguje stejně jako klasická pošta – i zde je odesílatel, nějaká zpráva a schránka příjemce. Jak už víte, **základem bezpečné komunikace je silné a bezpečné heslo. Stejně jako do poštovní schránky vám ale i do e-mailu může přijít podvodná zpráva, která se na první pohled tváří důvěryhodně.**

Nejen vy, ale i podvodníci jsou učenliví. A když chtějí získat vaše hesla a s nimi i přístup k vašim účtům, využívají různé triky. Mohou vás oslovit například e-mailem, ve kterém se vydávají za Policii ČR nebo jinou instituci, která budí respekt. Z e-mailové adresy, která na první pohled působí důvěryhodně například **158-policie@seznam.cz** vám může přijít historka o tom, že policie řeší bezpečnost hesel seniorů a v rámci tohoto šetření vám ověří sílu vašeho hesla. Stačí jí ho jen poslat a je to. V podobných případech se vždy jedná o podvod.

Dalším příkladem může být e-mail jakoby z banky, který vás nabádá k přihlášení se do internetového bankovníctví a k provedení nějaké kontroly. Scénář je však podobný. Pokud v e-mailu nalezneme zprávu, která se tváří jako z banky, důkladně zkontrolujeme adresu odesílatele a odkazy uvnitř zprávy (například zda tam místo „m“ není „nn“, místo „l“ není „i“ atd...) Takový odkaz by totiž mohl být past. Není ostuda zavolat i do banky a vše ověřit. **Opravdová banka heslo k vašemu účtu nikdy chtít nebude, ani chtít nemůže.** Stejně tak telefonicky ověřujte cokoli podezřelého – například u svého poradce nebo na oficiální lince pro podporu zákazníků.



Banka
heslo
k vašemu účtu
nikdy chtít
nebude

Spam & hoax aneb Internet z té horší stránky

Jedny z nejpálčivějších problémů, které e-mailovou komunikaci postihují, nazýváme spam & hoax.



Spam
není výhra,
ale obtěžující
mail

Spam je nevyžádaná zpráva, která mívá obvykle reklamní charakter a často se snaží působit dojmem, že vám někdo něco nabízí zdarma nebo že jste něco vyhráli.

V takovém případě se nenechte zlákat vidinou slunečné dovolené ani slušného přivýdělku a v první řadě se zeptejte sami sebe, zda jste se vůbec do nějaké soutěže hlásili. Tyto e-maily je obecně nejlepší ignorovat, usilují o to získat vaše data. V ideálním případě je ani neotvírejte – často jsou totiž rozpoznatelné už ze samotného předmětu e-mailu, který typicky vyvolává nadšení a gratuluje k výhře. Pokud takový e-mail otevřete, neodpovídejte.

Rozesílatel spamu vám určitě nedá nic zdarma. Naopak se z vás nějaké peníze nebo citlivá data snaží vymámit.

Hoax je naproti tomu poplašná zpráva, která se vás snaží vyděsit a nabádá k jejímu sdílení. Takový hoax škodí například tím, že může pošpinit něčí pověst – třeba nepravdivá zpráva o zapíchnuté injekční stříkačce v sedačce MHD poškodí dopravce. Hoaxy také manipulují veřejným míněním – třeba fotomontáž vlaku ověšeného uprchlíky na nádraží v Chebu vyvolává strach z imigrantů a šíří nenávisť. Příklady hoaxů můžete najít třeba na stránce www.hoax.cz. Pokud vám tedy přijde nějaká šokující zpráva, zde si můžete ověřit, zda se jedná o některý z hoaxů, který se právě šíří.

Hoaxy nerozesílejte dál, i když máte chuť pomáhat a varovat ostatní – jedná se zkrátka o výmysl a jejich šíření způsobuje jen paniku. A čím víc slov „Tohle musíš poslat dál!“, „Varuj své známé“ a podobně v nich najdete, tím to platí více. Poplašné zprávy jsou palčivé tím, že vám je může poslat i někdo, koho opravdu znáte a běžně s ním komunikujete. Pokud odesílatele takového e-mailu znáte, zdvořile ho upozorněte na tento jev a uklidněte. I když se totiž následně ukáže, že je nějaké sdělení lež, nikdy už se náprava, či dokonce omluva nedostane k takovému počtu lidí jako původní hoax.



Bezpečně na Facebooku

Výhodou sociálních sítí je, že oproti e-mailu nabízejí kromě obvyčejné komunikace i možnost vyhledávání známých, například přátel ze školy, z vojny nebo vzdálených příbuzných. Mezi nejrozšířenější sociální sítě patří Facebook nebo Instagram, který slouží především ke sdílení fotografií.

Musíte si však uvědomit, že to, jakým způsobem se zde chováte, co píšete a sdílíte, není oddělené od všední skutečnosti. Naopak. Na sociálních sítích se chovejte eticky a vězte, že vše, co zde uděláte, vás může dohnat ve skutečném světě. Pokud se tedy někým pohádáte v diskusi a sprostě mu vynadáte, při prvním náhodném setkání v obchodě to nemusí dopadnout dobře.

Kromě toho i sociální sítě mohou útočnickům posloužit jako nástroj, který zvýší efektivitu jejich útoků, protože zde mohou sbírat užitečné informace. **Stačí jedna fotka z termálních lázní, aby útočník zjistil, že nikdo není doma a je ideální čas na loupež. Předějit tomu můžete tak, že budete dobře pracovat s nastavením soukromí – tím určíte, kdo vidí vaše příspěvky.** Můžete je ukázat všem na internetu nebo jen přátelům, případně jen některým vybraným lidem. Dobře zvažujte také to, koho si mezi přátele na sociální síti přidáte, a dejte pozor na falešné profily, jejichž cílem může být vás poškodit.



- **Nepřidávejte si do přátel lidi, které neznáte**
- **Dejte pozor na falešné profily, mohou vás chtít poškodit**
- **To, že s někým máte společné známé, ještě není důvod si ho přidat mezi přátele**
- **Zabezpečte si profil silným heslem**
- **Nastavte si dobře soukromí a mějte kontrolu nad tím, komu svoje příspěvky ukazujete**

**Pár dobrých rad
na závěr**



**Ověřujte si
informace
a přemýšlejte
o nich v souvis-
lostech**

**Mějte
dostatečně
silná hesla**

**Spam či hoax
neposílejte dál,
ale rovnou ho
smažte**

**Na sociálních
sítích diskutujte
slušně a chráňte
si soukromí**

**Na veřejných
počítačích
hledejte jen obecné
informace
a odhlašujte se ze
svých účtů**

Kvíz

1) Co jsou fake news

- a) informace šířené za účelem větší prodejnosti předražených kuchyňských spotřebičů prostřednictvím skryté reklamy.
- b) úmyslně šířené dezinformace za účelem ovlivnit a zmanipulovat příjemce, proto se částečně zakládají na věrohodných informacích.
- c) pravdivé informace šířené tajnými službami na internetu a v TV mající za cíl odhalit vnitřní nepřátele demokracie.

2) Najděte určitě nepravdivou větu

- a) Sestřenice mého švagra Pavla Petra je jedináček a zatím nemá žádné potomky. Potenciální partnery a otce svých budoucích dětí vždy konzultuje se svým bratrem.
- b) Předvčerejšek skončil dříve než včerejšek, pozítřek začne později, než začne zítřek.
- c) V Paříži zapadá slunce dříve než v Londýně, ale později než v Praze.

3) Co je skrytá reklama v TV

- a) Prezentace zboží nebo firmy mimo blok reklamního vysílání, obvykle za nějakou formu úplaty a bez upozornění pro diváky, že probíhá prezentace.
- b) Propagace TV programů herci a moderátory během jejich vystupování v jiných TV programech.
- c) Propagace zboží, kterou dělá osoba, kterou nevidíme, slyšíme pouze její hlas.

Řešení

- 1) b) 2) a) Pokud je Petra jedináček, nemůže mít bratra 3) a)

**Podělte se
o své vědomosti
s 10 přáteli a uděláte
opravdu dobrý skutek!**

**Ted' už víte, že stačí trocha
selského rozumu a kritického
myšlení a internet pro vás bude
navždy jen dobrý sluha.
Proto budeme rádi, když se o své
vědomosti podělíte s přáteli.
Fake news, hoaxy a spamy se totiž
šíří rychleji než pravda.**

**Děkujeme, že pomůžete pravdě
dostat se dál.**

Brožura vznikla ve spolupráci
s Národním úřadem pro kybernetickou
a informační bezpečnost

