O2 | Chytrá škola

Vyznejte se v digitálním světě

www.o2chytraskola.cz

Nadace O2

Program O2 Chytrá škola učí děti, rodiče i pedagogy používat digitální technologie bezpečně a chytře.

E-book je výběrem toho nejdůležitějšího z oblasti internetové bezpečnosti, mediální a počítačové gramotnosti. Další informace, články, videa a výzkumy zdarma ke stažení najdete na portálu O2 Chytrá škola.

Příjemné čtení přeje
Nadace O2

Online bezpečnost

- Kyberšikana
- Internetoví predátoři
- Zdraví v kyberprostoru
- Nakupování online
- Online uličky podvodníků
- Falešné profily a jejich rizika
- Výzvy na internetu

Počítačová gramotnost

- Bezpečné heslo
- Zabezpečení sociálních sítí

Mediální gramotnost

- Fake news a hoax
- Reklama a zábava
- Média a jejich způsoby
- Ochrana osobních údajů
- Autorský zákon
- Mediální stereotypy
- Propaganda a cenzura

O2 | Chytrá škola

Nadace O2

Online bezpečnost

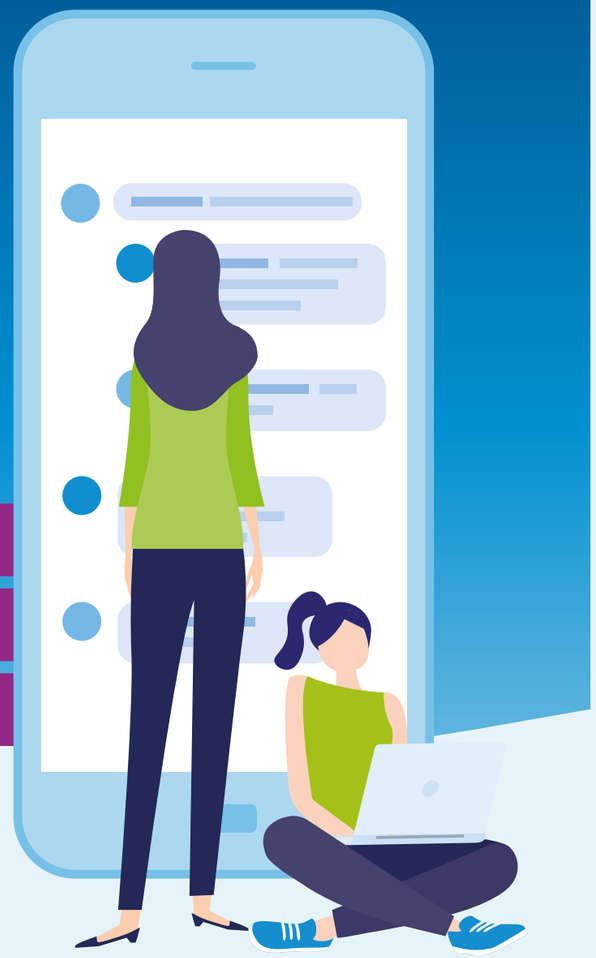
O2 | Chytrá škola

Kyberšikana

Šikanovat někoho online je stejně špatné jako šikanovat ho v běžném životě. Co hůř, v digitálním světě může mít oběť i tisíce trýznitelů z celého světa.

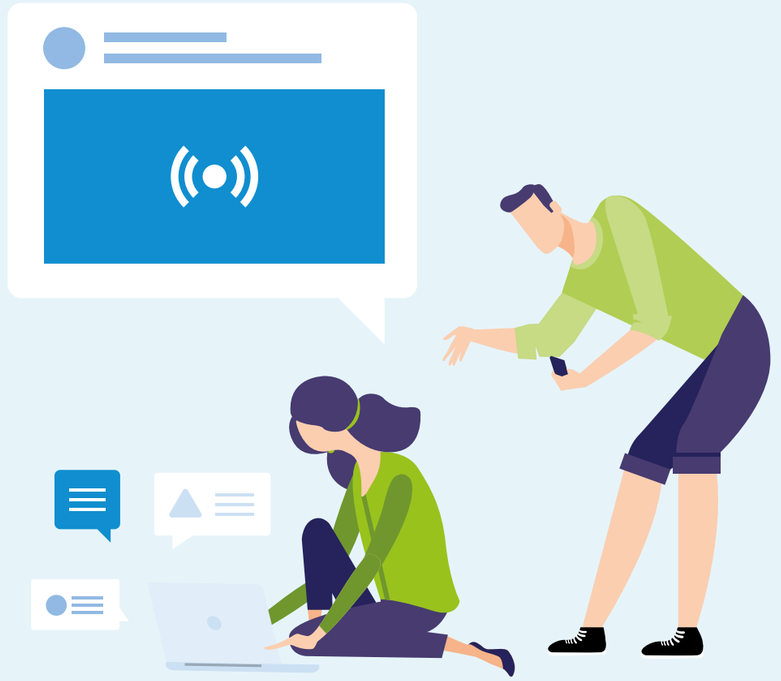
Co je pro jednoho zábava, může pro druhého být šikana. Šikany se účastníš, už když o zneužití cizích fotek, videí a konverzací víš a nikomu to neřekneš.

Co všechno může být šikana?
Jak se z ní vymanit?
A víš jistě, že někomu třeba neúmyslně neubližuješ?



Co je kyberšikana

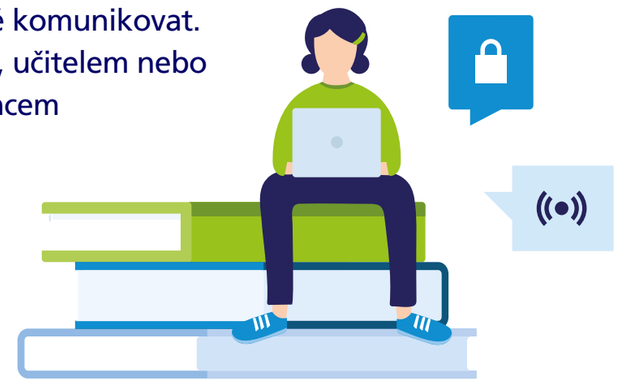
1. Pomlouvání, zastrašování, urážení nebo zesměšňování prostřednictvím e-mailu, SMS, chatu nebo v diskuzi.
2. Pořizování zvukových nahrávek, videí a fotek nebo jejich upravování a zveřejňování s úmyslem člověku ublížit.
3. Vytváření internetových stránek, které urážejí, pomlouvají nebo ponižují konkrétní osobu.
4. Vyloučení z online komunity.
5. Zneužívání cizího e-mailu nebo profilu a vydávání se za osobu, které patří.
6. Vydírání pomocí mobilu nebo internetu.
7. Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.



Tušíš, že se ti děje kyberšikana? • Přestaň s útočníkem komunikovat. Zablokuj přijímání útočníkových zpráv. • Zkus si schovat důkazy pro vyšetřování. • Určitě útok oznam.

Jak se chránit před kyberšikanou

1. Respektuj ostatní uživatele a chovej se k nim slušně.
2. Dobře si rozmysli, co komu posíláš.
3. Měj bezpečné heslo a nikomu ho nedávej.
4. Neposkytuj neznámým uživatelům své osobní údaje, podle kterých by tě mohli vystopovat.
5. Neposílej své fotky nebo fotky své rodiny.
6. Seznam se s pravidly dané služby, ať víš, co je zakázané dělat.
7. Pokud tě někdo šikanuje nebo vydírá, přestaň s ním okamžitě komunikovat. Poraď se o tom s rodiči, učitelem nebo aspoň starším sourozencem či kamarádem.



I žert může způsobit bolest

Ghyslain Raza (14 let, Kanada),

Ghyslain se natočil, když se snažil napodobit bojový styl Dartha Maula z Hvězdných válek. Spolužáci mu nahrávku ukradli a pro pobavení ji zveřejnili na internetu. Během několika týdnů se video stalo virální senzací a dočkalo se řady parodií, dokonce i v seriálech South Park, American Dad a Veronica Mars. Ghyslain byl pro smích celému světu. **Ghyslain** se psychicky zhroutil a musel se dlouhodobě léčit.

Jessica Logan (18 let, USA)

Po rozchodu zveřejnil Jessičin bývalý přítel její intimní fotografie, které mu poslala v době, kdy spolu ještě chodili. Jessica byla vystavena posměchu ze strany spolužáků. Útoky na ni ještě zesílily, když anonymně vystoupila v televizi, aby ostatní upozornila na rizika sextingu. **Jessica** spáchala sebevraždu.

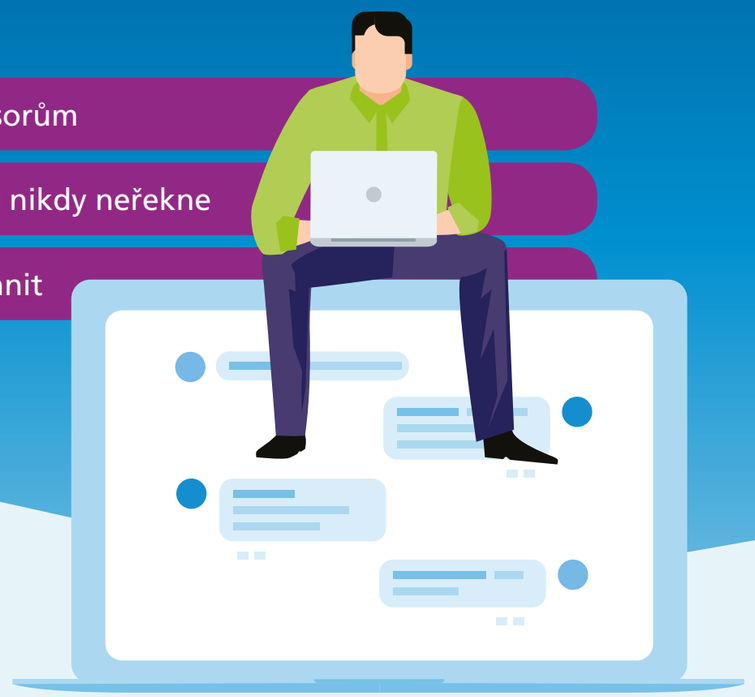
Ryan Patrick Halligan (13 let, USA)

Ryana dlouhodobě šikanoval spolužák, který ho i veřejně označil za gaye. Aby se Ryan zbavil posměchu okolí, rozhodl se najít si dívku. Na internetu si začal psát se spolužačkou a po čase se do sebe zamilovali. Když pak dívku oslovil ve škole, vysmála se mu. Dívka se románkem s ním jen bavila a jejich důvěrnou komunikaci posílala další lidem. **Patrick** se oběsil.

Další tipy, jak se chránit před šikanou, hledej na **www.o2chytraskola.cz**.

Internetoví predátoři

Cizí lidé jsou v digitálním světě ještě nebezpečnější než na ulici. Na internetu se totiž obvykle maskují jako důvěryhodní kamarádi a společníci.



Kyberstalking

Dlouhodobé sledování a obtěžování člověka za pomoci digitálních technologií. Pronásledovat tě může někdo, koho znáš, i naprosto cizí člověk, který si tě vyhlídne na internetu. Že tě sleduje, většinou poznáš až tehdy, když tě začne bombardovat zprávami, pomlouvat tě nebo ti dokonce vyhrožovat.

Kybergrooming

Manipulace, kterou sexuální predátoři používají, aby tě vylákali ven na schůzku a tam tě mohli napadnout. Dospělý se nejčastěji vydává za dítě. Pod falešným profilem se snaží získat tvou důvěru, osobní údaje, tajemství a lechtivé fotky k dalšímu vydírání.

Webcam trolling

Podvod, při kterém se útočník vydává za někoho jiného a používá k tomu ukořistěné nahrávky z webkamery. Video dotváří iluzi, že si opravdu píšeš s reálným dítětem nebo vrstevníkem. Napřímo spolu totiž nemůžete mluvit, protože tvůj společník má údajně rozbitý mikrofon. Nový „kamarád" se pokusí získat tvou důvěru, citlivé informace a pak tě přimět třeba ke svlékání před kamerou nebo osobní schůzce.

Nepomáhej agresorům

I když nepodlehneš a komunikaci ukončíš, jakmile pošleš jen jednu normální oblečenou fotku nebo budeš chvíli videochatovat, útočník záznam použije k tomu, aby se za tebe vydával a nalákal někoho jiného víc důvěřivého.

Co nový kamarád nikdy neřekne

aneb Pár frází, které odhalí nebezpečného podvodníka:

1. **Máš počítač ve svém pokojíku?**
   (Zjišťuje, jestli rodiče můžou sledovat komunikaci.)
2. **Jaké máš zájmy? Já mám rád počítačové hry a U2.**
   (Zjišťuje, čím by tě případně mohl uplatit.)
3. **Pošli mi fotku, já ti pošlu svoji.**
   (Získává kompromitující materiály, které může využít k tvému vydírání.)
4. **Chci ti poslat suprovou MMSku, napiš mi své číslo.**
   (Získává na tebe další kontakt.)
5. **Máš kluka/holku?**
   (Zjišťuje, jestli máš někoho, komu se můžeš svěřit.)
6. **V kolik chodí vaši do práce? Jsem doma od 6 do 8 sama.**
   (Zjišťuje, kdy je byt prázdný kvůli možnému vloupání.)
7. **Rodiče ti nerozumí, já ano, mně se můžeš svěřit se svými problémy.**
   (Snaží se získat tvou důvěru a informace pro pozdější vydírání.)
8. **Neříkej o tom mamince. Nenáviděla by tě.**
   (Zaplétá tě do sítě tajemství a izoluje tě od těch, kdo by ti pomohli.)
9. **Jestli se se mnou nesejdeš, zabiju se.**
   (Vydírá a snaží se tě vylákat ven.)
10. **Jestli mi neřekneš své pravé jméno, zveřejním tvoji fotku a napíšu o tobě, že jsi lesba.**
    (Vyhrožuje.)

Jak se můžeš chránit

1. Nevěř všemu a všem. I děti mají svoje zájmy a občas lžou, proč by to u dospělých bylo jinak.
2. Nesdílej s nikým informace a fotky, které s klidným srdcem nepověsíš babičce na ledničku.
3. Pozor na všechny, kdo se až příliš snaží hned získat tvou pozornost a důvěru. Kamarádství se buduje postupně a tak nějak přirozeně.
4. Rodiče přece o tvých kamarádech můžou (a měli by) normálně vědět. Pokud se někdo chce skrýt před nimi, skrývá něco před tebou.
5. Kdykoli máš pochyby, zeptej se rodičů, sourozenců nebo kamarádů. Víc hlav víc ví.

Víš o čem je řeč? Máš problém? Neboj se svěřit rodičům.
Anebo kontaktuj bezplatnou Linku bezpečí (116 111) nebo přímo policii (158).

Všechny finty a nekalé praktiky útočníků i to, jak se jim bránit, najdeš na **www.o2chytraskola.cz.**

O2 | Chytrá škola

Zdraví v kyberprostoru

Není to úplně fér, ale virtuální život někdy může způsobit skutečné neduhy. A je jen na tobě, jestli jimi budeš trpět.

Kybernemoci fakt existují

Esemeskový krk a tabletové rameno

jsou onemocnění páteře způsobená dlouhým předklonem hlavy a hrbením se při používání mobilu, tabletu a notebooku.

Syndrom falešného zvonění

je spíš kuriózní než nebezpečný. Jednoduše spočívá v tom, že je mozek tak navyklý na zvonění a vibrace telefonu, že je slyší a cítí, i když nikdo nevolá ani nepíše.

Myšitida

je zánět ruky způsobený častým používáním počítačové myši. Odtud ten název. Onemocnění nijak zvláštní, zato opravdu bolestivé. To nechceš.

Čistota půl zdraví

Tohle přísloví platí v oblasti technologií dvojnásob. Laboratorní testy totiž zjistily, že na běžném mobilu a klávesnici je víc nebezpečných bakterií než na záchodovém prkénku. Fuj!

Od půjčování přístrojů ostatním by tě tedy měly odradit hned dvě věci:

1. Když někomu půjčíš tablet, mobil nebo počítač, může se dostat k tvému e-mailu, profilům, fotkám a citlivým údajům.
2. Přístroj ti vrátí pokrytý vlastními bacily. A nezapomeň, že mobil si přikládáš k obličeji.

Zapamatuj si

1. Nepůjčuj telefon nikomu, po kom se nenapiješ z lahve.
2. Najez se raději mimo počítač a bez mobilu v ruce.
3. Pořiď si speciální přípravek na čištění klávesnic a elektroniky.
4. Nehraj si s mobilem, když sedíš na záchodě.

Závislost na internetu a technologiích

Co všechno je závislost? Jak se projevuje? Týká se i tebe? Nebo dokonce tvých rodičů?

Pokud…

1. Běžně dokážeš zkouknout celou sérii seriálu najednou a klidně kvůli tomu obětuješ spánek nebo víkend.
2. Klikáš z jednoho YouTube videa na jiné a než se naděješ, zjistíš, že několik hodin je pryč.
3. Kontroluješ mobil a nejnovější příspěvky, kdykoli se ozve notifikace.
4. Chatuješ s lidmi online, i když jsi ve společnosti někoho jiného právě teď a tady.
5. Kdykoli máš volnou chvilku, sáhneš automaticky po mobilu.

...pak se tu nejspíš rýsuje závislost.

Přespříliš času věnovaného mobilům a počítačům může škodit. Optimální je umět skloubit užívání moderních digitálních technologií s klasickou mezilidskou komunikací tváří v tvář a s dostatkem pohybu.

Ze slovníčku kyberpsychologa

Netolismus

značí závislost na internetu. Patří sem závislost na online hrách, sociálních sítích, chatování, seriálech, pornografii, ale i přehnaná kontrola e-mailů.

FoMO syndrom

(z anglického fear of missing out) je chorobný strach, že ti něco uteče, když pravidelně nezkontroluješ nejnovější dění na internetu, hlavně příspěvky na sociálních sítích.

Nomofobie

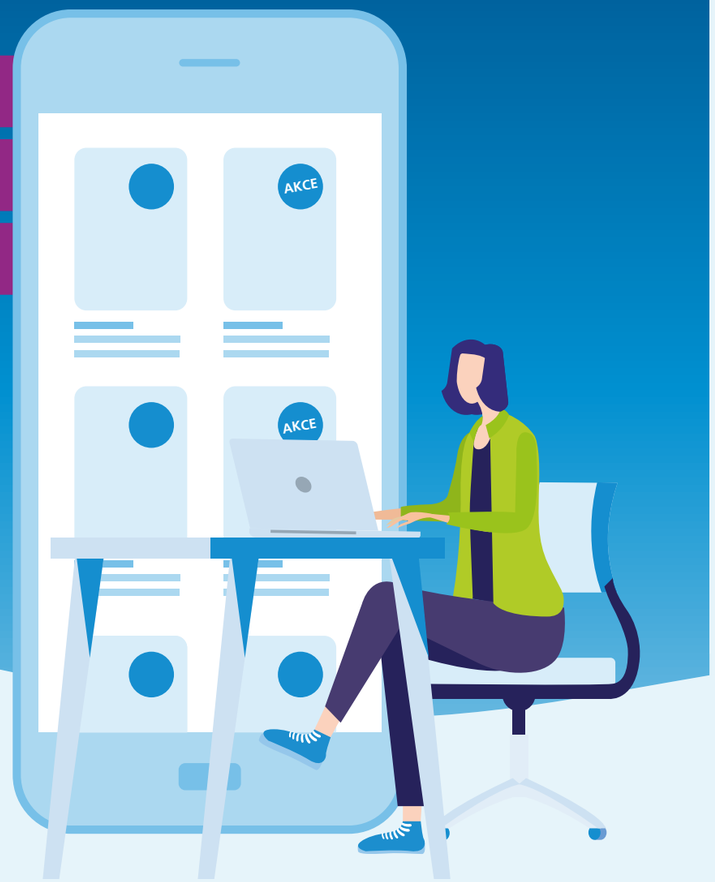
neboli „no mobile phobia“, je potřeba mít u sebe mobil neustále, spojená s až chorobnou obavou, že ho ztratíš, nebudeš mít signál nebo se vybije baterka.

Internet a technologie přinášejí spoustu dobrých věcí, pokud se používají tak, jak se má. Víc informací o online závislosti a zdraví na **www.o2chytraskola.cz**.

O2 | Chytrá škola

Nakupování online

Kupuješ si oblečení, muziku, hry a jejich rozšíření přes internet? Super! Tvoje peněženka ti vzkazuje „tohle si přečti.“



E-shopové must have

Než hodíš nejnovější „must have“ kecky do košíku, podívej se, jestli i e-shop má všechno, co musí mít:

Kontaktní údaje
jako název firmy nebo jméno podnikatele, adresa a IČO jsou vyžadované zákonem.

Telefonní číslo
je stejně důležité! Proč by měl e-shop potřebu ho skrývat?

Obchodní podmínky
jsou sice dlouhé a nudné čtení, ale najdeš v nich všechny možné háčky, třeba reklamační podmínky.

Fotky produktů
a kvalitní popisky se všemi informacemi, které o produktu potřebuješ vědět, jsou znakem prodejce, který myslí na zákazníky.

Recenze a reference

Doporučení a hodnocení ostatních lidí ti pomůžou s výběrem nejen správného zboží, ale i e-shopu. Pamatuj ale, že i reference se dají zfalšovat.

Nejlepší je vložit jméno zboží nebo e-shopu do vyhledávače a podívat se na recenze na několika různých webech. Pokud je hodnocení na stránce prodejce jen a jen kladné, už to je podezřelé.

Doprava a platba

Pravda je, že ani jedna z možností, jak za zboží zaplatit, není ideální. Všechny ale mohou proběhnout v pořádku, pokud znáš jejich výhody, nevýhody a rizika.

Platba převodem

+ Není potřeba mít u sebe hotovost, cena dopravy bývá při platbě předem nižší.
– Převod může trvat několik dní a banka ti za něj může účtovat poplatky.

Bezpečnost:
Banky mají své převody špičkově zabezpečené, ale e-shop ti zboží nemusí poslat.

Platba rychlým převodem

+ Platba je rychlá jako u karty, stačí kliknout na tlačítko své banky a potvrdit platbu.
– Tlačítka pro rychlý převod mají jen některé e-shopy.

Bezpečnost:
Převod je stejně skvěle zabezpečený jako převod z internetového bankovnictví, ale obchod ti objednávku nemusí poslat.

Platba přes PayPal

+ Rychlá a okamžitá platba jako u karty.
– Musíš se registrovat a založit si účet.

Bezpečnost:
Velmi bezpečná platba, pokud máš silné heslo a z účtu se pokaždé odhlásíš.

Platba kartou

+ Nejrychlejší a nejpohodlnější způsob platby.
– Vyplňuješ údaje ze své karty a ty mohou být ukradeny, e-shop ti opět nemusí nic poslat.

Bezpečnost:
Platby přes platební brány jsou zabezpečené. Údaje z tvé karty se ale dají ukrást tak, že platíš na veřejně přístupné Wi-Fi nebo počítači, nemáš zabezpečený počítač a mobil nebo si kartu nehlídáš a někdo si opíše čísla.

Platba na dobírku

+ Platíš, až když zboží skutečně přijde.
– Musíš si zboží vyzvednout, ne vždy můžeš platit kartou, za dobírku si e-shopy účtují peníze navíc.

Bezpečnost:
Poměrně bezpečná, pokud platíš hotově nebo dodržíš zásady platby kartou.

Podívej se na **www.o2chytraskola.cz** a nauč se, jak při nákupech ochránit své peníze.

Online udičky podvodníků

Výraz surfovat na netu není zas tak mimo. Na síti je opravdu moře informací a zábavy, ale taky návnad nahozených pro důvěřivé uživatele.

Nauč se je poznávat a můžeš digitálním světem proplouvat v klidu.

Sociální inženýrství

Manipulace, při které se útočník vydává za důvěryhodný web nebo tvého skutečného kamaráda, patří k nejnebezpečnějším. Hlavním cílem je okrást tě o peníze. K tomu podvodník využívá podvržené stránky, vymyšlené soutěže, zprávy a SMS z falešných osobních profilů.
Často mu pomáhají počítačové viry a škodlivé softwary, které vytvoří cestičku k datům a heslům ve tvém počítači nebo telefonu.

Phishing

Takzvané rhybaření je druh sociálního inženýrství, které jako udičku nahazuje podvrženou verzi běžné a důvěryhodné stránky, nejčastěji přihlašovací stránky na Facebook nebo do internetového bankovnictví. Zadané přihlašovací údaje tak snadno ukradne a použije k přihlášení a nekalostem.

O co jim jde?

Tvé přihlašovací údaje

tvá hesla do e-mailu a Facebooku jsou vstupní branou k většině tvých účtů.

Číslo tvé karty

kdokoli má údaje z tvé karty, může její pomocí nakupovat, aniž ji kdy držel v ruce nebo viděl naživo.

Mimochodem …

… přihlašovací údaje a kartu je potřeba chránit i mimo digitální svět. Proto si hesla ani PINy nikam nepiš. Pamatuj si je. A nikomu je nedávej ani neříkej.

Jak se bránit

1. Používej selský rozum.
2. Důvěřuj, ale prověřuj.
3. Zkontroluj si správnost webovky v adresním řádku prohlížeče.
4. Poslouchej varování prohlížeče, že jde o nebezpečnou stránku.

Nakažlivý internet

Tvůj počítač, tablet i mobil se mohou nakazit raz dva. Kvalitní a ověřený antivirový program ochrání zařízení před většinou nástrah. Nakonec je to ale právě tvoje klikání, které rozhoduje, s kolika neřády se antivir bude muset vypořádat.

Proto neklikej na podezřelé obrázky a odkazy, ať si do přístroje nevpustíš někoho z těchhle:

- **Trojský kůň**
  je virus, díky kterému útočník získává přístup do tvého zařízení a k informacím uvnitř něj.
- **Keylogger**
  je specifický virus, který zaznamenává, co píšeš na klávesnici. Včetně tvých hesel.
- **Ransoware**
  „unese“ tvůj počítač tak, že ho zašifruje. Pak tě vyzve k zaplacení „výkupného“, které má znovu zpřístupnit tvá data. To se ale nestane.
- **Spyware**
  zneužívá webové stránky, aby získával data z tvého počítače. Běžně se používá pro reklamu, ale může posloužit i ke krádeži hesel a čísla kreditky.
- **Malware**
  není virus, i tak ale škodí. Zavrtá se do tvého přístroje a zpomalí ho, protože využívá jeho výpočetní kapacitu pro vlastní účely.
- **Adware**
  je typ malwaru, který ti zobrazuje nevyžádané reklamy. Pokud ho včas nezlikviduješ, zaplaví tvůj přístroj vyskakovacími okny.

Metody sociálního inženýrství a škodlivých programů jsou velmi prohnané. Zjisti o nich víc a jak se jim bránit na www.o2chytraskola.cz.

O2 | Chytrá škola

Falešné profily a jejich rizika

Jak víš, že ti skutečně píše tvůj kamarád? Není ta zpráva trochu divná? Jak snadno se na internetu lže a podvádí? A kolik tě to nakonec bude stát peněz?

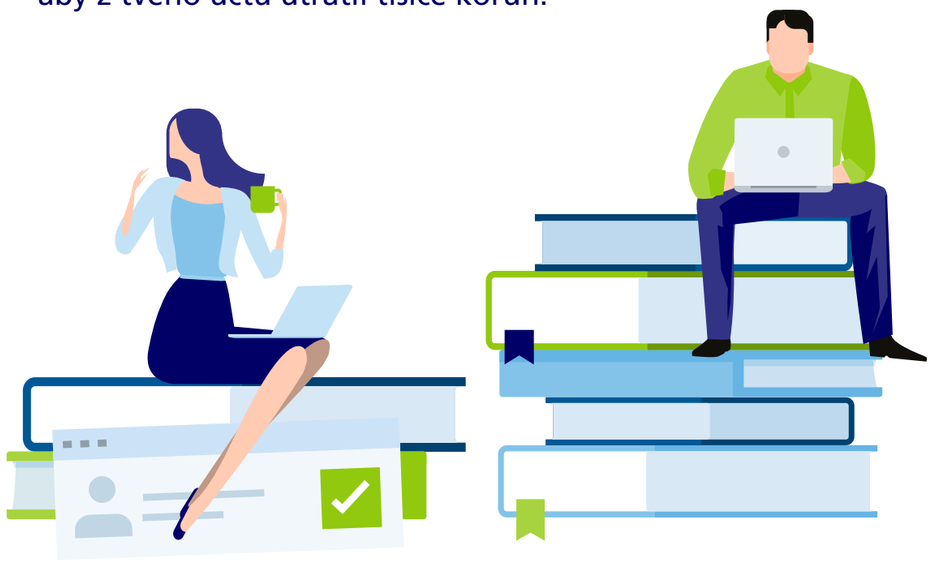
Profily se kradou i kopírují

Za tvého kamaráda, ale vlastně i za tebe, se může vydávat úplně kdokoli. Stačí si na tvé jméno a fotku založit profil. Nebo ještě líp, tvůj profil ukrást.

Co z toho kdo má?

Falešné profily si podvodníci zakládají, protože tě chtějí:

- **Sledovat**
  Stalker tě může kontaktovat pod falešnou identitou, aby o tobě získal další informace.
- **Manipulovat**
  Sexuální predátor nejdřív získá tvou důvěru a důvěrné informace, pak tě jimi může vydírat a nutit k osobní schůzce.
- **Okrást**
  Zloději často stačí mít tvé telefonní číslo a tvou důvěru, aby z tvého účtu utratil tisíce korun.



M-platby jsou nejhorší

M-platby jsou platby, které se ti nestrhávají z účtu, ale z mobilního kreditu nebo paušálu. Fungují tak třeba dárcovské SMS nebo SMS jízdenky na MHD.

Jak tě okradou?

1. Zloděj tě kontaktuje nejčastěji přes Messenger nebo jinou sociální síť pod identitou tvého kamaráda. Tu ale zkopíroval nebo ukradl.
2. Napovídá ti historku o zablokovaném účtu, ztrátě peněženky nebo něco podobného.
3. Pak tě požádá o tvoje telefonní číslo, aby si na něj mohl nechat poslat kód ke zpřístupnění svého účtu. (Ačkoli by tvé číslo měl mít a mohl by si kód nechat poslat na svůj mobil.)
4. Pokud mu kód pošleš, potvrdíš tím platbu, kterou mezitím na tvé číslo provedl, a ty přijdeš o peníze.

V horším případě se nevědomky přihlásíš ke službě, která tě bude kasírovat pravidelně, poskytneš zloději přístup k číslu platební karty nebo svému účtu a on je zneužije.

Jak si ochráníš účet

1. Používej dvoufázové ověření pro přihlášení do všech účtů, hlavně e-mailu a sociálních sítí.
2. Nikomu neříkej své heslo a vlastně ani další informace, jako třeba telefon, e-mail nebo číslo platební karty.
3. Nastav si profily na všech sociálních sítích jako soukromé a vypni si viditelnost přátel i pro své přátele.
4. Pokud ztratíš mobil, okamžitě ho zablokuj.

Máš zkušenost s podvodem?

Pokud se s pokusem o podvod nebo falešným profilem setkáš, okamžitě na něj upozorni někoho staršího.

1. Falešný profil jde na každé sociální síti nahlásit jako škodlivý, stačí kliknout do sekce Nastavení.
2. Vytvoř si okamžitě printscreeny obrazovky, kde probíhá konverze s podvodníkem. Poslouží policii jako důkaz.
3. Varuj kamarády, pokud ti někdo účet ukradne, ať je nepotká stejný osud.

Popravdě…

…většinou jde o podvodné skupiny ze zahraničí, na které je česká policie krátká. Nepomůže ti ani zákaznická podpora sociální sítě, protože ani ty největší nejde většinou kontaktovat přímo.

Proto je nejlepší obranou prevence.

Důvěřuj, ale prověřuj a chraň si své účty.

Zjisti o falešných účtech a podvodnících víc na www.o2chytraskola.cz

O2 | Chytrá škola

Challenges (výzvy) na internetu

Internetové výzvy nejsou vždycky jen špatné. Některé pomáhají dobré věci. A jiné jsou prostě jen sranda. Často se ale stává, že můžou být i hodně nebezpečné.

No kdo tohle vymyslel?

Online challenges často začnou jako hoax, takže jsou úplně smyšlené. Jak se o nich už mluví, lidé je začnou zkoušet a stanou se skutečností.

Výzvy, které ublížily

Oběti po celém světě mají na starosti výzvy typu “Sněz...”.
Při nich se lidé pokusili například sníst extra pálivé papričky, lžíci koření, prací tablety nebo obaly od potravin. Svědkem jejich utrpení můžeš být díky videím, která nasdíleli.

- Cinnamon Challenge
- Ghost Pepper Challenge
- Tide Pod Challenge

Jizvy a jiná zranění, často s doživotními následky, si přivodili adepti na pokoření výzev jako:

- Salt and Ice Challenge
- Eyeballing Challenge
- Snorting Challenge
- Duct Tape Challenge

Výzvy, které zabíjejí

Modrá velryba (2016)
původně vznikla jako hoax, ale díky její medializaci si děti opravdu začaly dávat stupňující se nebezpečné úkoly, při kterých se zraňovaly a které řadu z nich dovedly k smrti.

Momo Challenge (2018)
je v podstatě stejná jako výzva Modrá velryba jen s tím rozdílem, že k plnění nebezpečných úkolů člověka nutí Momo – děsivý tvor napůl žena a napůl kuře, pod hrozbou, že ublíží jeho blízkým.

Choking Challenge (už od 90. let)
spočívá v tom, že se člověk nechá škrtit dokud neomdlí, nebo se „jen nechá lehce přidusit" pro ten pocit, když se krev vrací do hlavy. Riskuje tím ale poškození mozku.

Challenge je nejspíš pěkný hnus, když...

1. Má někomu ublížit.
2. Působí bolest a ohrožuje život.
3. Vyžaduje ničení majetku a bezohlednost.
4. Používá hrozby a vydírání.
5. Dítě se o ní bojí říct dospělým, aby nebyl průšvih.

Tomuhle se říká challenge

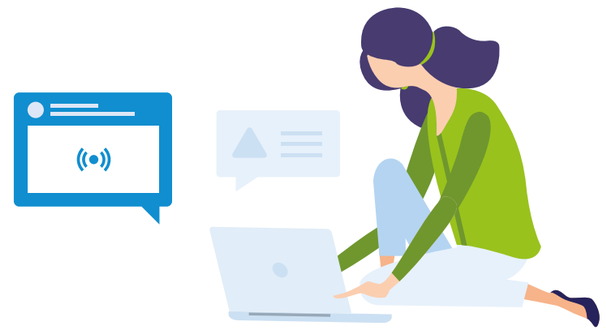
Většina výzev rychle přijde a zase odezní, ale můžeš se jimi inspirovat a vymyslet vlastní, stejně vtipnou nebo prospěšnou. Třeba nastartuješ nový letošní virál.

Mannequin Challenge (2016)
spočívala v tom, že lidé jakoby zmrzli uprostřed toho, co dělali, zatímco kamera se pohybovala dál.

Harlem Shake (2013)
je o tom, že na písničku nejdřív šíleně tancuje jeden člověk, nastane střih a všichni kolem se přidají. Kostýmy a masky ujetost výzvy jen posilují.

Ice Bucket Challenge (2014)
při kyblíkové výzvě na sebe lidé lili kbelíky s úplně ledovou vodou, aby zvýšili povědomí o amyotrofické laterální skleróze (ALS).

Trashtag Challenge (2019)
v rámci ní lidé uklízejí odpad z přírody a fotky místa před a po úklidu pak sdílejí pod hashtagem #trashtag, aby inspirovali ostatní.



Koukni na **www.02chytraskola.cz** a zjisti o výzvách víc.

Počítačová gramotnost

O2 | Chytrá škola

Bezpečné heslo

Jsou tvůj e-mail, Facebook, Instagram, WhatsApp, Snapchat a další appky zabezpečené, nebo taky děláš tyhle chyby?

Zjisti, jak dlouho potrvá hackerům prolomit tvoje hesla a kudy se dostanou ke tvým fotkám a chatům.

Jak dlouho trvá prolomit heslo

Představ si, že se snažíme rozlousknout tvoje heslo s 6 znaky.
Jak dlouho to potrvá, záleží na obtížnosti hesla.

275 986

2 minuty

Heslo složené jen z číslic.

g7b uN6

55 minut

Složené z číslic a malých i velkých písmen abecedy.

g7* uN6

9 hodin

Složené z číslic, malých a velkých písmen a speciálních znaků (@, #, %).

g7*u N6 7

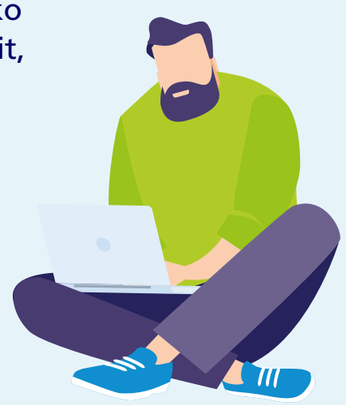
5 týdnů

Složené z číslic, malých a velkých písmen, speciálních znaků.
Přidali jsme JEDEN znak navíc!

Hackeři ti vidí do hlavy...

...a spoléhají se, že uděláš jednu z běžných chyb.
Přechytrač je jednoduše tak, že tyhle věci nebudeš dělat:

1. Tvoje heslo nikdo nepotřebuje znát, ani kamarád. Prostě ho nikomu nedávej.
2. Neposílej ho nikomu ani e-mailem, SMSkou, přes WhatsApp nebo Messenger.
3. Nepoužívej heslo, které jde najít ve slovníku, křestní jméno ani příjmení.
4. Nenech internetový prohlížeč zapamatovat si heslo pro příští přihlášení. Než z počítače odejdeš, odhlas se ze všech účtů a aplikací.
5. Při používání kontrolních otázek nevybírej jako odpověď informace, které se dají snadno zjistit, např. jméno matky, domácího mazlíčka, datum narození apod.
6. Nikdy neměj stejné heslo k víc účtům najednou.
7. Kvalitní heslo není potřeba měnit do okamžiku, než ho někdo odhalí.
8. Hesla si nikam nepiš. Zapamatuj si je.



Vytvoř si neprůstřelné heslo

1. Při tvorbě hesla použij číslice, velká i malá písmena abecedy a speciální znaky.
2. Nevyhýbej se kontrolním otázkám při přihlášení. Ale nepoužívej jako odpověď informace, které se dají snadno zjistit. Klidně i lži a odpověď si vymysli.

Nezapomeň na dvoustupňové ověřování

Délka prolomení hesel se stále zkracuje. Všude, kde je to možné, proto používej dvoustupňové ověřování. Chrání tě v případě, že tvé přihlašovací údaje k účtu někdy uniknou na internet. K účtu se přihlásíš nejen heslem, ale budeš muset udělat i něco dalšího – například zadat kód poslaný na tvůj telefon nebo tvůj otisk prstu.

Top 10 nejhloupějších hesel internetu

Na seznamu nejsnáz prolomitelných hesel se tahle objevují každý rok. Kdo je používá, koleduje si o problém.

1. 123456
2. Password
3. Qwerty
4. Welcome
5. Abc123
6. 111111
7. 1qaz2wsx
8. Master
9. Login
10. Admin

Jak lze také pracovat s hesly?

Existuje několik aplikací pro správu hesel (tzv. **password manager**), které si hesla nejen pamatují, ale umí je i vytvořit.
Například: LastPass, 1Password, StickyPassword, RoboForm.

Super hack programátorů

Tenhle trik používají programátoři při vymýšlení vlastních nedobytných hesel. Funguje takhle:

1. Vymysli si krátkou větu s aspoň 1 číslovkou, například:
   Můj pes má čtyři nohy a jeden ocas
2. Z každého slova použij první písmeno a číslovky změň na čísla, dostaneš:
   mpm4na1o
3. Teď převeď některá písmena na velká, třeba:
   MpM4Na1o

Teď už jen stačí heslo trochu změnit a máš pokryté všechny účty

Heslo do e-mailové schránky
MpM4Na1o._ ml

Heslo na Facebook
MpM4Na1o._ fb

Heslo na Instagram
MpM4Na1o._ inst

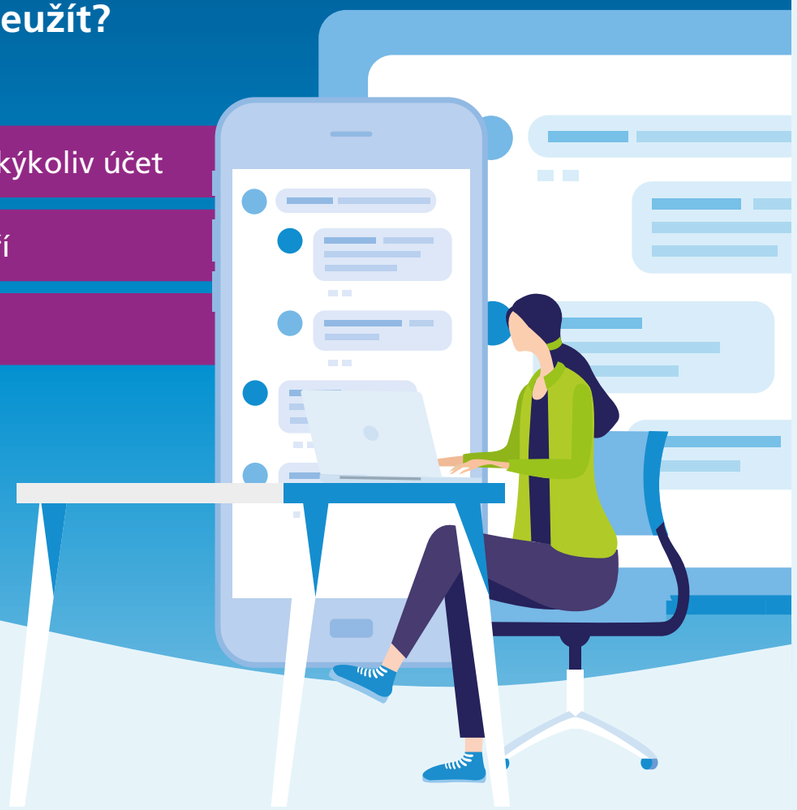
Heslo do počítačové hry
MpM4Na1o._ game

Další tipy, jak zaručeně ochráníš svoje účty, najdeš na **www.o2chytraskola.cz**.

O2 | Chytrá škola

Sociální sítě – zabezpečení

Máš v nich opravdu jen své přátele? Kde jsou nejslabší místa tvých profilů a jak se toho dá zneužít?



Když si zakládáš jakýkoliv účet

Překonej lenost a opravdu si nastuduj pravidla používání sítě. Co se na ní smí a nesmí a jaké chování se doporučuje.

Vymysli si bezpečné heslo aspoň s 8 znaky a nech si ho jen pro sebe. Ideálně k tomu přidej i bezpečnostní otázku nebo dvoufázové ověřování přes mobil. Nebo využij některou z aplikací pro tvorbu a správu hesel (tzv. password manager).

Nevyplňuj zbytečně víc informací, než musíš. Políčka, která nejsou povinná, nevyplňuj. To koneckonců platí pro každou registraci na netu.

Dej si tu práci s nastavením soukromí, tedy s tím, kdo tvoje příspěvky a informace o tobě může vidět.

Co na socky nepatří

1. **Osobní údaje**
   Ani při vyplňování profilu neuváděj svůj věk, datum narození, adresu, informace o pracovišti rodičů atd. Tví noví kamarádi nemusejí být těmi, za koho se vydávají. Asi 10 % účtů na sociálních sítích je falešných.

2. **Informace o rodině a domácnosti**
   Nikdo nemusí vědět, kolik vás doma bydlí a kdy jedete na dovolenou. Pro zloděje je to jako pozvánka do tvého pokoje.

3. **Fotka tvého obličeje vyfocená zepředu v profilovce**
   Řada sítí používá funkci automatického rozpoznání obličejů, která tě právě podle profilovky pozná a označí i na fotkách, které sdílel někdo další.

4. **Intimní fotky a videa**
   Už jen mít je v mobilu nebo počítači je riziko, natož je s někým sdílet. Jakmile k nim někdo další získá přístup, má nad tebou moc. Může tě s nimi vydírat nebo šikanovat.

! Hraješ hry v prostředí sociálních sítí?
Zjisti si, jaké údaje s ostatními hráči sdílíš.

Pozor:
někdy i hra vyžaduje velké množství osobních údajů...

Co dělat když…

...narazíš na nevhodný obsah

Video s násilím nebo stránky, které někoho ponižují, jsou formou šikany. Nepodporuj ji a nahlas ji.
Tlačítkem pro nahlášení nevhodného obsahu je vybavená skoro každá sociální síť.

...přijímáš nového kamaráda

Než někoho přijmeš mezi kamarády nebo sledující, projeď si jeho profil, jestli je opravdový. Na sítích najdeš kupu falešných a spamovacích účtů.

Koukni na **www.o2chytraskola.cz** a zjisti víc o tom, jaké nástrahy na síti mohou čekat.

Mediální gramotnost

O2 | Chytrá škola

Hoaxy a fake news

Poplašná zpráva, novinářská kachna, kanadský žertík nebo zkrátka jen podvod. To je pár dalších jmen pro hoax a fake news.

Neškodná zábava?

Zatímco hoaxy vznikají spíš jako žert, fake news jsou často produktem dezinformačních webů a médií, které se snaží ovlivnit veřejné mínění cíleným šířením nepravd. Oba typy manipulace ale škodí stejně.

1. Vyvolávají paniku a šíří strach.
2. Pomáhají extremistickým skupinám.
3. Nebezpečné rady můžou lidem ublížit.
4. Poškozují lidi i firmy, o kterých se zmiňují.
5. Spamují e-maily a zatěžují linky a servery.

Druhy hoaxů

Poplašná zpráva
manipuluje s pravdou nebo přímo lže a snaží se čtenáře přimět k dalšímu šíření. Přitom vystupuje jako dobrák, který pomáhá lidem.

Kanadský žertík
chce hlavně pobavit. Přináší jen těžko uvěřitelnou informaci, z fotek bývá téměř na první pohled patrné, že jde o fotomontáž.

Smyšlená petice
nejčastěji bojuje proti údajnému plánovanému zpoplatnění nějaké sociální sítě a sbírá tak e-maily pro další spamy.

Prosba o pomoc
snaží se zapůsobit na city příběhem lidí ve svízelné situaci a emotivními fotkami. Často žádá o peníze a šíří se i potom, co už dávno není aktuální.

Řetězový dopis štěstí
nejdřív se šířil klasickou poštou, pak e-maily a dnes i po sociálních sítích. Zneužívá pověrčivost lidí k šíření spamu.

Podvodná výhra
pracuje s příslibem snadného zisku nebo opravdu lákavých cen. Stačí poslat trochu peněz, registrovat se nebo jen kliknout.

Nepravdu spolehlivě prozradí

1. Dramatické a až příliš názorné fotky, které by státem regulovaná média nemohla ani použít.
2. Gramatické chyby, chabá stylistika a spousta vykřičníků.
3. Odvolávání se na autoritu, nebo naopak tvrzení, že zpráva unikla a oficiální média o ní mlčí.
4. Snaha zaujmout, vystrašit nebo vzbudit soucit za každou cenu.
5. Výzva ke sdílení s co největším počtem dalších lidí.

Jak nenaletět hoaxům a fake news

1. Nevěř všemu, co se k tobě dostane. Víc než polovina lidí sdílí články jen podle nadpisu. Nikdy je nečetli.
2. Vždy si zprávu ověř i na oficiálních médiích a dalších zdrojích. Pokud o ní nepíší, je pro to důvod.
3. Ověř si původ obrázku nebo videa přes funkce Reverse Image Search a Reverse Video Search. Nejspíš zjistíš, že jsou ukradené z jiného článku a zobrazují úplně jinou realitu.
4. Pozoruj, jak píšou a mluví oficiální média. Hoaxy a fake news se vyjadřují spíš jako bulvár než televizní noviny.

Jedna babka povídala

Některé hoaxy byly tak úspěšné, že se z nich pomalu staly městské legendy, a ještě dneska je někoho můžeš slyšet říkat vážným hlasem.

Záchranný PIN

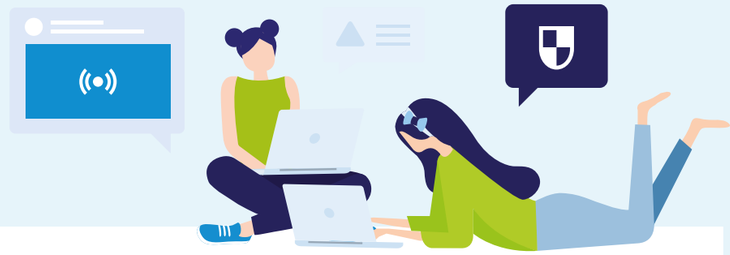
Tahle povídačka tvrdí, že pokud musíš vybrat peníze z bankomatu pod nátlakem, máš svůj PIN zadat opačně. Přístroj ti peníze vydá, aby uspokojil násilníka, ale zároveň tajně přivolá policii.
Nic takového se ale nestane.

Injekční stříkačky na sedadlech

Dodnes je živá poplašná zpráva, že narkomani nakažení HIV z nenávisti k celému světu dávají do sedadel v kině a MHD infikované injekční jehly. Až když se píchneš, všimneš si vzkazu: „Nakazili jste se HIV.“

Řetězové dopisy

Znáš to. Pošli do 15 minut tohoto andílka 10 lidem a budeš mít štěstí. Když ho nepošleš, budeš mít 10 let smůlu, tvá rodina tě zavrhne, tvůj dobytek pojde a z cloudu se ti smažou všechny fotky.



Jak chránit před nepravdami ostatní

1. Nelajkuj a nesdílej všechno, co postnout tvoji kamarádi, bez rozmyslu. Přesně takhle se hoaxy a fake news šíří.
2. Naopak se neboj napsat komentář, upozornit na nepravdivost a ideálně odkázat na zdroj, který podvod odhaluje.
3. Nepřeposílej a nesdílej řetězové dopisy, neověřené prosby o pomoc a petice. Šíříš tak spamy.

Aktuální i zlidovělé hoaxy českého internetu najdeš na webech www.hoax.cz nebo manipulatori.cz.
V zahraničí se jim věnují stránky:
www.hoax-slayer.com, www.hoaxbuster.com nebo www.hoaxes.org.

Zjisti víc o tom, jak fungují hoaxy, fake news a média, na www.o2chytraskola.cz.

O2 | Chytrá škola

Reklama

Pozor toto není sponzorovaný příspěvek.

Reklama není špatná…

Tvé oblíbené blogy, YouTube kanály, ale i denní tisk nebo večerní zprávy můžou existovat jen díky placené reklamě.
Média a influenceři dělají kvalitní obsah, aby měli sledovanost. Firmy platí, aby jejich odběratelům mohly ukázat svůj produkt. A lidi vědí, co si koupit. Reklama může prospívat všem, třeba i propagovat dobrou věc.

…ani dobrá

Reklama nezbytně nelže ani neříká pravdu. Říká, co chceš slyšet, a ukazuje, co chceš vidět. Nefér začíná být až tehdy, když se snaží zamaskovat, že reklamou je. Například, když instagramerka nepřizná spolupráci se značkou nebo když youtuber doporučí produkt, kterému nevěří, protože za to dostal zaplaceno.

Přesný zásah

Každý web, na který přijdeš, si pamatuje tvoji návštěvu díky cookies na stránce. Sociální sítě sbírají údaje o tom, co sleduješ. Google zase ví, co hledáš a kde se pohybuje tvůj mobil. Vědí tak přesně, jaké reklamy ti mají ukazovat.

Bannerová slepota

Ví se, že většina lidí už moc nereaguje na klasické reklamní bannery na stránkách. Proto se tyhle reklamy přesouvají do feedů tvých sociálních sítí, stories, a dokonce i messengerů.

Virální videa

Virální videa se internetem šíří přirozeně a živelně. Pravdou ale je, že za většinou z nich stojí dobře placení experti, kteří vědí, jaké video natočit a jakým lidem ho podstrčit. Ptáš se na jejich motiv? Peníze, co jiného.

I v případě, že novou senzaci do světa sami nevypustili, chytří marketéři se hned chytnou příležitosti a využijí ji ve prospěch své značky. Jen si toho všimni při příštím výskytu virálního memu.

Reklamní blok

Reklamě se nikdy úplně nevyhneš, ale na internetu můžeš spoustu z ní jednoduše zablokovat. Do internetového prohlížeče jde přidat rozšíření, které brání zobrazování bannerové reklamy na webech.

Taky se tím zbavíš otravných reklamních spotů mezi videi na YouTube.

Produkt v hlavní roli

Product placement je chytře kamuflovaná reklama. Produkt se ve filmu, videoklipu nebo na fotce objeví jakoby náhodou.
Někdy je nepřehlédnutelný, jindy rafinovaně nenápadný.
Cílem je dostat ti zboží a značku podprahově do hlavy.

Schválně si příště ve filmu nebo videoklipu všimni, čím hrdina jezdí, co pije a jaký mobil má. Nejspíš napočítáš hned několik značek.
A ano, všechny zaplatily, aby byly vidět.

Další informace, jak reklama funguje a jak se jí případně bránit, najdeš na [www.o2chytraskola.cz.](http://www.o2chytraskola.cz)

O2 | Chytrá škola

Média a jejich způsoby

Máš radši dobré zprávy, nebo ty špatné?
Dá se médiím věřit? Kde je pravda?

Nauč se rozlišovat nestranné zprávy od těch manipulativních.

1. Sociální sítě jako média
2. Sečteno podtrženo
3. Titulky můžou za všechno
4. Clickbait
5. Generátory titulků

Veřejnoprávní média

jsou placená z koncesionářských poplatků a řídí se nejpřísnějšími pravidly. Měla by být tak nezávislá, aby je mocní a politické strany nemohli zneužívat pro své zájmy. U nás jsou tři – Český rozhlas, Česká televize a Česká tisková kancelář.

Seriózní média

jsou soukromá a žijí z reklamy. Zakládají si ale na novinářské cti a etice, takže by měla být také nezávislá a objektivní. Za seriózní se u nás považují třeba deníky MF Dnes, Lidové noviny, Hospodářské noviny nebo E15.

Bulvární média

jsou soukromá a také existují díky reklamě. Zaměřují se na celebrity, senzace a emoce. S pravdou si moc hlavu nelámou, novinářská etika se jich netýká. Informace z nich je potřeba brát s rezervou.

Dezinformační weby

jsou soukromé stránky, které často platí cizí vlády. Mají za úkol šířit falešné zprávy a konspirační teorie, aby ovlivnily názor veřejnosti. Seriózní média se snaží shazovat tvrzením, že o některých věcech záměrně mlčí.

Sociální sítě jako média

Ne nadarmo se řazení příspěvků na sociálních sítích říká news feed (news = novinky nebo taky noviny; a feed = přísun nebo krmivo), protože nás doslova krmí novinkami.

Algoritmy sociálních sítí filtrují, co vidíš, na základě tvého dosavadního klikání.

Takže ti ukazují jen obsah, který chceš vidět. A naopak neukazují obsah, který je s tvými zájmy v rozporu. Když ti ale chybí další úhly pohledu na věc, nemáš kontrolní informaci a spíš uvěříš nepravdě.

Sečteno podtrženo

Pokud tvé informace o světě pocházejí jen z feedu sociálních sítí a od tvých kamarádů, může se svět jevit jako hodně temné nebo naopak sluníčkové místo. Nic ale není černobílé. Proto si informace ověřuj a zajímej se i o názor druhé strany.

Titulky můžou za všechno!

Novináři, blogeři i youtubeři moc dobře vědí, že titulek je nejdůležitější. Dobré znění či změna titulku může znamenat mnohonásobně víc kliknutí.

A kliknutí znamenají peníze.

Clickbait

Tohle anglické slovíčko označuje titulky a obrázky, které tě nalákají k rozkliknutí článku nebo videa za účelem zvednutí návštěvnosti a sledovanosti. Často mohou klamat. Co chceš vědět, se po kliknutí nedozvíš. Bulvární média, dezinformační weby, ale i podvodné a prodejní stránky je běžně používají.

S titulky tímhle způsobem pracují i youtubeři. Jsou v tom ale trochu fikanější a lákají tě místo senzací na osobní obsah typu „Příběh, jak jsme se seznámili...“, „Moje první...“, „Končím s veganstvím“ nebo jen prosté „Q&A“.

Generátory titulků

S clickbaitovými titulky ani není potřeba se příliš namáhat. Stačí zadat klíčové slovo do některého z mnoha title generátorů na internetu. Zkus třeba český Generátor šokujících titulků od Masarykovy univerzity.

Když do něj dosadíš slovo petarda, tohle ti vyplivne:

1. 10 způsobů, jakými z vás reklamní agenti udělají závisláka na petardách
2. 6 důvodů, proč být závislý na petardách
3. 8 věcí, které vám média neprozradila o petardách
4. 10 způsobů, jak vám petardy pomohou žít až do sta let
5. Petardy ovládají školy ve Francii, úřady o tom mlčí
6. Nejneuvěřitelnější článek o petardách, který jste kdy četli
7. Zbraně nezabíjejí lidi, to petardy nás zabíjejí!
8. Souvislost mezi petardami a sexem nalezena!

Zjisti víc o tom, jak fungují média, titulky a falešné zprávy, na **www.o2chytraskola.cz**.

O2 | Chytrá škola

Ochrana osobních údajů

Můžeš na svůj profil vyvěsit fotku kamarádů? Nebo dokonce úplně cizích lidí? Kdo ti může posílat reklamní e-maily a jak moc musí aplikace střežit tvé jméno nebo telefonní číslo?

1. Osobní údaj
2. Citlivý údaj
3. Fotky lidí na internetu
4. Listina dětských práv

Osobní údaj

Jednoduše jde o každou informaci, na základě které tě jde identifikovat.

1. Jméno a příjmení
2. Datum narození
3. Rodné číslo
4. Adresa trvalého pobytu
5. E-mailová adresa
6. Telefonní číslo
7. Číslo občanky nebo pasu
8. IP adresa
9. Fotka, video nebo zvuková nahrávka

Citlivý údaj

Je informace, která se týká tvého soukromí a mohla by tě nějak poškodit, třeba způsobit šikanu nebo diskriminaci.

1. Rasový nebo etnický původ
2. Náboženské vyznání
3. Politická příslušnost
4. Sexuální orientace
5. Zdravotní stav
6. Odsouzení za trestný čin
7. Genetické a biometrické údaje

Fotky lidí na internetu

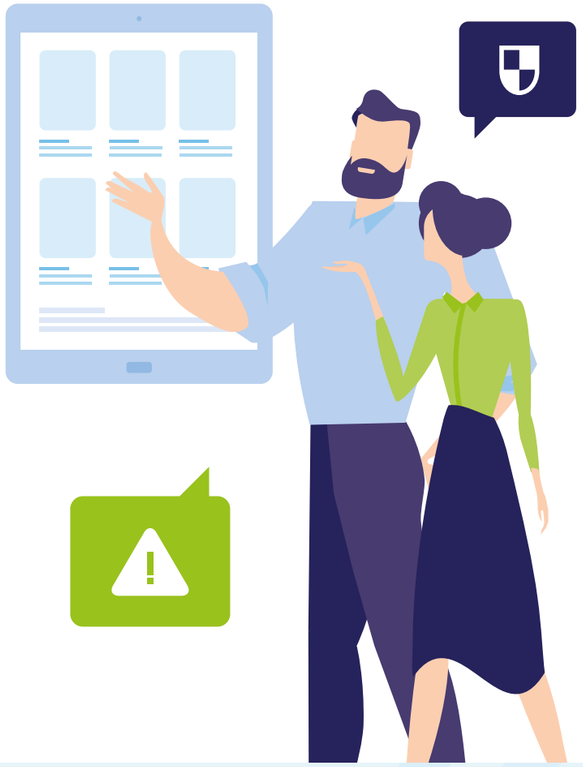
Zveřejnit fotku, video nebo zvukovou nahrávku člověka jde na internetu, v televizi nebo v novinách jen s jeho svolením. Média mohou tohle pravidlo porušit, pokud materiál použijí pro zpravodajské účely jako ilustrační fotku nebo záběr.

Tvá práva a povinnosti

Pokud ti kamarád (nebo ty jemu) ochotně pózuje na fotky, můžeš to brát i jako souhlas s jejich zveřejněním. Pokud tě ale požádá, ať je z profilu stáhneš, musíš to udělat. Stejné právo máš koneckonců i ty, kdyby někdo fotil tebe.
Cizí lidi můžeš fotit taky, ale dej si pozor, ať jim není vidět do obličeje. Fotka nebo video je taky nesmějí zachycovat v nedůstojné situaci.

Příklad:

Pár celebrit už v minulosti upadlo v nemilost pro body shaming, když na svých sociálních sítích sdíleli fotku nebo video cizího člověka s negativními komentáři na jeho tělo. Provinili se totiž hned dvakrát – jednak zveřejněním fotky bez souhlasu, jednak šikanou člověka kvůli jeho vzhledu.



Listina dětských práv na internetu

1. Mám právo bádat, učit se a užívat si na internetu všechny dobré věci.
2. Mám právo nevyplňovat na internetu žádné formuláře a neodpovídat na otázky.
3. **Mám právo uchovávat veškeré informace o sobě v tajnosti.**
4. Mám právo se na internetu cítit bezpečně a být v bezpečí.
5. Mám právo ignorovat e-maily a zprávy od lidí, které neznám nebo kterým nevěřím.
6. Mám právo vždy požádat rodiče nebo vychovatele o pomoc.
7. Mám právo necítit se provinile, když se na obrazovce počítače objeví odporné věci.
8. Mám právo nahlásit dospělým každého, kdo se na internetu chová divně.
9. Mám právo, aby mne nikdo neobtěžoval a netrápil.
10. Mám právo, aby mi lidé na internetu prokazovali respekt.

Přečti si taky, v čem je nebezpečná funkce rozpoznání obličeje, na portále www.o2chytraskola.cz.

O2 | Chytrá škola

Autorská práva

Je stahování seriálů a filmů zločin? Jakou fotku můžeš použít na blog a kde seženeš legální hudbu do svého videa?

Autorské právo

Chrání zájmy každého tvůrce, jako jsou hudebníci, filmaři, spisovatelé, blogeři, malíři, ilustrátoři, grafikové, programátoři nebo třeba architekti.

1. Autorem se člověk stává automaticky a svých práv se nemůže vzdát.
2. Práva na své dílo ale může prodat nebo někomu přenechat.
3. Autorské právo se dědí, ale platí jen 70 let po smrti autora. Pak je dílo volně k dispozici všem.
4. Jen majitel práv ti může dát svolení k použití díla.

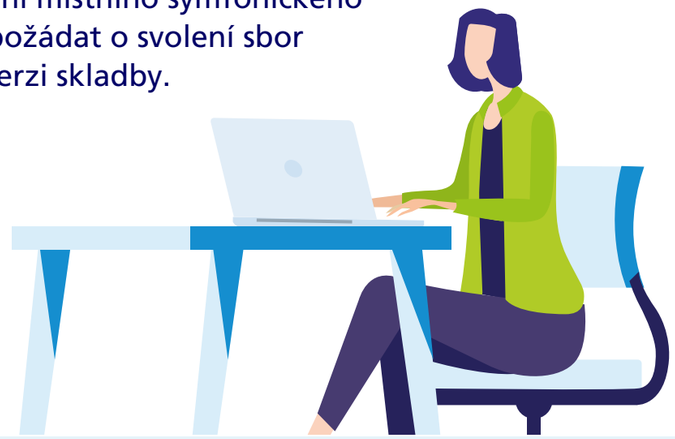
Zločin, nebo ne?

1. **Stahování filmů a seriálů**
   Pokud streamuješ nebo stahuješ filmy a seriály jen pro sebe, tak ne. Pokud ale stahuješ přes torrent (kde při stahování sdílíš) nebo pak stažená videa dáš dalším lidem, porušuješ zákon.
2. **Používání softwaru**
   Legálně můžeš používat řádně koupené, bezplatné nebo zkušební verze (trialy) programů. Pokud si software stáhneš nelegálně a rozchodíš ho přes crack, porušuješ zákon.
3. **Použití cizí fotky na blogu**
   Pokud ti autor fotky dovolil ji použít, všechno je v pořádku. Jestli ne, porušuješ zákon.
4. **Použití cizí hudby ve videu**
   Jestli ti autor odsouhlasil použití, směle do toho. Pokud ne, můžeš dostat i pokutu za porušování jeho práv.

Kde sehnat fotky a hudbu zdarma

1. Od kamarádů hudebníků a fotografů (samozřejmě s jejich svolením)
2. Z bezplatné foto-, video - nebo audiobanky na internetu
3. Na internetu, pokud jde o materiál s volnou licencí

Příklad:
Potřebuješ do svého videa na YouTube hudební podkres. Chceš se vyhnout autorským právům, a tak použiješ symfonii od Beethovena, která už je zdarma. Jenže chyba lávky. Na skladbu už sice nikdo autorská práva nemá, ale na nahrávku v podání místního symfonického sboru ano. Musíš tedy požádat o svolení sbor nebo si nahrát vlastní verzi skladby.



Creative commons

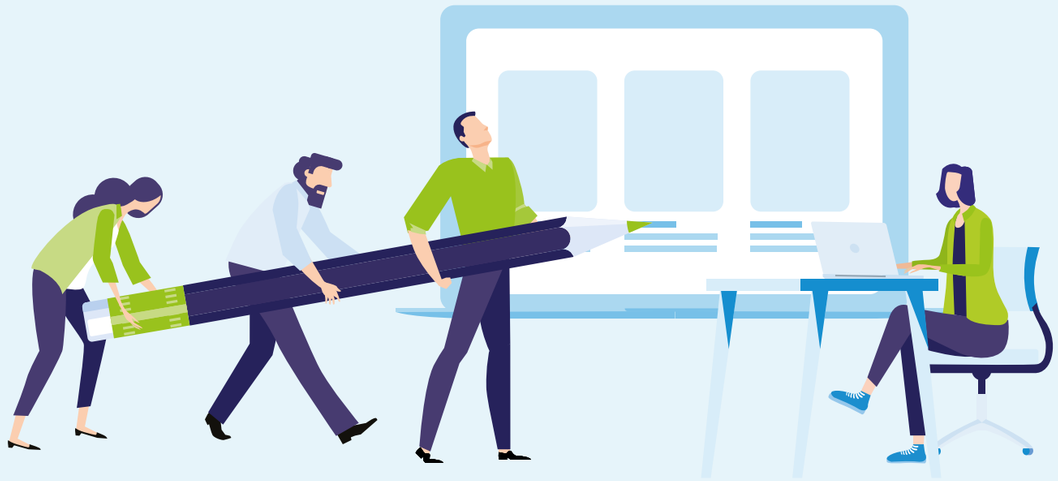
Creative commons označuje všechen obsah, který jeho autoři dali lidem zdarma k užívání. Značka CC pak udává, jak přesně můžeš fotku, hudbu nebo video použít. Nejčastěji je to k nekomerčním účelům.

Autorská práva a sociální sítě

Na sociálních sítích můžeš zveřejňovat jen svoje věci nebo díla ostatních, když k tomu máš jejich souhlas.
Jiné je to ovšem se sdílením postů, které už zveřejnil někdo jiný. Ty můžeš v rámci sociální sítě šířit bez obav.

Příklady

1. Zveřejnit na Instagramu fotku, která není tvoje, bez souhlasu autora je porušení pravidel. Ale sdílet fotku z kamarádova Instagramu na svém Facebooku už ne.
2. Nahrát na YouTube video bez souhlasu autora je porušení pravidel. Udělat si na YouTube seznam z videí, které uveřejnil někdo jiný, ale ne.



Podívej se na **www.o2chytraskola.cz** a zjisti víc o tom, co a jak můžeš stahovat a sdílet.

Mediální stereotypy

Jsou vojáci zelené mozky, muslimové teroristi a bezdětné ženy sobecké kariéristky? Co je pravdy na stereotypech, které slýcháš ze všech stran?

Co je stereotyp

Jako stereotyp označujeme často nepřesné a ne zcela pravdivé představy o člověku nebo lidech, které většinová společnost sdílí. Stereotypy můžeš chápat taky jako předsudky, i ty jsou založené na informacích a názorech z druhé ruky nebo nedokonalém prvním dojmu.

Kdo stereotypy vytváří

1. Většinová společnost (mainstream)
2. Média všeho druhu
3. Zájmové a politické skupiny

Kdo jsou obětí stereotypů

1. **Cizí národnosti**
   Poláci jsou kšeftaři, Kolumbijci zase drogoví dealeři a Britové pijí jen čaj.
2. **Etnika a rasy**
   Romové zneužívají sociální dávky, Afroameričané jsou skvělí sportovci a Asiatům jde matematika.
3. **Náboženské a ideologické skupiny**
   Katoličtí kněží zneužívají děti, muslimové jsou teroristi a vegani jsou přecitlivělí radikálové.
4. **Sociální skupiny**
   Gayové jsou zženštilí, boháči jsou zlí vykořisťovatelé a blondýnky jsou hloupé.
5. **Profesní skupiny**
   Policisté jsou natvrdlí, úřednice nepříjemné a kopáči se líně opírají o lopatu.
6. **Ženy vs. muži**
   Ženy se řídí hlavně city a jsou špatné řidičky, muži nikdy nepláčou a neptají se na cestu.

Média a stereotypy

Se stereotypy pracují dezinformační weby, bulvár, ale i seriózní média. Seriózní média to jen nedělají přímo. Nikdy stereotypy nepojmenovávají, podají je na příkladu jedince, který zavedený stereotyp potvrzuje. Tím ti potvrdí to, co už si dávno myslíš.

A proč to dělají?
Protože čtenáři, diváci a posluchači to tak chtějí.
Mediální stereotypy vyjadřují názor lidí a zároveň ho vytvářejí.
Problém je, že třeba v případě národnostních menšin se výrazně častěji mluví o špatných věcech než o těch dobrých. Do zpráv se proto dostane případ jednoho Roma zloděje, ale už ne příběh všech těch ostatních, kdo žijí spořádaný život.

Ach jo

Pokud nemáš přímou zkušenost s menšinou nebo skupinou, běžně kolující stereotypy jsou bohužel tvým hlavním zdrojem informací.

Stereotypy můžou bolet

Stereotypy do sebe nasáváme od malička z filmů, pohádek, novin i toho, co říkají lidi kolem nás. Pokud je bezmyšlenkovitě opakuješ, aniž si vytvoříš vlastní názor, můžeš nechtěně ublížit třeba kamarádovi, kterého se stereotyp týká.

Stereotypy jsou nebezpečné

Stereotypy pracují na jednoduchém principu – kdo není jako my, je potenciální hrozba. V historii už stereotypy mnohokrát posloužily k tomu, aby z lidí udělaly podřadná stvoření bez lidských práv. Například pokus o vyhlazení všech židů za 2. světové války nebo staletí, kdy otroctví bylo zcela běžné a život otroka měl takovou hodnotu, jakou mu přisoudil jeho majitel.

Podívej se na **www.o2chytraskola.cz** a zjisti o stereotypech víc.

Propaganda

Co je propaganda?
Kdo za ní stojí a co má v plánu?
A je vlastně propaganda nezbytně špatná věc?

Co je propaganda

Propaganda má za cíl ovlivnit naše názory, postoje a přimět nás chovat se tak, jak její autoři zamýšleli. Nejčastěji s námi manipuluje přes emoce, jako je například strach. Krmí nás většinou nepravdami a informacemi vytrženými z kontextu. Často zamlčuje nebo překrucuje fakta, která je vyvracejí.

Jeden z nejhorších příkladů propagandy je nacistická protižidovská propaganda, která začala před 2. světovou válkou a vyústila vyvražděním milionů židů v koncentračních táborech během ní.

Kde se vzala

Slovo propaganda máme z názvu Posvátné kongregace pro šíření víry (Sacra congregatio de propaganda fide). Ta vznikla na začátku 17. století a jedním z jejích úkolů byla osvěta ohledně katolické církve. Dnes bychom to nejspíš označili marketingovým termínem „budování značky“.

3 odstíny propagandy

Propaganda ale nemusí být vždycky jen špatná. Vlastně rozlišujeme několik druhů propagandy.

1. **Bílá propaganda**
   (známe její zdroj i cíl)
   Stojí za ní konkrétní instituce a svými technikami je srovnatelná s reklamou. Její záměr je vždy pozitivní, například osvěta o používání bezpečnostních pásů, o rizicích kouření nebo třeba o prospěšnosti pohybu a zdravé stravy.
2. **Šedá propaganda**
   (neznáme zdroj, ale známe nebo tušíme cíl)
   Snadno poznáme, že jejím cílem je třeba útok na politickou stranu nebo firmu a snaha jim uškodit. Nemůžeme ale přesně říct, kdo za útokem stojí. Šíří mylné nebo zavádějící informace, aby toho docílila.
3. **Černá propaganda**
   (neznáme zdroj a neznáme přesný cíl)
   Je nejzákeřnější a nejnebezpečnější, protože používá lži, fake news, hoaxy a manipulaci. Působí na emoce silnými sděleními a skrývá své pravé záměry i autora. Často si navléká masku rádoby věrohodných zdrojů (dezinformační weby).

Jak propaganda manipuluje

Propaganda stejně jako reklama útočí na naše základní emoce. Dělá to dokonce i propaganda pozitivní.

Nebezpečné jsou ale techniky šedé a černé propagandy:

1. Apeluje na náš strach.
2. Svaluje vinu na toho, kdo se jí nehodí.
3. Nálepkuje menšiny, etnika, zájmové skupiny a další oponenty.
4. Vymýšlí si a vědomě lže.
5. Manipuluje s obrázky a videi.

Cenzura

Cenzura (ve zkratce) zabraňuje tomu, aby se zveřejňovaly informace a názory, které odporují systému a ideologii státu (třeba komunismu, dřív např. fašismu). Týká se knih, filmů, umění, masových médií, ale i sociálních sítí. Provádí ji stát nebo instituce, které k tomu stát pověřil.

- **Stojí to v ústavě**
  U nás je cenzura zakázaná. Jiné země na světě ale takové štěstí nemají. Například v Číně nebo Severní Koreji běžně nejdou spustit některé webové stránky nebo sociální sítě jako Facebook.

Čti o propagandě a jejích dopadech na www.o2chytraskola.cz