

Strážci na internetu

Martin Kožíšek

Vydavatel:

CZ.NIC, z. s. p. o.

Milešovská 5, 130 00 Praha 3

Edice CZ.NIC

www.nic.cz

1. vydání, Praha 2024

Kniha vyšla jako 32. publikace v Edici CZ.NIC.

© 2024 Martin Kožíšek

Toto autorské dílo podléhá licenci Creative Commons BY-ND 4.0 (<https://creativecommons.org/licenses/by-nd/4.0/>). Dílo však může být překládáno a následně šířeno v písemné či elektronické formě, na území kteréhokoliv státu, za předpokladu, že nedojde ke změně díla a i nadále zůstane zachováno označení autora a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Překlad může být šířen pod licencí CC BY-ND 4.0.



Spolufinancováno
Evropskou unií

cz.nic | SPRÁVCE
DOMÉNY CZ

ISBN 978-80-88168-73-7

STRAŽCI
NA internetu

Obsah



Část 1 – Hesla a zabezpečení.....	10
Kapitola 001 – Registrace.....	10
Kapitola 002 – Jak by mělo vypadat heslo.....	11
Kapitola 003 – Jak mít dlouhé heslo, a přitom si ho pamatovat.....	12
Kapitola 004 – Musím si pamatovat desítky hesel?	13
Kapitola 005 – Generátory hesel.....	14
Kapitola 006 – Správce hesel.....	14
Kapitola 007 – Mám vyplňovat telefonní číslo do účtu?.....	15
Kapitola 008 – Dvoufázové ověření (2FA)	16
Kapitola 009 – Co dělat, když přijdu o heslo.....	18
Kapitola 010 – Jak se může útočník dostat k heslu?.....	19
Kapitola 011 – Byl můj účet nebo moje heslo zneužito?	20
.....	
Část 2 – Ochrana mobilního telefonu	21
Kapitola 012 – Půjčování telefonu	22
Kapitola 013 – Jak zabezpečit telefon pomocí PIN.....	23
Kapitola 014 – Jak si zabezpečit telefon pomocí gest.....	24
Kapitola 015 – Zabezpečení telefonu pomocí biometrických „hesel“	25
Kapitola 016 – Automatické uzamknutí displeje	26
Kapitola 017 – Co je IMEI a na co ho budu potřebovat.....	28
Kapitola 018 – Co dělat, když mi ukradnou telefon.....	29
Kapitola 019 – Co dělat, když dostanu nový telefon.....	30
Kapitola 020 – Zálohuj!	31
Kapitola 021 – Aktualizuj!.....	32
Kapitola 022 – Mám mít antivir v telefonu?.....	33
Kapitola 023 – Jak poznat, že je telefon zavirovaný.....	34
Kapitola 024 – Instalace aplikací odjinud.....	35
Kapitola 025 – Jaké aplikace si stáhnout.....	36
Kapitola 026 – Placené aplikace	38
Kapitola 027 – Výhody sdílení polohy přes aplikace.....	39
Kapitola 028 – Nevýhody sdílení polohy přes aplikace	40
Kapitola 029 – Náhledy zpráv.....	41

Kapitola 030 – Premium SMS.....	42
Kapitola 031 – Smishing	44
Kapitola 032 – Jak se připojit bezpečně na Wi-Fi síť.....	45
Kapitola 033 – Omez používání telefonu před spaním.....	46
Kapitola 034 – Bluetooth.....	47
Kapitola 035 – VPN	48
.....	
Část 3 – Internetové prohlížeče a vyhledávače	49
Kapitola 036 – Co je internetový prohlížeč	50
Kapitola 037 – Cookies.....	51
Kapitola 038 – Anonymní okna a historie.....	52
Kapitola 039 – Viry.....	53
Kapitola 040 – SPAM.....	55
Kapitola 041 – Phishing	56
Kapitola 042 – Prodávám. A nenaletím.....	58
Kapitola 043 – Hoax	59
Kapitola 044 – Doplnky do prohlížeče (Pluginy)	61
Kapitola 045 – Clickbait.....	62
Kapitola 046 – Vyhledávače	63
Kapitola 047 – Vyhledávání obrázků, článků nebo videí.....	65
.....	
Část 4 – Sdílení obsahu na internetu	66
Kapitola 048 – Digitální stopa.....	67
Kapitola 049 – Jaký obsah sdílet?.....	69
Kapitola 050 – Co můžeš sdílet.....	70
Kapitola 051 – Označování uživatelů.....	71
Kapitola 052 – Nikdy bez oblečení!.....	72
Kapitola 053 – Streamování	73
Kapitola 054 – Nebudte lhostejní.....	74
Kapitola 055 – Testíček.....	75
.....	
Část 5 – Sociální média.....	76
Kapitola 056 – Co je sociální síť?	77
Kapitola 057 – Typy sociálních sítí.....	78
Kapitola 058 – Jaký obsah sdílet na síti.....	79



Kapitola 059 – Lajky	81
Kapitola 060 – Přezdívky	82
Kapitola 061 – Falešné profily a jak je odhalit	83
Kapitola 062 – Více o falešných profilech	85
Kapitola 063 – Co mám dělat, když narazím na fejk?	86
Kapitola 064 – Osobní údaje jsou velmi cenné, opatruj je!	87
Kapitola 065 – Ignorece/Blokace	88
Kapitola 066 – Chladná hlava	90
Kapitola 067 – Selfie	91
Kapitola 068 – Králičí nory	93
Kapitola 069 – Bublíny	95
Kapitola 070 – Třetí strany	96
Kapitola 071 – Jak odejít ze sítě, která mě už nebaví	97
.....
Část 6 – Seznamování na internetu	98
Kapitola 072 – Seznamky	99
Kapitola 073 – Zrcadlení, metoda podvodníků	100
Kapitola 074 – Oslovení útočníků – Rychle na věc	101
Kapitola 075 – Neodolatelné nabídky	102
Kapitola 076 – Snaha tě izolovat od ostatních	103
Kapitola 077 – Podvod s webkamerou	104
Kapitola 078 – Mluvíš jako můj děda	105
Kapitola 079 – Seznámení naživo	106
Kapitola 080 – Ptej se na podrobnosti	108
Kapitola 081 – Jména	109
Kapitola 082 – Predátoři	110
Kapitola 083 – Další testíček!	112
.....
Část 7 – Kyberšikana	113
Kapitola 084 – Co je kyberšikana	114
Kapitola 085 – Rozdíl mezi šikanou a kyberšikanou	115
Kapitola 086 – Kyberšikana jako nepovedený žert	116
Kapitola 087 – Kyberšikana „v dobrém úmyslu“	117
Kapitola 088 – Kyberšikana kvůli digitální stopě	118
Kapitola 089 – Proč zrovna já?	119
Kapitola 090 – Když budu anonymní, nikdo mě neodhalí!	120
Kapitola 091 – Verbální útoky	121
Kapitola 092 – Rozliš, zda jde o kyberšikanu	123
Kapitola 093 – Ztrapňování šířením fotografie nebo fotomontáže	124



Kapitola 094 – Ztrapňování šířením fotografie nebo fotomontáže (příběh)	125
Kapitola 095 – Ztrapňování šířením videa nebo zvukové nahrávky	126
Kapitola 096 – Dívka z autobusu (příběh)	127
Kapitola 097 – Vyhrožování a zastrasování	128
Kapitola 098 – Vyhrožování a zastrasování (příběh)	129
Kapitola 099 – Krádež identity	130
Kapitola 100 – Krádež identity (příběh)	131
Kapitola 101 – Průnik na účet s cílem oběť zesměšnit	132
Kapitola 102 – Průnik na účet s cílem oběť zesměšnit (příběh)	133
Kapitola 103 – Obtěžování prozváněním	134
Kapitola 104 – Obtěžování prozváněním (příběh)	135
Kapitola 105 – Vydírání	136
Kapitola 106 – Vydírání (příběh)	137
Kapitola 107 – Nechtějí mě ve třídní skupině (digitální ostrakizace)	138
Kapitola 108 – Vyloučení z kolektivu (ostrakizace) příběh	139
Kapitola 109 – Stalking	140
Kapitola 110 – Stalking (příběh)	141
Kapitola 111 – Trolling	142
Kapitola 112 – Trolling (příběh)	143
Kapitola 113 – Je kyberšikana trestná?	144
Kapitola 114 – Obrana proti kyberšikaně	145
Kapitola 115 – Filmy a seriály ke kyberšikaně	146
Kapitola 116 – Testíček	147
.....
Část 8 – Rizika spojená s hrami	148
Kapitola 117 – Online hry	149
Kapitola 118 – Loot boxy	150
Kapitola 119 – Krádeže herních účtů	151
Kapitola 120 – Čas strávený online	152
Kapitola 121 – Esport	153
Kapitola 122 – Modrá velryba	154
Kapitola 123 – Online výzvy (Online challenges)	155
Kapitola 124 – Kocourovo desatero bezpečného hraní online her	156
Kapitola 125 – Závěrem	157



Nazdárek, moje jméno je **MIA** a na internetu se hlavně bavím s kámoši. Snažím se jim poradit, když se dostanou do těžké situace. Mezi nimi je i Kocour, kterej pořád vymejší na internetu nějaký ptákoviny.



Ahoj, já jsem **KOCOUR** a baví mě hlavně hry a sociální sítě. Hodně času trávím na internetu tím, že sjiždím videa nebo poslouchám hudbu. Hraju hry a taky čas od času streamuju nebo se seznamuju s novými kočkama.



Moje jméno je **ROBOT**, model **Ypsilon**. Mezi moje naprogramování patří listování v encyklopedii, uvádění informací na pravou míru nebo radím, jak být na internetu v bezpečí.



Základy, jak být na internetu v bezpečí



Internet je možná jeden z největších vynálezů lidstva

Bla, bla, bla. Vždycky přijde někdo s tím, že je něco největší, cool a tak



Jak to myslíš, Kocoure?

Dřív to byl telegraf, telefon, rádio. Pak přišla televize...



A první počítač...

Ten první by se vám ale do bytu nevešel.
Můj praprapraděda vážil tunu. Ale já už jsem v kapesní verzi.



Prostě to zapnu a hraju



Nebo se můžeš podívat, co se děje ve světě,
seznámit se, dívat se na videa nebo...

Někoho okrást, podvést, zneužít



Ale no tak, Kocoure, internet je fajn. Jen si musíme dát na pár věcí pozor

Na pár?



Dobrá, tak se na to společně podíváme.
Zapněte svůj digitální a kočičí mozek a jdeme na to!

Část 1

Hesla a zabezpečení

Silné a bezpečné heslo je velmi důležité pro pohyb na internetu. Heslo potřebuješ pro využívání většiny služeb a je jedno, jestli používáš internet z počítače, tabletu nebo mobilu. Dáme ti pár tipů, jak si ho správně nastavit a používat.

Kapitola 001 – Registrace

Věnuj čas registraci do nové služby. Není nutné vyplňovat všechny položky ve formuláři (třeba to, jaké máš zájmy, nebo nepovinné osobní údaje).

Ty důležité ale vyplň pečlivě. Všechno lze rychle odkliknout, ale když zapomeš heslo, už ho nejspíš nedostaneš zpátky.





**Osobní údaje na internetu jsou ta nejcennější věc.
Zvaž, jaké informace službám poskytujes.**

Kapitola 002 – Jak by mělo vypadat heslo

Při vymýšlení hesel si zkus zapamatovat pár pravidel:

- 1] Nemělo by být jednoduché (např. 123456, heslo, jméno, slovo)
- 2] Střídej malá i velká písmena, číslovky a speciální znaky
- 3] Do hesla přidej více než jeden speciální znak (@, \$, €, &, # apod.)
Čím složitější heslo je, tím těžší je ho uhádnout. Zkus speciální znak ale nedávat na začátek ani na konec
- 4] Vyvaruj se slov, osobních údajů nebo frází, které může někdo znát (datum nebo rok narození, adresa, číslo popisné, jméno domácího mazlíčka, název oblíbené knihy nebo filmu, jídla apod.)
- 5] Heslo nemusí mít kilometr, ale je dobré, aby bylo delší. Ideální heslo má mít minimálně 8 znaků, doporučuje se jich ale 15

Nikomu
své heslo
nesděluj!



Podívej se, za jak dlouho se dá prolomit heslo



8 znaků

Heslo obsahuje:

- Malá i velká písmena
- Číslovky
- Speciální znaky

**Prolomení hesla za
40 minut**

12 znaků

Heslo obsahuje:

- Malá i velká písmena
- Číslovky
- Speciální znaky

**Prolomení hesla za
3.000 let**

15 znaků

Heslo obsahuje:

- Malá i velká písmena
- Číslovky
- Speciální znaky

**Prolomení hesla za
1.000.000.000 let**

Kapitola 003 – Jak mít dlouhé heslo, a přitom si ho pamatovat



To si mám opravdu pamatovat heslo delší než moje jméno?

Dá se to trochu hacknout. Chceš super vychytávku?
Máš nějakou oblíbenou písničku nebo frázi, kterou nikdo nezná?



Skákal pes přes oves, přes zelenou louku...

Jako vážně?
No dobře, u každého slova změň velikost písmen
a přidej za slova speciální znaky a máš superbezpečné heslo



SkakaL@PeS?PreS!OveS nebo OveS-PreS-PeS-SkakaL!



Pokud používáš slovní frázi jako heslo, můžeš přehodit pořadí slov. Podívej se i na kapitoly 004 – 008, které ti poradí, jak heslo uchovat v bezpečí.

Které z následujících hesel není silné?

nONX08†%/?\$_P\

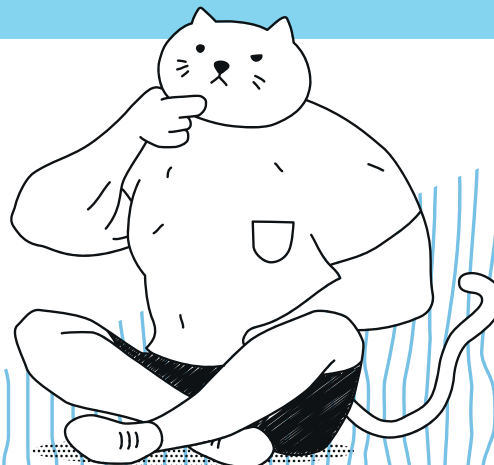
Oskar2015

QwertyQ

jedU*VlakeM_d0@Skoly

JJrZ-o@AS

Anet4



Kapitola 004 – Musím si pamatovat desítky hesel?



Na internetu jsou miliony služeb. Kdybych chtěl být na každé z nich, musím mít pokaždé jiné heslo?

Já mám digitální mozek, ale ty bys to určitě nezvládl.



Takže můžu mít všude stejné heslo?

To určitě ne! Kdyby totiž tohle heslo uniklo a dostalo se do nepovolaných rukou, ohrozilo by to všechny tvoje účty na službách, které jsi používal.



Robot má možná nekonečnou paměť, ale je jasné, že my si všechna hesla nemůžeme zapamatovat. Naštěstí známe pár vychytávek, které nám mohou s hesly pomoci



Některé služby použiješ jen pro jednorázovou akci, soutěž nebo si nastaviš odběr newsletteru s nabídkami. Když účet ztratíš nebo heslo zapomeneš, nic se nestane. U těchto služeb můžeš mít všude totožné nebo nějaké jednodušší heslo.

Takže si místo milionu hesel budu pamatovat jen polovinu, super!



Vezmi si papír a rozděl ho čarou na dvě poloviny. Na levou stranu napiš seznam všech služeb nebo aplikací, které obsahují osobní údaje. Na pravou stranu pak ty, které používáš, ale neobsahují důležité informace

Kapitola 005 – Generátory hesel

Pokud tě nenapadá, jaké silné heslo si zvolit, můžeš využít některou ze služeb, které je vygenerují za tebe. Nastavit si můžeš jeho délku nebo to, jestli bude obsahovat speciální znaky nebo velká a malá písmena.



Už generuju

Jo. Náhodný slova, kterýma mě zahlcuješ,
když chci odpočívat. Zííiv



Stránky, na kterých se můžeš při vytváření hesla inspirovat:

<https://www.avast.com/cs-cz/random-password-generator>

<https://www.eset.com/cz/generator-hesel/>

<https://www.nove-heslo.cz/>

Kapitola 006 – Správce hesel

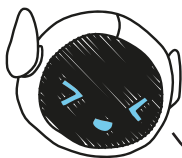
Pamatovat si tolik různých a složitých hesel není jednoduchá věc. Naštěstí existuje tzv. správce hesel, který všechna hesla uloží na jedno místo, což je nejen pohodlné, ale i bezpečné.

Nemusíš se bát, je to vlastně takový trezor, který je zašifrován nejnovějšími
a nejsložitějšími algoritmy



Správce hesel je dostupný pro mobilní telefony, tablety i počítače. Některé jsou zdarma, některé však placené. Mezi nejznámější aplikace pro správu hesel patří: 1Password, Keeper, Bitwarden nebo StickyPassword.

Kapitola 007 – Mám vyplňovat telefonní číslo do účtu?



Pokud jde o důležitou službu, kterou využíváš denně nebo která obsahuje osobní údaje, tak ano. Takovou službou mohou být sociální sítě, e-maily, bankovní účty apod. Nemusíš se bát, že tvoje číslo někdo zneužije.

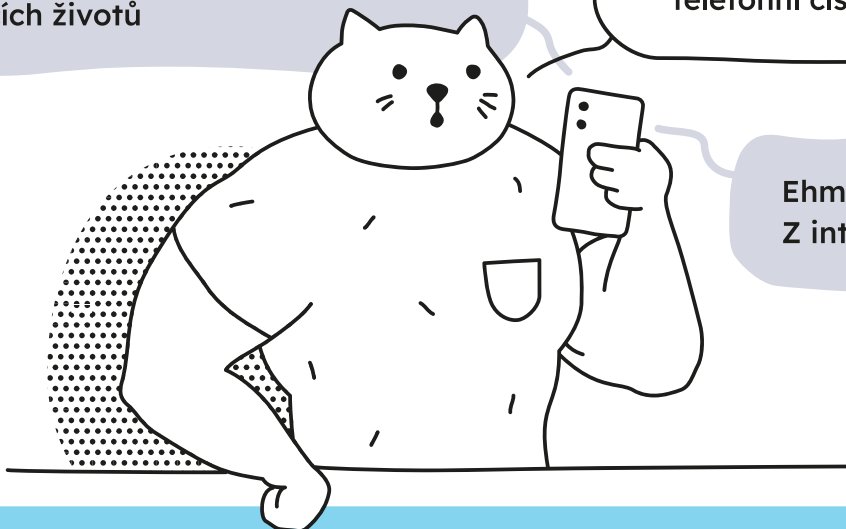
Telefonní číslo ale nedávej neznámým službám



Haló, to je pan Kocour?
Rád bych Vám nabídl nejnovější
robotický vysavač se zárukou devíti
kočičích životů

Odkud znáte moje
telefonní číslo?

Ehm...mmm...
Z internetu?



Když zapomeněš heslo nebo se ti někdo dostane do účtu, necháš si poslat nové heslo nebo kód k jeho obnovení na mobilní telefon.

Kapitola 008 – Dvoufázové ověření (2FA)



Služby, které obsahují osobní údaje, komunikaci nebo finance, bychom měli chránit, jak nejlépe dovedeme

s nožem v ruce



takhle to Robot nejspíš nemyslel



Kromě hesla by měla mít služba ještě další způsob zabezpečení

Dvě hesla?

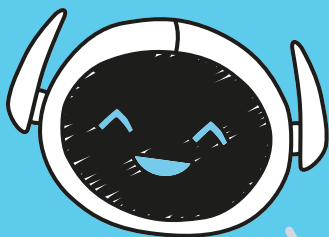


je to marný, je to marný, je to...

Mia opustil/a skupinu



Myslel jsem spíš dvoufázové ověření



Vypadá to složité. Ale je to velmi jednoduché a jedná se o jeden z nejlepších způsobů zabezpečení tvého účtu.

Při přihlašování do účtu pomocí jména a hesla musíš ještě něčím jiným prokázat, že je účet tvůj. Po zadání hesla tak budeš muset zadat další potvrzení.

Může jít o SMS, PIN, otisk prstu, biometrický sken obličeje nebo třeba jen potvrzení v aplikaci instalované v telefonu.

Ale neboj, většina služeb navíc umí poznat, že se přihlašuješ ze svého počítače, a na nic dalšího se tě neptá.



Někdy to může být otravné, ale vyplatí se to. Představ si, že máš účet na herním portálu a nakoupené drahé hry. Byla by škoda o ně přijít jen kvůli špatnému zabezpečení. Tolik peněz, achievementů, skinů a dalších věcí.

3

kroky k 2FA

Heslo

• • • • • |

Potvrďte přihlášení v aplikaci

OK

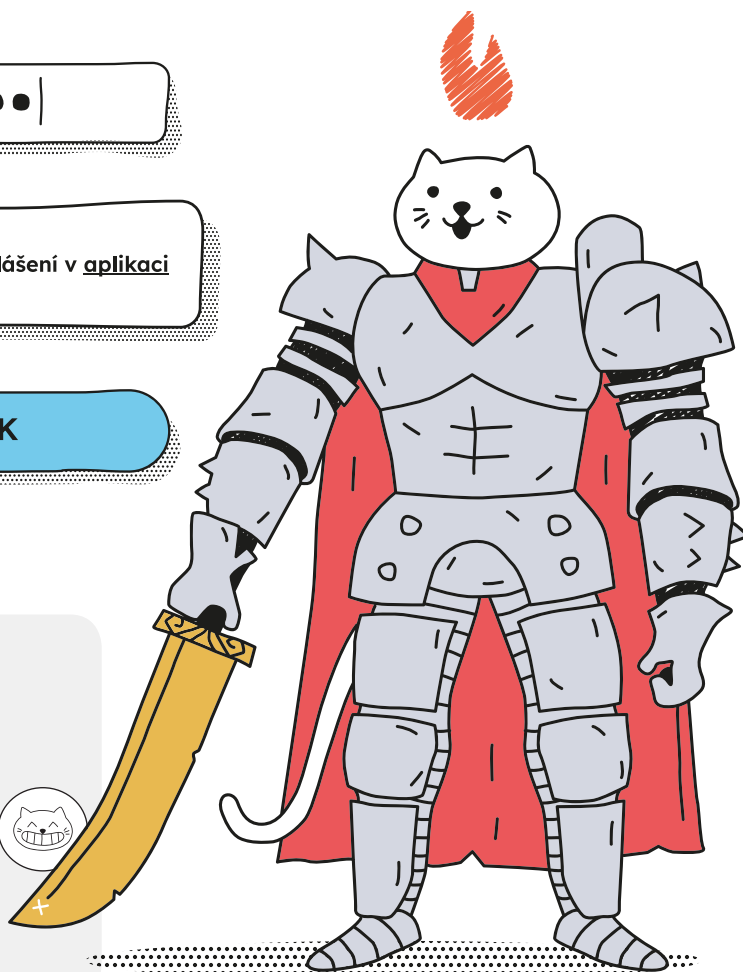


Já žádné hry nehraju

To mě nepřekvapuje. Ale já mám fakt hustý skiny na kočičí zbraně



Jako zlatý dráp?



Kapitola 009 – Co dělat, když přijdu o heslo

O heslo můžeš přijít mnoha způsoby. Nejčastější situací ale je, že ho zapomeneš. Proto je při registraci účtu důležitá pečlivost. Už víš, že si nové heslo můžeš nechat zaslat na telefonní číslo, pokud je vyplněno v registraci. Někdy je záchytným bodem jiná e-mailová schránka, ověřené kontakty nebo další vyplněné údaje.

Jak to bylo...
MňauVrrr, nebo Mňaučiči...
MýtMyš, nebo MítMyš?



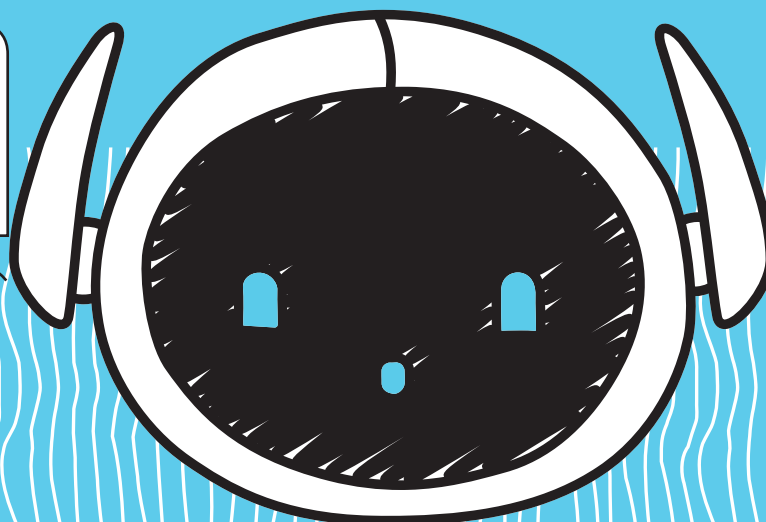
Kde najdeš pomoc?

Odkazy na záchranu hesla najdeš většinou v „patičce“ stránky (na stránce úplně dole) nebo v menu stránky. Obvykle se odkaz jmenuje **Nápověda, Technická podpora, Napiš nám nebo Obnovit heslo**. Budeš muset vyplnit formulář. Některé služby ti ale nabídnou chat s operátorem nebo telefon s ním.

Kapitola 010 – Jak se může útočník dostat k heslu?

- Uhádne ho, protože je příliš jednoduché. Obsahuje například jméno, nějaké slovo a k tomu přidanou číslovku (Martin1, Katka123, admin555...)
- Máš ho napsané na lístečku, v sešitu, řekneš ho kamarádům nebo někdo uvidí, jak ho zadáváš do počítače nebo mobilu
- Zapomeneš se odhlásit z veřejného počítače
- Připojuješ se na neznámou, nezabezpečenou Wi-Fi
- Získá ho podvodem, třeba přes phishing (kapitola 041)
- Zaútočí pomocí speciálních nástrojů (například škodlivý software)
- Pokud používáš stejné heslo na více službách, pak stačí, když heslo unikne i jen z jediné z těchto služeb
- Použije tzv. slovníkový útok, který velmi rychle odhalí nejčastější slova a jejich kombinace (Kokos123, Praha_13, Novak1979...)

**Dříve bylo možné účty
ochránit jen kontrolní
otázkou. To už dnes nestačí.
Pokud by na ni někdo uhodl
odpověď, můžeš o účet přijít.**



Kapitola 011 – Byl můj účet nebo moje heslo zneužito?



Robote, dá se zjistit, jestli už někdo můj účet zneužil?

Zadej svůj e-mail na službě <https://haveibeenpwned.com/> a uvidíš

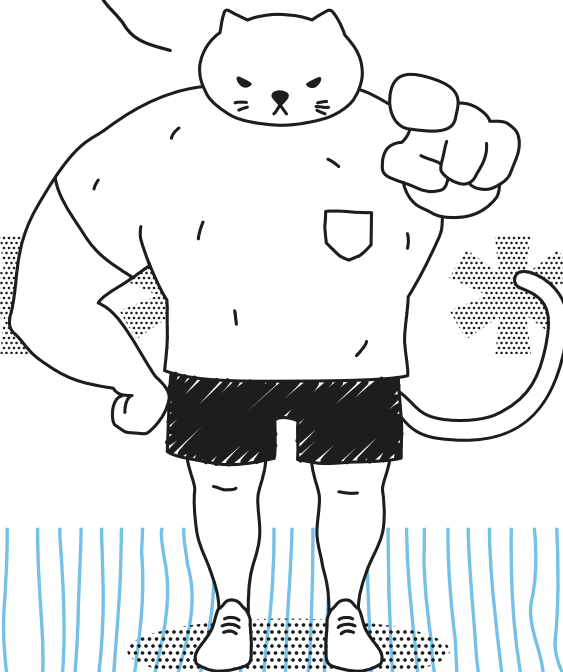


Já mám strach

Kocour tě sice může naučit nějaký kočičí chvaty,
ale bude stačit, když si to heslo okamžitě změníš



Jestli mi ukradneš heslo,
tak si tě najdu!



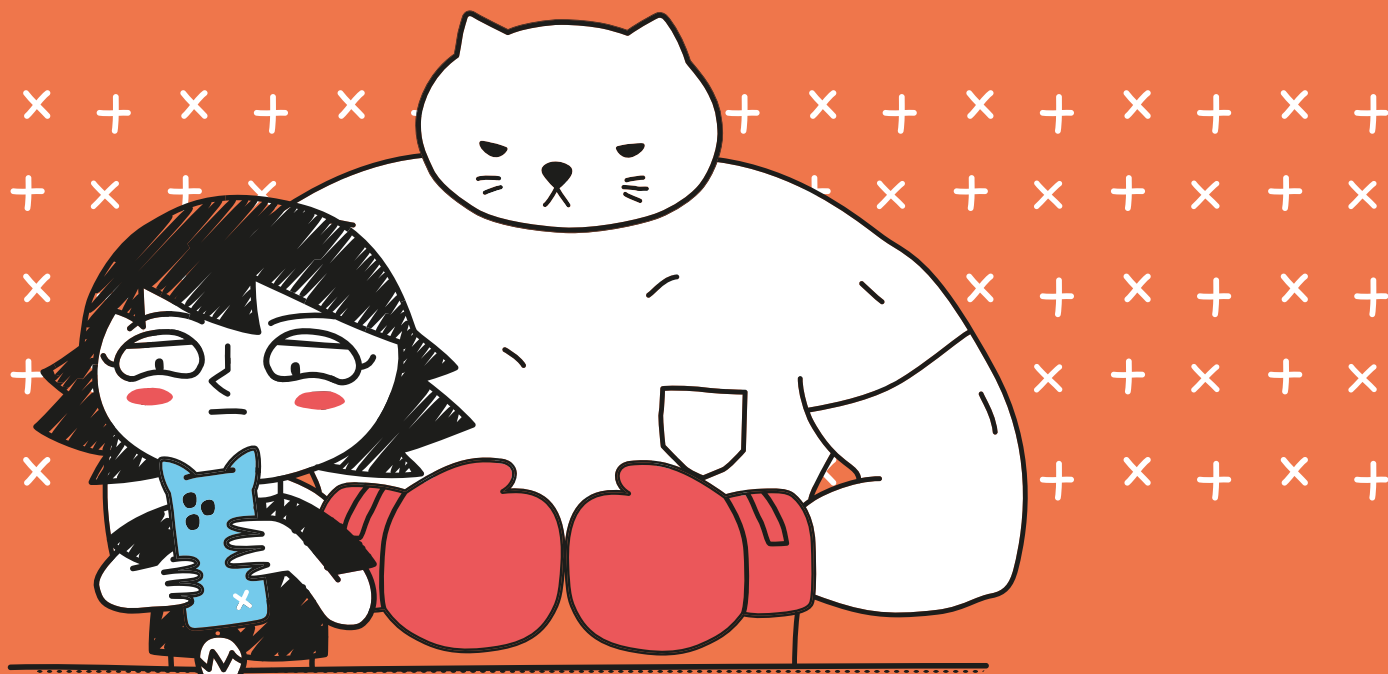


Část 2

**Ochrana mobilního
telefonu**

Kapitola 012 – Půjčování telefonu

Určitě víš, že bychom neměli telefon půjčovat cizím lidem. Kamarádům také ne. Když se i přesto tak rozhodneš, buď u toho a měj svůj telefon pod dozorem. Proč? V telefonu jsme většinou automaticky přihlášení k mnoha službám a cizí lidé se k nim mohou jednoduše dostat.



Mobilní telefon je vlastně malý kapesní počítač. Umí dost věcí a je také docela drahý, byla by škoda přijít o něj nebo o údaje v něm obsažené. Spousta z nás má v telefonu velké množství fotek, videí nebo informací. Obsahuje také soukromou komunikaci, kterou by neměl vidět nikdo cizí.

Mobil je můj
vzdálenější
bratranec



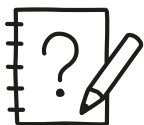
Kapitola 013 – Jak zabezpečit telefon pomocí PIN

PIN je bezpečnostní číselný kód, který bývá většinou čtyřmístný. PIN je nám obvykle přidělen, ale je možné si ho změnit. Stejně jako u hesel bychom si měli nastavit takový PIN, který nebude možné tak jednoduše uhodnout.

Špatné piny

Čísla opakující se nebo jdoucí za sebou (1212, 1234, 4321, 1111 atd.)

Čísla spojená s námi nebo blízkou osobou, jako je datum a rok narození (1102, 2009 apod.)



Zkus vymyslet z hlavy nějaké číselné kombinace, které se týkají tebe nebo tvých kamarádů.



Pokud se někdo cizí dostane ke tvému telefonu, pravděpodobně vyzkouší nejpoužívanější číselné kombinace. U čtyřmístného PIN můžeš vytvořit přibližně 10.000 různých kombinací, z nich je ale téměř 300 lehce uhodnutelných. Dobrá zpráva ale je, že se po několika neúspěšných pokusech telefon nebo SIM karta pro odemknutí zablokuje.

Někteří výrobci telefonů nastavují automaticky lehce zapamatovatelný PIN. Ten je dobré co nejdříve změnit na vlastní.



Kapitola 014 – Jak si zabezpečit telefon pomocí gest

Jednou z nejčastějších možností, kterou využíváme k zabezpečení telefonu, jsou speciální gesta. Telefon nebo tablet se odemkne, pokud správně vytvoříme na obrazovce symbol. Toto zabezpečení nepatří mezi nejsilnější.



Když už se rozhodneš používat gesta k odemykání displeje, zvaž další možnost zabezpečení. Ideální je kombinace gest a biometrických údajů.

Zkus si displej telefonu čas od času vyčistit. Mohou být na něm vidět stopy po gestech.



Já gesta nepoužívám, protože jsou slabá

A není to spíš tím, že by sis drápama poškrábal displej?



Kapitola 015 – Zabezpečení telefonu pomocí biometrických „hesel“

Jedná se o jednu z nejbezpečnějších metod, jakou si můžeš zabezpečit vlastní účet nebo zařízení. Technologie se navíc velmi rychle vyvíjí a je velmi obtížné ji obejít nebo prolomit. Na rozdíl od jiných ochran účtu tyto mají velkou výhodu. Nelze je zapomenout nebo ztratit.

Mezi nejčastější biometrické údaje, které slouží k zabezpečení účtu, patří:



A co když někdo k odemknutí použije místo skenu obličeje moji fotku?

To by možná šlo, máš docela placatý obličej



Nemusíš se bát, zařízení kontroluje, zda jde o trojrozměrný obraz



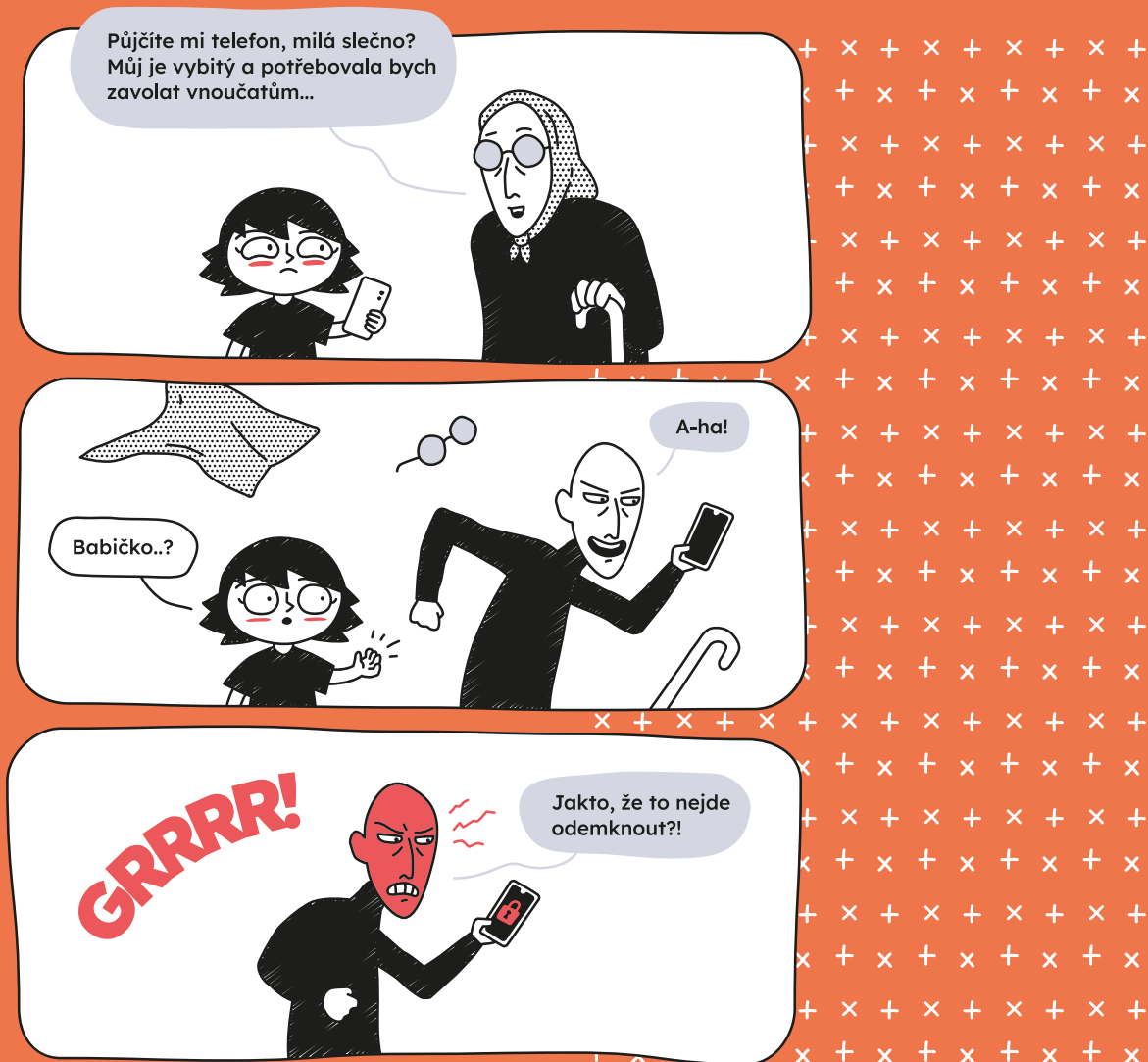
Já mám sice placatý obličej, ale mám na rozdíl od tebe prsty



Technologie odemykání pomocí otisku prstu není nová, ale významně se rozšířila až v roce 2013. Tehdy ji začala využívat společnost Apple ve svém telefonu iPhone 5S. Dnes je toto ověřování nejrozšířenější u telefonů se systémem Android. Otisky se neukládají nikde online, převedou se do digitálního klíče, který se pak předá příslušné aplikaci.

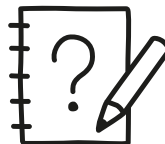
Kapitola 016 – Automatické uzamknutí displeje

Když svůj telefon používáš na veřejnosti, mysli na to, že ho máš odemčený. Pokud ti ho někdo vezme, může se dostat do něj a vlastně do všeho, co obsahuje. Zabránit se tomu dá jednoduše.





Chytré telefony mají funkci, která při jejich nepoužívání uzamkne displej. Když pak telefon vezmeš po nějaké době do ruky, musíš ho znovu odemknout. Dobu, než se telefon automaticky uzamkne, si můžeš nastavit. Od pár vteřin po minuty (nebo vůbec). Je to důležitá ochrana proti tomu, aby se cizí návštěvníci dostali do tvého telefonu.



Jaká je podle tebe ideální doba, než se telefon sám uzamkne?

- ✗ Jednotky vteřin
- ✗ 10 - 30 vteřin
- ✗ 30 vteřin - 1 minuta
- ✗ Nemusí se zamykat



Robote, ty se nezdáš, ty víš o těch telefonech dost věcí

Vrrrrr

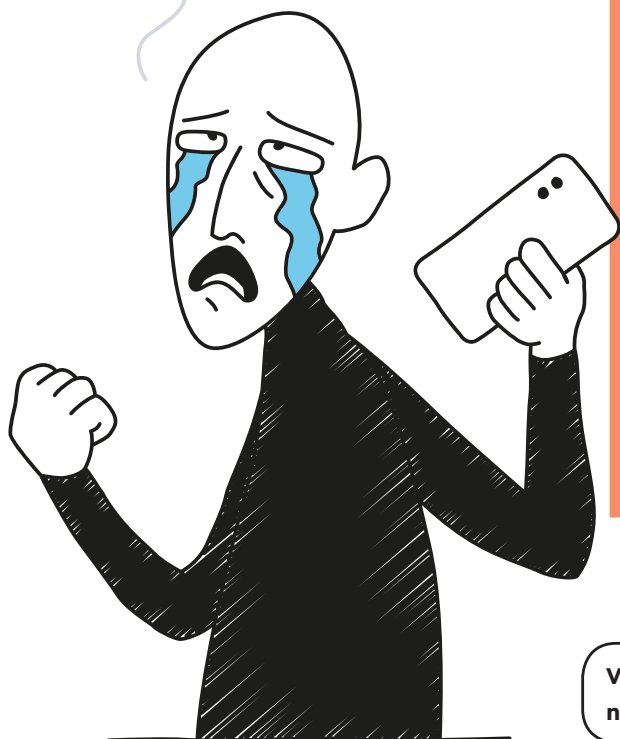
/Vrni jako plechová krabice/



Kapitola 017 – Co je IMEI a na co ho budu potřebovat

IMEI (International Mobile Equipment Identity) je unikátní patnáctimístné číslo mobilního telefonu, které mu přiděluje jeho výrobce. Toto číslo ukládá mobilní operátor do speciálního registru. Po nahlášení krádeže telefonu pak přístroj na základě tohoto čísla může operátor zablokovat.

Vyzkoušel jsem všechno!
Vyměnil jsem i SIM kartu,
ale telefon stále nefunguje!



Kde najdu IMEI

- × Na zadní straně telefonu nebo pod jeho baterií.
- × Na dokladu o jeho koupi.
- × Většina telefonů ho dokáže zobrazit na displeji.

Vyzkoušej si zadat v telefonu
následující kód: ***#06#**



Kapitola 018 – Co dělat, když mi ukradnou telefon

Krádež telefonu není příjemná situace. I pokud byl telefon hodně levný nebo starší, měli bychom jeho krádež oznámit. Důležité jsou dva kroky:

- 1] Obrát se na svého operátora, který zablokuje SIM kartu
- 2] Obrát se na Policii ČR, která zažádá operátory o zablokování telefonu podle jeho IMEI čísla



Na stránkách <https://aplikace.policie.cz/patrani-mobily/> podle čísla IMEI zjistíš, jestli byl telefon odcizen.

Na Policii ČR musíš vlastnictví telefonu prokázat:
Účtenkou, fakturou, záručním listem nebo krabicí s výrobním číslem IMEI.



Kapitola 019 – Co dělat, když dostanu nový telefon

Když vyměňujeme nový telefon za starý, nestačí jen vyměnit SIM kartu. Některá data v telefonu zůstávají.

Předtím, než vyměníš telefon:

- ✗ zazálohuj si veškeré údaje
- ✗ odhlas se ze všech účtů
- ✗ vymaž historii
- ✗ v nastavení telefonu vyhledej „Obnovení továrních dat“ nebo „Obnovení továrního nastavení“



Kapitola 020 – Zálohuj!

Fotky, videa, komunikace nebo uložené herní pozice mohou nenávratně zmizet, pokud nebudeš svoje zařízení zálohovat. Většina chytrých telefonů zálohuje automaticky na vzdálené úložiště (tzv. cloud).



Zkus vyjmenovat situace, za kterých můžeš přijít o data.
Nápovědu najdeš dole – poblíž čísla stránky.



Při zálohování dat se vyskytl problém.
Vaše kočičí fotky před zrcadlem zabírají
mnoho místa. Mám je smazat?

Smazat

Zachovat



Podívej se na internet a do vyhledávače si zadej frázi
„jak zálohovat telefon/mobil“. Existuje celá řada návodů pro
různé operační systémy nebo typy zařízení.

Kapitola 021 – Aktualizuj!

Můžeš mít sice nejmodernější telefon, ale pokud nebudeš pravidelně aktualizovat jeho systém nebo klíčové aplikace, stává se zranitelným.



Kvůli chybám v aplikacích či systému se mohou útočníci dostat k SMS, stáhnout si fotografie, zapnout mikrofon nebo sledovat tvoji polohu.



Aktualizace obsahují nejen vylepšení aplikací, ale záplatují i jejich bezpečnostní chyby

A většinou mi to pak změní vzhled



Zvykneš si jako na nové granule

Zapni si automatické aktualizace operačního systému ve svém telefonu. U jiných aplikací se vyplatí pár dní počkat.



Kapitola 022 – Mám mít antivir v telefonu?

Mobilní telefony s aktualizovaným operačním systémem Android nebo iOS jsou velmi dobře chráněny. Škodlivý software (více viz Kapitola číslo 039) se může dostat do telefonu několika způsoby. Nejčastěji přes neznámé aplikace z neoficiálních obchodů a pohybem na internetu.

Antivirový program by tedy měl určitě každý mít. Některé jsou zdarma, některé placené. Investice do nich se ale vyplatí.



Antivirových programů je celá řada. Vyzkoušet můžeš třeba tyto:

- Norton Mobile Security
- ESET Mobile Security
- Avast Mobile Security



Kapitola 023 – Jak poznat, že je telefon zavirovaný

Pokud je tvůj telefon napaden škodlivým kódem, může se chovat zvláštně. Předejít napadení telefonu můžeš antivirovým programem.

Některé známky možného napadení telefonu:

- ✗ Baterie telefonu se rychle vyčerpává
- ✗ Objevují se aplikace, jejichž stažení si nevybavuješ
- ✗ Vyskakují na tebe reklamy
- ✗ Aplikace se stále zavírají
- ✗ Telefon se často restartuje, zamrzá nebo přehřívá
- ✗ Tvoje data se velmi rychle vyčerpávají

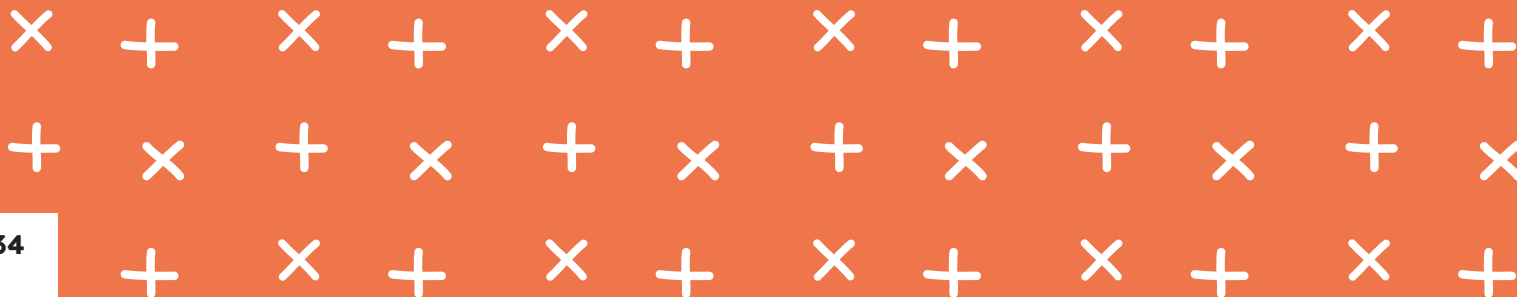


Pokud nepomůže antivir, můžeš telefon uvést do továrního nastavení nebo nebo nebo nebo...

Co se s ním stalo? Ted' nevím, jak to dopadne



Zamrzl. Jak ty v pubertě. Asi by chtěl odvézt do servisu.



Kapitola 024 – Instalace aplikací odjinud

Aplikace do telefonu si instaluj jen z oficiálních míst výrobce. Mezi největší patří Google Play, App Store, Microsoft Store nebo Samsung Galaxy Store.



Pokud si stahuješ aplikace z oficiálních a ověřených obchodů, je riziko, že bude tvůj telefon napaden škodlivým softwarem, malé. Obchody už jejich bezpečnost ověřují. Nikdo ale není neomylný.



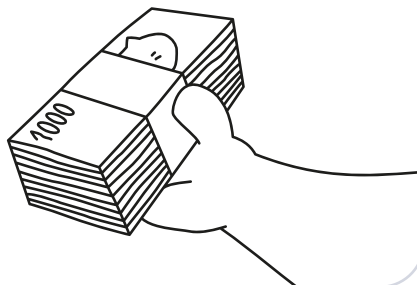
Kapitola 025 – Jaké aplikace si stáhnout

Do dnešních mobilních telefonů si můžeš i díky velké paměti nahrát stovky různých aplikací. Než si stáhneš aplikaci z obchodu, podívej se pozorně na několik věcí:



Vymyslel jsem super appku na detekci grilovaných buřtů v okolí

To je ale blbost xDD



Buřtoappka 9.000

1.000.000.000 stažení

- ✗ Vývojáři si mohou zaplatit reklamu na své aplikace. Nespoléhej na doporučení obchodu.
- ✗ Pročti recenze. Nejen ty s pěti hvězdičkami, ale i ty nejhorší. Můžeš zjistit, že aplikace není tak dobrá, jakou se na první pohled jeví.
- ✗ Pozorně se podívej na podmínky používání aplikace. Některé mohou sbírat více údajů, než je potřeba.
- ✗ Není Messenger jako Messenger. Některé aplikace se mohou jmenovat podobně nebo mít podobné logo. Zneužívají podobnost loga i názvu a mohou být i placené.
- ✗ Podívej se, kdy byla aplikace v obchodě naposledy aktualizována. Pokud to bylo před delší dobou, nestahuj ji. Nemusí být již bezpečná.



Potřebovala bych nějakou aplikaci s budíkem do školy

Šprtka, aby tam byla první...



Tahle vypadá super! Má tisíc vyzváněcích tónů!

A opravdu ta aplikace potřebuje znát tvoji polohu, mít přístup do tvé fotogalerie a k tvým hovorům nebo informaci o tvé Wi-Fi?



**Jen v App Store je téměř pět milionů aplikací,
z toho je zhruba půl milionu her. Každý den je přidáno tisíc
nových aplikací.**

Kapitola 026 – Placené aplikace

Velká část aplikací v obchodech je placená. Buď za ně zaplatíš jednorázově, nebo po nějaké době používání. Na to si dej pozor. Pročti si pozorně podmínky o předplatném. Některé aplikace se tváří, že jsou zadarmo, a po několika týdnech odhalíš nepříjemné překvapení.



Najdi si ve svém telefonu položku **Předplatné**. Obvykle se v telefonu nachází v položce **Nastavení**. Zde můžeš své platby za aplikace spravovat.



Čas od času se podívej, které aplikace nepoužíváš, a smaž je. Předtím z nich ale odstraň osobní informace, odhlas se ze všech účtů a vymaž historii.

Kapitola 027 – Výhody sdílení polohy přes aplikace

Některé aplikace potřebují ke své funkčnosti zapnutí lokalizace. Může jít o navigaci, aplikace s mapami, počasím nebo třeba Pokémon GO. Bez zapnuté lokalizace bude nejspíš aplikace nepřesná nebo nefunkční.

Výhody používání lokalizačních služeb v telefonu:

- Najít, kde jsme, když se ztratíme v přírodě či neznámém městě
- Najít nejbližší zastávku, bankomat...
- Sdílet s přáteli místa, která jsme navštívili

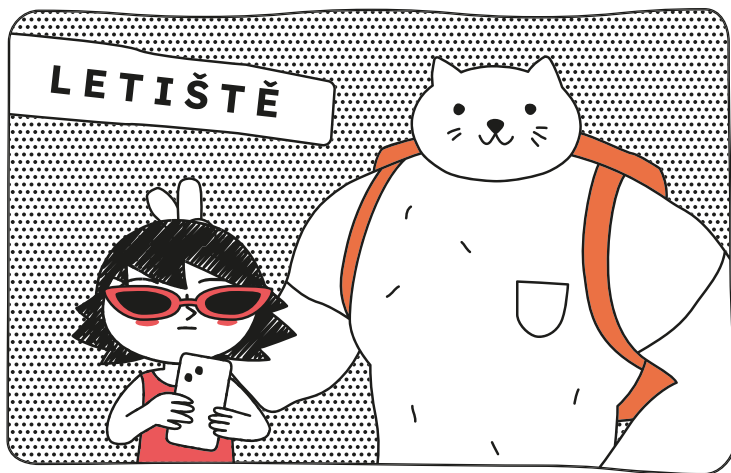


Kapitola 028 – Nevýhody sdílení polohy přes aplikace

Každá služba se dá zneužít. Zvaž proto, u jakých služeb je potřeba sdílet informace o tvém pohybu v místě a čase, ve kterém se nacházíš.



Někteří lidé si mohou na základě tvých sdílených informací dát dohromady, kde se nacházíš nebo jaká místa navštěvuješ nejčastěji. Zjistit lze, do jaké školy chodíš nebo kde bydlíš. Pak už je jednoduché tě dohledat.



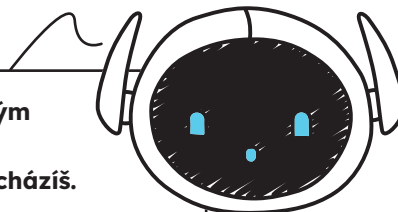
#dovolena #konecne
#nakonecsveta



nejsemzlodej_777


Večer si zajdu pro tvůj počítač

Na internet dávej fotografie nebo videa až s určitým časovým odstupem, když už na příslušném místě nejsi. Omez také sdílení fotek s označením polohy, na které se pravidelně nacházíš.




Kapitola 029 – Náhledy zpráv


Pokud na telefonu obdržíš zprávu, standardně to bývá tak, že se zobrazí její náhled. Někdy i v případech, pokud je obrazovka vypnutá. To se může jevit jako užitečná věc. Pokud však nejsi u svého telefonu, může si zprávu přečíst kdokoliv.




Kočkomáma
Granule máš v misce




Banka
Na účet Vám přišlo 50.000 Kč




Kočka
Miluju tě, ale Micině to neříkej!




MňauTube
Sleduj nové kočičí hot video!



Nastavení náhledů zpráv můžeš upravit.
V telefonu je tato volba umístěna většinou v položce „Oznámení“ nebo „Zprávy“.



Chat
Máte novou zprávu.



MňauTube
Nová notifikace!

Kapitola 030 – Premium SMS

Přes telefon si můžeš koupit jízdenku do MHD, hlasovat v soutěži, koupit balíčky do her nebo zaplatit drobné služby. Tyto SMS zprávy jsou zpoplatněny prémiovou cenou (Premium SMS), která může dosáhnout částky až 99 Kč. V některých případech až 999 Kč.

Prémiových SMS mohou zneužít různí podvodníci. Nejčastějším podvodem je takováto situace:

Ahoj, tady Pepa ze třídy, mám nový účet, jaké máš telefonní číslo?

xxx xxx xxx

90x856621246:
Kód: QWASD998465sd22

Pošleš mi prosím zprávu, co ti přišla?

**Přijít můžeš o tisíce.
Nikomu nesdílej kódy,
které ti přišly přes SMS!**

Podívej se na číslo zprávy. První část nám podle kódu říká, o jakou službu jde.

901 – Hlasování a soutěže

902 – Platby za zboží a služby

(jízdenky, přístup na Wi-Fi...)

903 – Aplikace, hry a kredity do nich

904 – Digitální obsah (loga, melodie, horoskopy...)

906 – Hlasování a soutěže

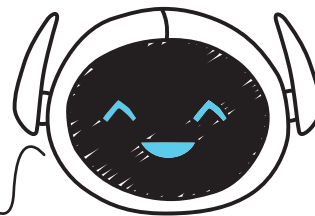
908 – Loterie

909 – Služby pro dospělé

87777 – Charita, darovanou částku si určujete sami

Poslední číslo značí cenu v Kč.

Premium SMS můžeš zakázat. Stačí, když zavoláš svému operátorovi nebo je zrušíš v jeho aplikaci.



Premium SMS ★

Horoskop na dnešek:
Dnes budete našťvaná

Z vašeho účtu bylo
strženo 99 Kč



Kapitola 031 – Smishing



Slovo **smishing** je kombinací slov SMS a phishing. Jde o podvod, kterým se z tebe útočník snaží dostat pomocí SMS zprávy údaje jako heslo, platební údaje ke kartě, PIN apod.

Jak poznat, že jde o podvodnou zprávu?

- ✗ SMS tě nabádá ke kliknutí na neznámý odkaz
- ✗ Odkaz bývá zkrácený
- ✗ Podvodníci se vydávají za známé společnosti (pošta, úřad nebo banka aj.)
- ✗ SMS obsahuje výzvu, vyvíjí časový nátlak nebo slibuje peníze
- ✗ Může občas obsahovat gramatické chyby



- ✗ Neklikejte na přiložené odkazy
- ✗ Zprávu smažte
- ✗ Když si nebudete jisti, zavolejte dané společnosti



Gratulujeme!!!!!!!

Vyhráváte 10.000 Kč! Pro vyzvednutí ceny klikněte na tento odkaz a zadejte číslo karty, abychom vám výhru mohli poslat na váš účet

Kapitola 032 – Jak se připojit bezpečně na Wi-Fi síť



Co je **Wi-Fi** – Pojem Wi-Fi (Wireless Fidelity) se označuje bezdrátové propojení koncových zařízení (počítač, tablet, chytrý telefon) k počítačové síti, která je lokální nebo internetová. Nejedná se tedy o připojení k internetu, jde o funkci, která přenáší signál.

Než se připojíš na Wi-Fi, podívej se na pár rad

- ✗ Do e-mailu, sociálních sítí nebo důležitých služeb se připojuj pouze přes aplikaci
- ✗ Používej zašifrované stránky, které poznáš podle toho, že před začátkem webové adresy obsahují HTTPS
- ✗ Dej si pozor na sítě, které se tváří jako „free“ nebo „public“
- ✗ U neznámých sítí si nenastavuj automatické připojení
- ✗ Věnuj pozornost varováním ze strany svého prohlížeče, antiviru nebo jiného bezpečnostního systému
- ✗ Při používání Wi-Fi používej VPN (viz kapitola 035), ta zašifruje přenos dat a nikdo cizí tvoji komunikaci nerozluští



Útočník může přes router, který šíří veřejnou Wi-Fi, sledovat všechna připojená zařízení.

Za chvíli mi začíná CatBowl, a já u toho nebudu!



Kapitola 033 – Omez používání telefonu před spaním

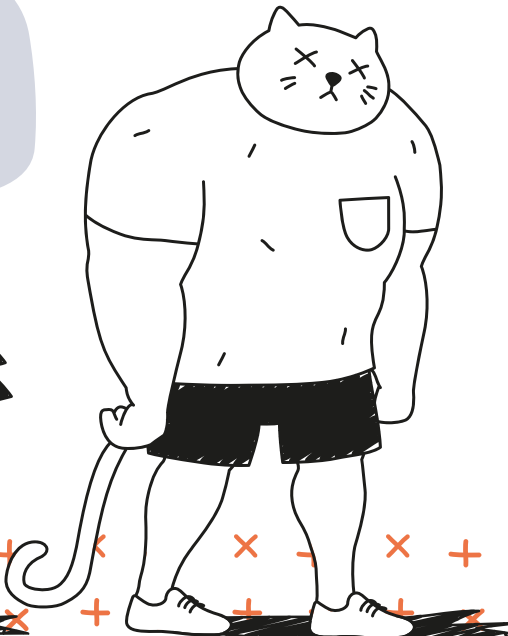
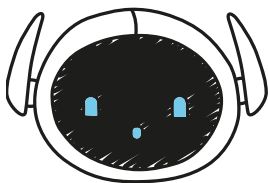
Používáš mobil, tablet nebo počítač před spaním? A víš, co je to tzv. modré světlo? Modré světlo je všude okolo nás, jedná se o jednu ze složek slunečního světla. Díky němu dokáže náš organismus rozpoznat, jestli je den, nebo noc. Pokud se vystavuješ nepřirozenému modrému světlu v noci, tvoje tělo přestává produkovat hormon melatonin, což ovlivňuje kvalitu spánku, nebo se ti může hůře usínat.



Melatonin – Spánkový hormon

V těle se začíná produkovat po západu slunce. Když ale trávíš čas před spaním koukáním do telefonu, do počítače nebo na televizi, tvůj organismus si myslí, že je stále den.

Únavě, nevyspání nebo častému probouzení v noci se můžeš vyhnout tak, že odložíš telefon aspoň hodinu předtím, než půjdeš spát.



Kapitola 034 – Bluetooth



Bluetooth je bezdrátová technologie pro výměnu dat mezi blízkými zařízeními. V závislosti na podmínkách má dosah zhruba deset až padesát metrů a jde o relativně bezpečnou technologii. Zařízení mění frekvenci až stokrát za vteřinu, aby se bránila hackerským útokům.



Proč se tomu říká Bluetooth? Vždyť to žádné zuby nemá

Zuby, zahnutý nahoru...



Název Bluetooth je odvozen od jména dánského krále Haralda Bluetootha (Modrozuba), který vládl v 10. století a oplýval výbornými diplomatickými schopnostmi. Tato technologie, podobně jako kdysi král Harald, usnadňuje vzájemnou komunikaci, proto po něm byla na jeho počest pojmenována. Znak Bluetooth vznikl spojením runových znaků pro písmena H a B.

I když je technologie Bluetooth relativně bezpečná, dodržuj pár zásad:

- Při návštěvě přeplněných míst měj Bluetooth vypnutý
- Aby byl proveden útok přes Bluetooth, musí být útočník poblíž. Hlídej si proto své okolí
- Nastav si na svém zařízení režim „Skryté“ místo režimu „Zjistitelné“
- Připojené zařízení by mělo být pravidelně aktualizováno



Kapitola 035 – VPN

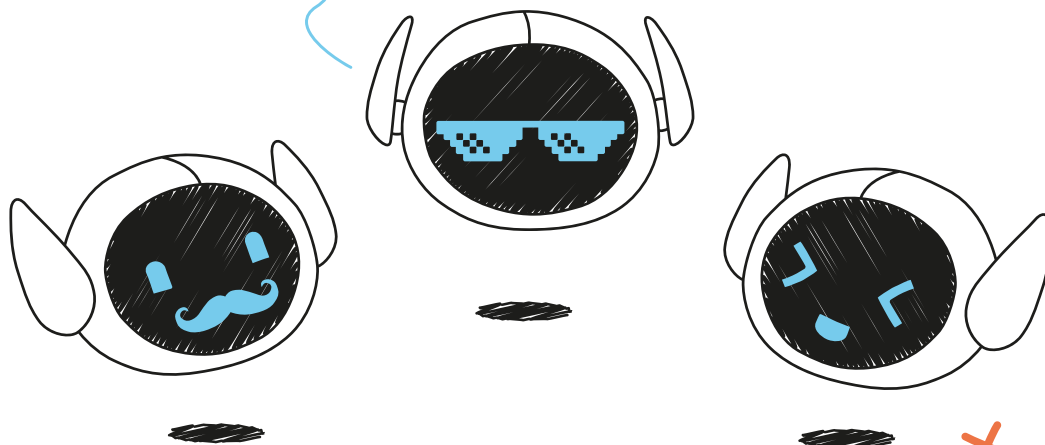


VPN – Virtual Private Network (virtuální privátní síť). Jde o službu, která umožňuje prohlížet internet v soukromí. Při připojování k veřejným sítím Wi-Fi vytváří zašifrované spojení. Zůstaneš tak v anonymitě, schováš svoji IP adresu a nikdo se nedostane k tvoji komunikaci.

Další výhody používání VPN:

- V zahraničí se můžeš podívat na české streamovací služby, které jsou jinak blokovány
- Některé instituce (školy, knihovny, úřady) mají zablokované určité stránky. Třeba sociální sítě nebo YouTube. Přes VPN se na ně ale dostaneš
- VPN tě ochrání před sledováním. Sledovat tě mohou hackeři, podvodníci nebo tvůj operátor

Nevýhodou naopak může být pomalejší připojení nebo to, že jde většinou o placenou službu.



Část 3

Internetové prohlížeče a vyhledávače

Kapitola 036 – Co je internetový prohlížeč

Internetový prohlížeč (nebo také browser) je téměř nejdůležitější program v počítači nebo telefonu. Díváš se jeho prostřednictvím na internetové stránky, zobrazuje texty, obrázky nebo videa.

Obsah jako jsou obrázky, videa nebo texty se po internetu přenášejí pomocí protokolu Hypertext Transfer Protocol.



Já mám Chrome, má ho každý kocour v naší třídě! A taky více než 2,5 miliardy lidí po celém světě! (cítí se nad věcí)

Kocoure, a víš, že nejpoužívanější neznamená automaticky nejbezpečnější?



Nedávný výzkum označil za nejvíce bezpečné v systému Windows prohlížeče Mozilla Firefox, Microsoft Edge a Opera.



Prvním prohlížečem na světě byl WorldWideWeb, který vznikl koncem roku 1990. Aby jeho název nebyl zaměňován s World Wide Webem (WWW), byl později přejmenován na Nexus.

Kapitola 037 – Cookies

Cookies jsou krátké textové soubory vytvářené webovým serverem, které se ukládají ve tvém prohlížeči. Cookies zaznamenávají informace o tvé návštěvě, uchovávají vyplněné formuláře, pamatují si tvoje poslední vyhledávání nebo ovlivňují, jaká reklama se ti bude zobrazovat. Mohou ti usnadnit pohyb na internetu.

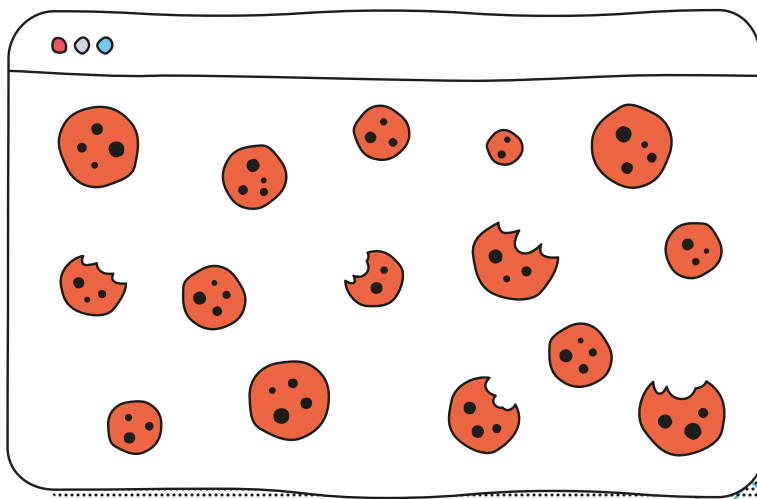


Proč se to jmenuje cookies? To dostanu za prohlížení webu nějakou sušenku?

To bys pak byl na internetu pořád a byl bys jako koule



V anglosaských zemích dávají hostům při návštěvě sušenky (cookies), aby se cítili lépe a aby byla navozena příjemná atmosféra. Takové “sušenky” dostáváte i vy jako návštěvníci webu



Kapitola 038 – Anonymní okna a historie

Cookies nám sice mohou usnadnit pohyb na internetu nebo ušetřit čas, sbírají však celou řadu údajů. Pokud používáš internet ve škole nebo na jiném zařízení, mohou se k tvým dříve používaným, vyhledávaným nebo uloženým informacím dostat cizí lidé.



Využij anonymní okno v prohlížeči

Anonymním prohlížením procházíš internet bez ukládání informací o navštívených stránkách a svého chování na nich.

Vymaž historii prohlížení

V prohlížeči můžeš vymazat historii prohlížení. Tuto možnost najdeš většinou v Nastavení pod položkou Historie nebo prostřednictvím klávesové zkratky Ctrl+H. Vymazat se dá celá historie nebo i jen určité období. Při dalším spuštění se budou cookies opět ukládat.



Pokud smažeš historii a s ní soubory cookies, odhlásí tě to z webů a tvoje uložená nastavení budou smazána.

Kapitola 039 – Viry

Některé webové stránky nebo aplikace mohou obsahovat škodlivý program. Jde o malware, toto slovo vzniklo složením dvou slov (malicious, což znamená škodlivý, a software). Do tvého zařízení se nejčastěji viry dostávají přes prohlížeč, například tím, že otevřeš zavirovanou přílohu e-mailu nebo odkaz vedoucí na infikovanou stránku.

Počítačových virů je mnoho, podívej se na ty nejčastější:



Spyware

Je to takový špión. Tajně slídí a sbírá informace, které pak posílá útočníkovi. Nejčastěji na něj narazíš při stahování a instalaci programů či her z neověřených zdrojů.



Trojský kůň (Trojan)

Funguje na principu trojského koně známého ze starověkých bájí. Útočníci škodlivý kód různě maskují a zakrývají jeho skutečnou funkci.



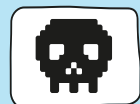
Adware

Bez souhlasu zobrazuje internetové reklamy nebo obsah ve vyskakovacích oknech.



Cryptojacking

Útočník využívá tvoje zařízení (počítač, mobil, tablet) k tomu, aby na něm neoprávněně těžil kryptoměny.



Ransomware

Je kombinací dvou slov – ransom (výkupné) a software. Zablokuje ti zařízení a nutí tě zaplatit výkupné.



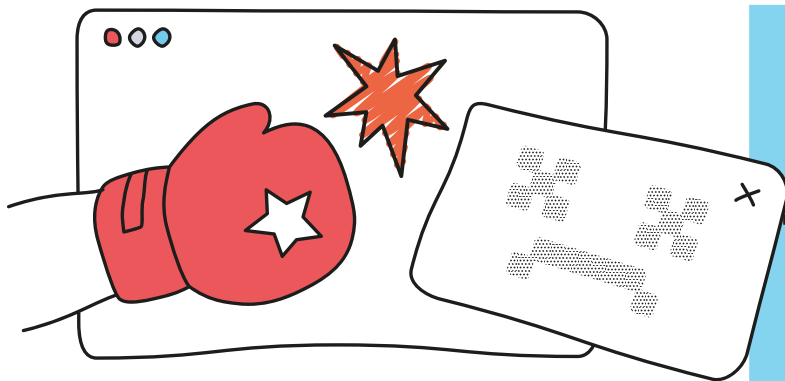
Antivir mi píše, že mě napadl počítačový červ

Tak jdi na veterinu



Jak odhalit virus v počítači nebo na mobilním telefonu?

- Tvoje zařízení je pomalé jak hlemýžď
- Vyskakují na tebe nevyžádaná okna
- Rychle ti dochází místo na disku
- Operační systém, programy nebo aplikace často „padají“ nebo se restartuje zařízení
- Začíná ti chodit velké množství spamu
- Antivir nefunguje nebo ti nejde zapnout
- Tvoje zařízení jede na plné obrátky, a přitom nic neděláš



**Přidej si do prohlížeče
rozšíření blokující
vyskakovací okna nebo
zobrazování reklam.**

Kapitola 040 – SPAM

SPAM jsou nevyžádané hromadné zprávy. Může jít o reklamní sdělení, SMS, e-maily nebo zprávy zobrazované na velkém počtu míst.

Internetovou sítí proudí miliony zpráv za vteřinu. Drtivá většina z nich je nevyžádaných. Téměř všechny odstraní ještě před doručením velké firmy (Google, Seznam, Meta...). Pokud se k tobě nějaká zpráva (spam) dostane, zprávu ani přílohy neotvírej, případně neklikej na odkazy, které jsou v ní umístěné.



Právě mi napsali, že jsem vyhrál v loterii 200 miliónů \$

Já jsem dostala zprávu, že se naučím anglicky přes noc, když si koupím speciální helmu...

A já zase můžu zhubnout 30 kilo za týden!



E-maily mohou obsahovat možnost „Odhlášení odběru“. Pokud odesílatele neznáš, na tento odkaz neklikej. Jen tím útočníkům říkáš, že je tvůj e-mail aktivní, a spamu ti bude chodit více.

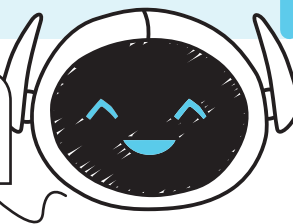
Kapitola 041 – Phishing

Anglické slovo fishing znamená rybaření nebo rybolov, phishing je označení pro rozesílání „návnady“ v naději, že „se chytí“ některé oběti. Jde o podvodnou techniku, při které se z tebe bude někdo pokoušet vymámit osobní nebo citlivé údaje (hesla, číslo kreditní karty aj.). Podvodník se vydává za známé služby, organizace nebo jednotlivce.

Jak poznat phishing

- Špatná gramatika, zpráva může obsahovat špatnou češtinu
- Výhodná nabídka (dědictví, výhra v loterii, zboží zadarmo, balík na poště...)
- Divná adresa může obsahovat překlepy (např. místo seznam.cz je „saznam.cz“), kterých si na první pohled nemusíš všimnout
- Naléhavost (nutí tě udělat něco rychle, nedávají ti čas na rozmyšlenou)
- Chtějí osobní nebo citlivé údaje (žádná banka ani jiná instituce je nevyžaduje přes e-mail nebo zprávy)

Najed' myši na odkaz, na který máš kliknout, ale neklikej na něj.
Objeví se ti náhled adresy, na kterou odkaz povede.



Některé phishingové stránky vypadají úplně stejně jako ty pravé. Poznáš je jen podle URL adresy.

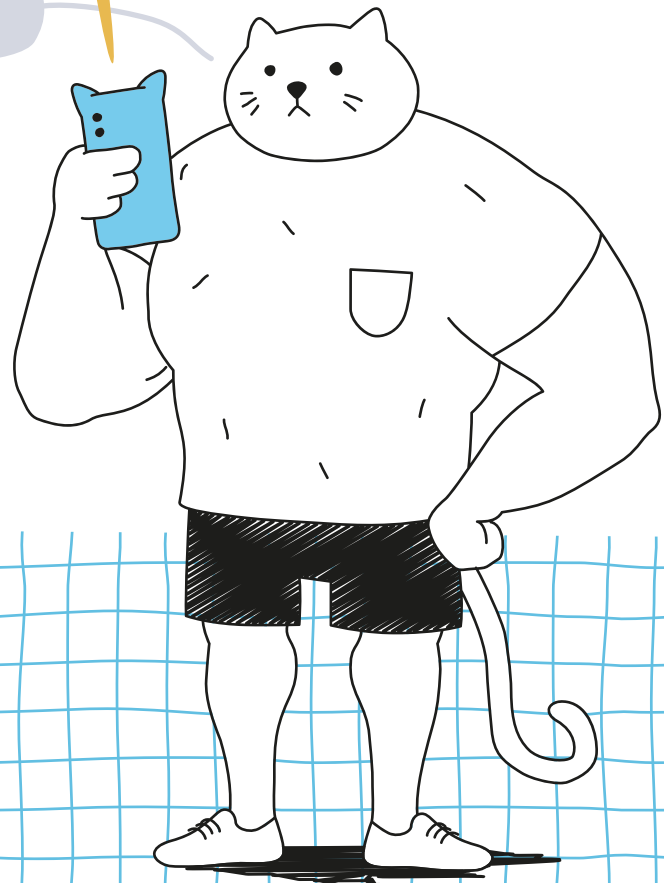
Ověř si v adresní řádce prohlížeče, že je doména správná.

Antivirový program nebo prohlížeč tě mohou upozornit, že se jedná o podvod. Neber toto upozornění na lehkou váhu.

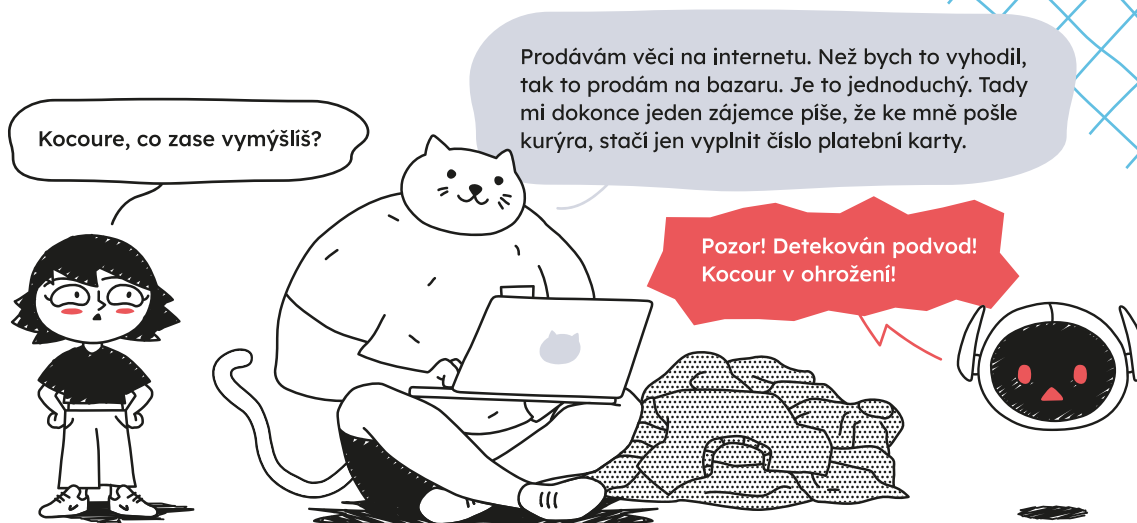
Dobrý den, tady pošta.
Dorazil ti balík, pro více
informací klikni zde:
www.xyzpost.zy/18kp96wwq

Ale já žádný nečekám... To bude
asi překvapení od Miciny...

To pravé překvapení tě čeká,
až na to klikneš.



Kapitola 042 – Prodávám. A nenaletím



Jak vypadá nejběžnější podvod?

- Vystaviš zboží na internetu
- Ozve se ti zájemce a zeptá se, zda je stále k dispozici
- Nabídne ti, že zaplatí přepravní službu, která si pro zboží dojede
- Podvodník ale bude chtít, abys vyplnil údaje na stránkách přepravce
- Stránky přepravce budou působit věrohodně, ale mají divnou www adresu
- Tam se po tobě bude chtít i vyplnění platební karty
- Než se naděješ, přijdeš o všechny peníze na účtu

Totéž platí, pokud budeš zboží chtít od někoho koupit!



Pokud budeš prodávat věci na internetu, nikdy nevkládej údaje z platební karty.

Kapitola 043 – Hoax

Název hoax (čti houks) v překladu znamená falešná zpráva, výmysl, mystifikace, novinářská kachna nebo poplašná zpráva. Cílem hoaxu je tě zaujmout, vystrašit, vyvolat paniku a donutit tě k nějaké reakci. Zpráva tě například bude varovat před vymyšleným nebezpečím. Některé hoaxy ale vznikají proto, aby tebe nebo jiné uživatele internetu pobavily.

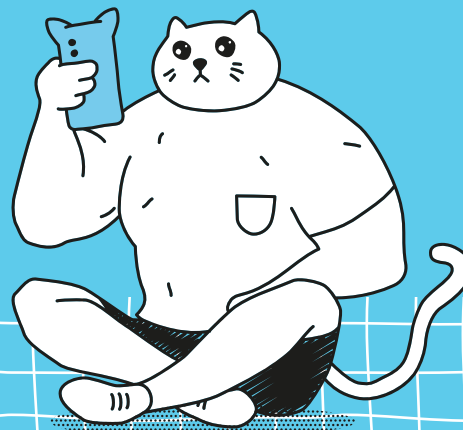
Když nepodepíšu petici,
tak nám budou ve škole
vařit jen mrkev!

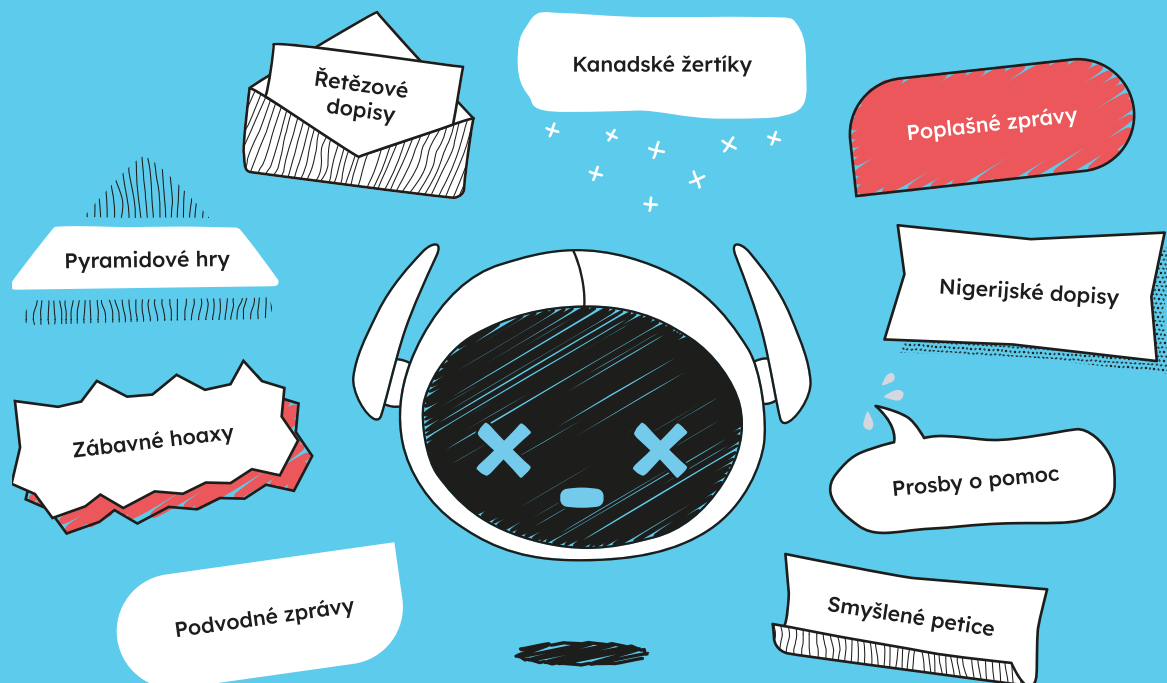


Když tuto zprávu nepřepeču
do pěti minut, zrezne mi
procesor!



Tady čtu, že nám Evropská
unie chce zakázat písmeno Ř!





Hoaxy nikdy nepřeposílej dál! S přeposláním informace můžeš sdílet svoje nebo i cizí údaje (např. e-mail).



Nevěř všem informacím, které nalezneš na internetu. Zkus si všechny informace ověřovat z více zdrojů (v knihovně, na Wikipedii nebo přes specializované stránky). Mezi stránky, které vyvracejí hoaxy, patří www.hoax.cz nebo www.manipulatori.cz.

Kapitola 044 – Doplnky do prohlížeče (Pluginy)

Do svého prohlížeče si můžeš stáhnout programy, které jim přidají nové funkce. Stáhnout se dají z oficiálních webů prohlížečů. Mohou pomoci s blokováním reklamy, s překladem stránky nebo usnadnit práci s obsahem.



Stejně jako u aplikací v mobilu si můžeš stáhnout nepřeberné množství pluginů. Pluginy potřebují ke své práci paměť. Když jich budeš mít mnoho, prohlížeč se zpomalí.

Kapitola 045 – Clickbait



Clickbait – pochází ze slov click (kliknutí) a bait (návnada), tedy návnada na kliknutí. Většinou jde o poutavý titulek zprávy, který nás nutí na ni kliknout. Dost často ale v obsahu článku senzaci nenajdeš.

10 zaručených tipů,
jak se zbavit akné

ŠOK NA VEČÍRKU!
MICINA MÁ NOVÉHO PŘÍTELE

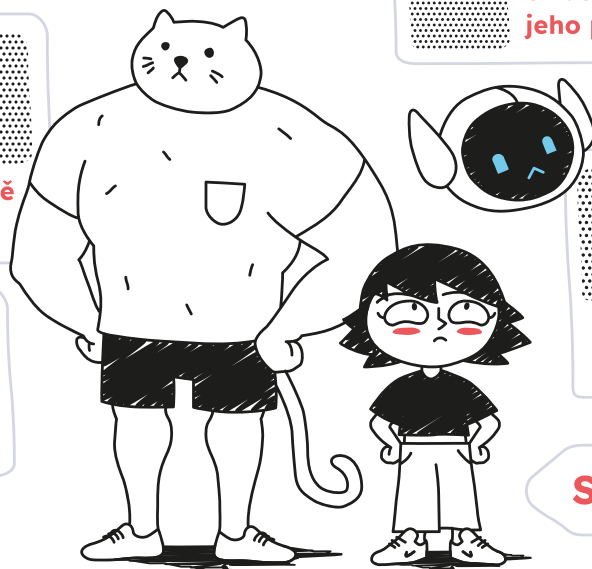
Strašné! Podívejte se na
jeho poslední fotky

Tento recept si určitě
zamilujete

VELKÁ SOUTĚŽ O
1.000
NOVÝCH IPHONŮ

TO JSTE JEŠTĚ
NEVIDĚLI...

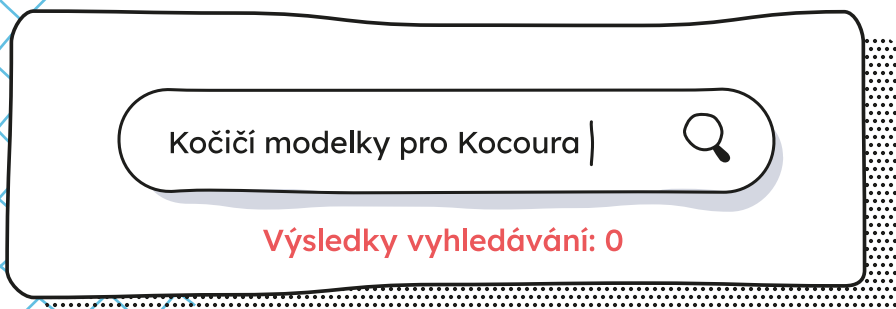
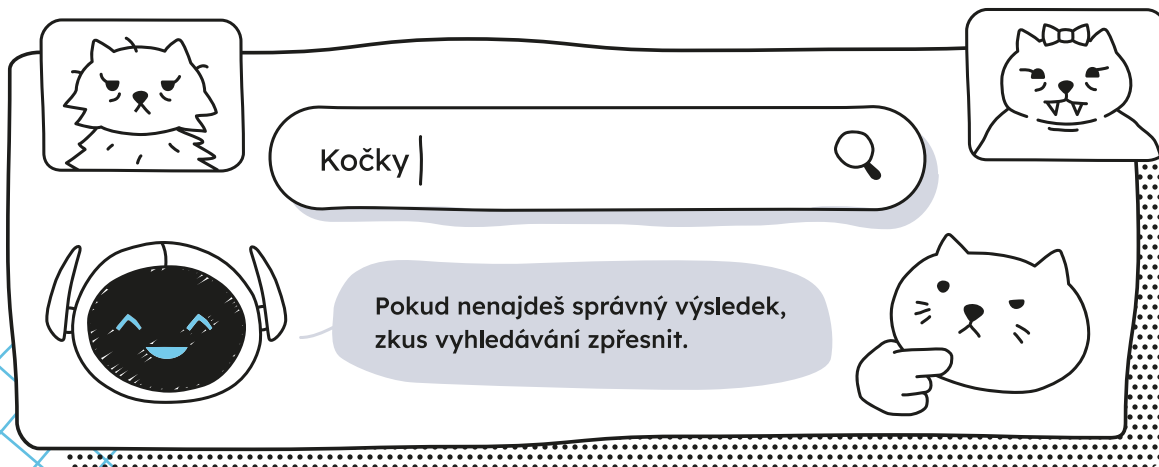
SLEVA 90 %



Stránky tě mohou nalákat na zajímavý titulek. Stránka ale slibovaný obsah nebude obsahovat, jen se ti bude zobrazovat velké množství reklamy. Čím déle se budeš pohybovat na stránce s reklamou, tím více si podvodník vydělá peněz.

Kapitola 046 – Vyhledávače

Internetový vyhledávač je služba, která ti umožní vyhledávat na internetu informace. Nemusíš si pamatovat přesnou adresu stránek, stačí zadat slovo, frázi či nějaký dotaz a vyhledávač ti nabídne nejvhodnější výsledky svého pátrání na internetu.



Vyhledávače prohledávají internet pomocí důmyslných algoritmů. Každý vyhledávač je má jiné, můžeš se tedy potkat s tím, že ti různé vyhledávače nabídnou jiné výsledky.





Na prvních místech vyhledaných výsledků nemusí být stránka, kterou hledáš. Mohou se ti zobrazovat reklamní sdělení. Zkus se podívat i na další stránky výsledků.



Mezi největší vyhledávače v Česku patří Google, Seznam nebo Bing. V některých nedemokratických zemích jsou služby úplně zakázané a zobrazují jiné výsledky. Tipneš si, o jaké země jde?

Nápověda: https://cs.wikipedia.org/wiki/Cenzura_na_internetu

Schválně, co najdu na internetu o Kocourovi...



Kocour
muž

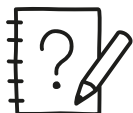
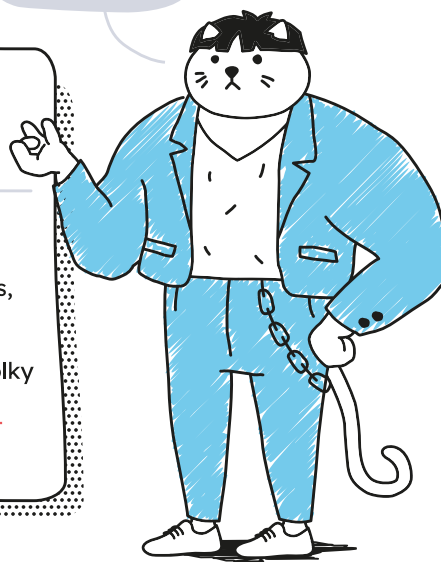
Stav: Single

Koníčky: Gaming, Fitness,
Lezení po stromech

Oblíbení jídlo: Lososové rolky

Životní sen: Chce se stát
slavným zpěvákem

...No a co?



Pokud na internetu sdílíš veřejný obsah (informace, fotografie, příspěvky...), bude si ho internet až do jeho smazání pamatovat. Obsah vytváříme nejen my, ale i kamarádi nebo cizí lidé. Dej do vyhledávače své jméno a podívej se, co se o sobě dozvíš. Více si povíme v kapitole 048 - Digitální stopa.

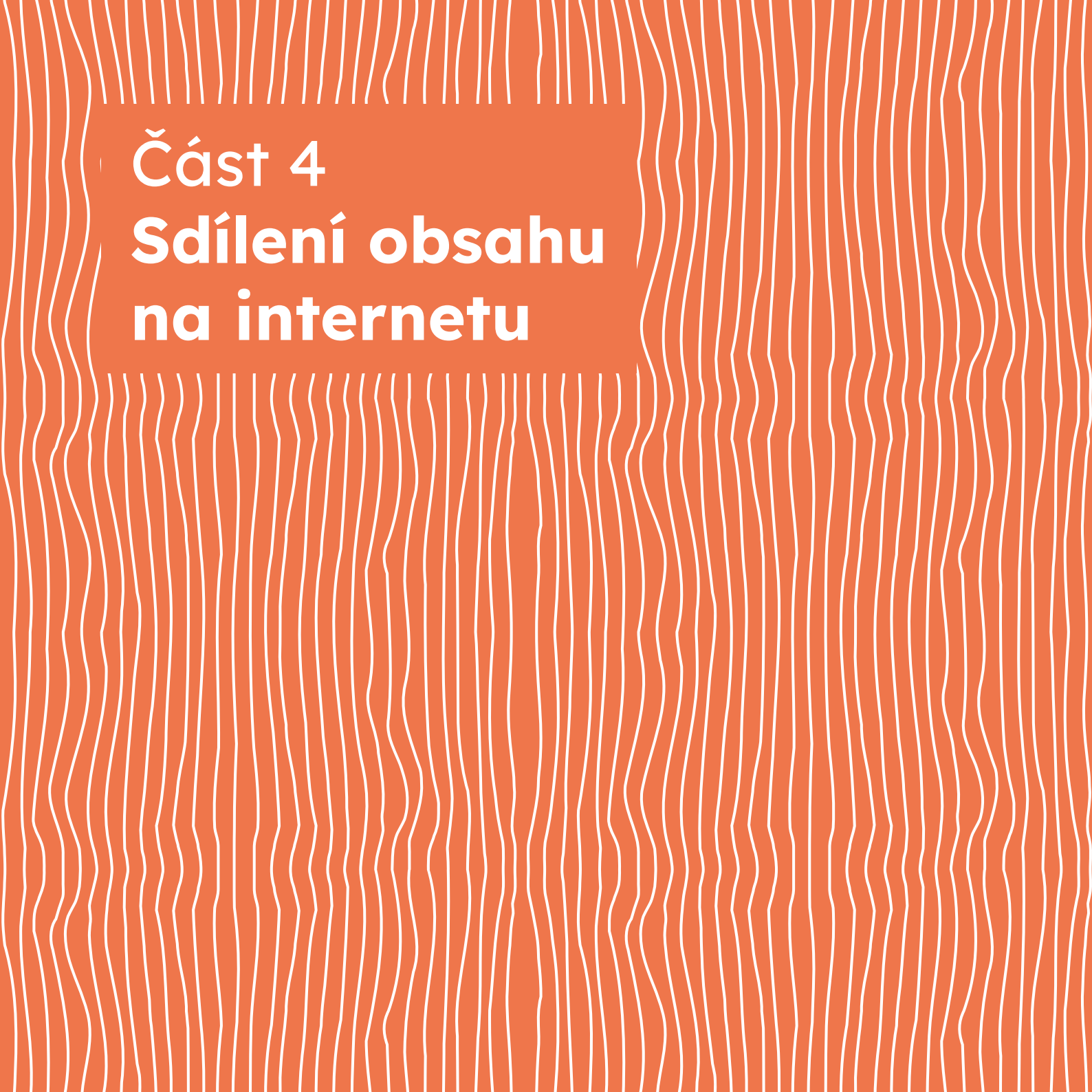
Kapitola 047 – Vyhledávání obrázků, článků nebo videí

Vyhledávače dokážou najít na internetu nejen textové informace, ale i obrázky či videa nebo zobrazují zprávy s hledaným výrazem. Vyhledávat můžeš nejen pomocí textových frází, ale i pomocí nahraného obrázku.



Máš nějakého oblíbeného streamera, herce, zpěváka nebo jinou známou osobnost? Zkus zadat jeho jméno do vyhledávače a najdi o něm informace, obrázek, video nebo novinový článek.

Mezi nejoblíbenější vyhledávače obrázků u nás patří Google Lens, Tineye, Seznam nebo Pinterest.

The background of the slide is a solid orange color with a pattern of thin, white, vertical wavy lines that create a textured, wood-grain-like effect.

Část 4

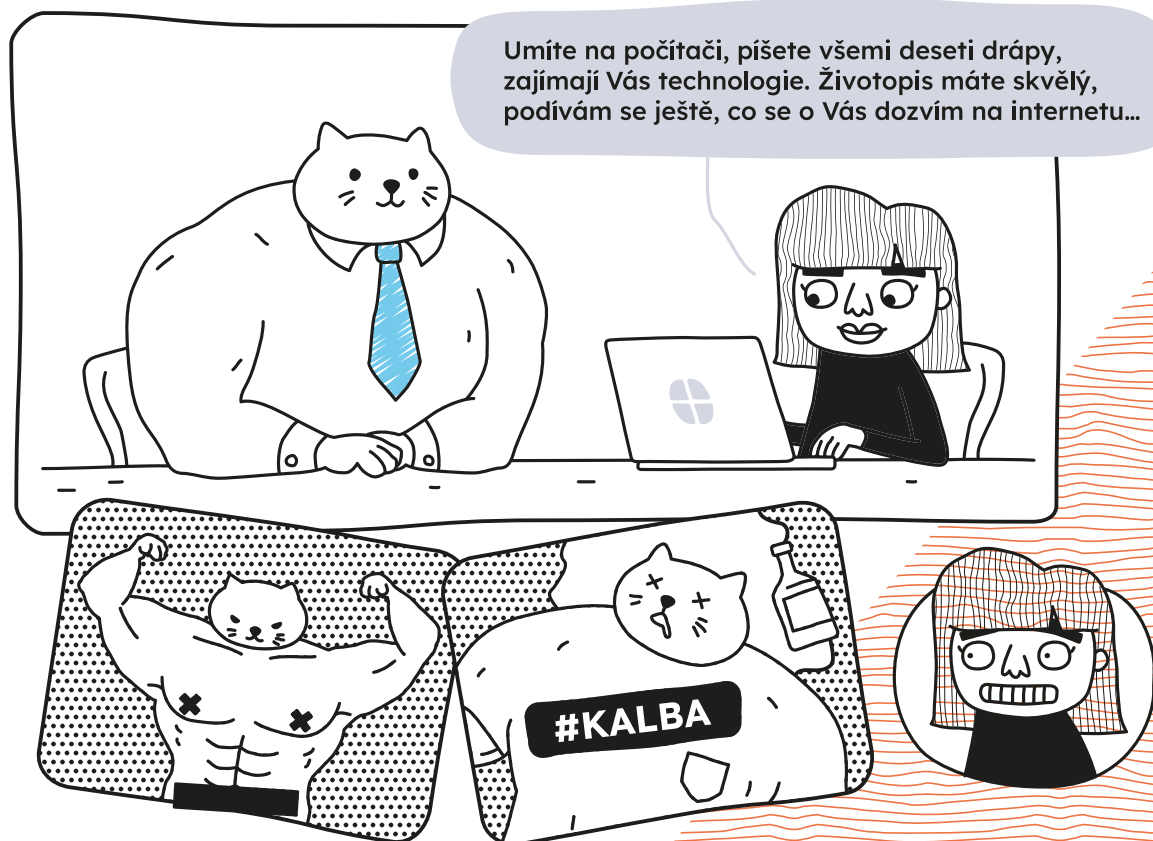
Sdílení obsahu na internetu

Kapitola 048 – Digitální stopa

Pohybem na internetu za sebou zanecháváme „drobečky“, informace, které nazýváme digitální stopou. Digitální stopu vytváříš nejen ty, ale i tví kamarádi, rodina nebo cizí lidé. Ukážeme ti, jak tě v budoucnu může tvoje digitální stopa dostihnout.

Životopis

Společnosti, u kterých se jednou budeš ucházet o zaměstnání, si ověřují informace nejen ze životopisu, ale i z tvé digitální stopy.



Nečekaná návštěva

Pokud budeš neuváženě zveřejňovat informace, může si někdo dát jedna a jedna dohromady



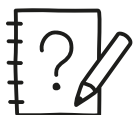
Digitální stopy jsou i technického charakteru. Může jít o cookies, IP adresu, metadata z fotografií, „lajky“ nebo geolokaci apod. Tyto informace mohou sbírat provozovatelé služeb a díky nim na tebe cílit reklamu „na míru“.



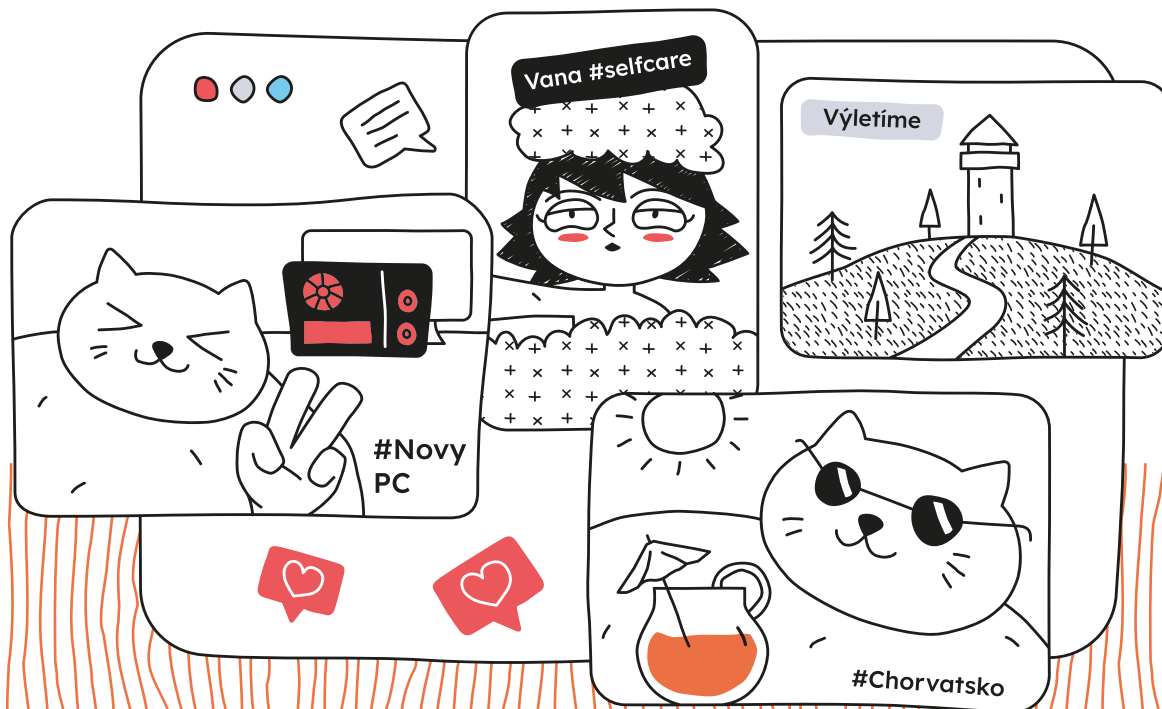
Svou digitální stopu nemůžeš úplně vymazat, zkus se tedy zamyslet, zda ti některé informace, které sdílíš, nemohou v budoucnu ublížit.

Kapitola 049 – Jaký obsah sdílet?

Říká se, dvakrát měř, jednou řež. Obsah, který nahraješ na internet, si může nejen kdokoliv prohlédnout, ale i stáhnout a šířit dál. Internetem pak po celém světě mohou kolovat desítky nebo stovky kopií. Když se později rozhodneš všechny kopie vymazat, bude to téměř nemožné.



Podívej se na obrázky a zamysli se, zda by jejich sdílení na internetu mohlo být pro tebe nebo tvé okolí nějak rizikové. Zkus také vymyslet proč.



Kapitola 050 – Co můžeš sdílet

Telefonem si můžeš nejen zavolat, ale také vytvářet fotografie nebo videa, to už víš. Víš ale, jaký obsah můžeš sdílet na internetu? Fotografování, natáčení videí a sdílení má svá omezení.

§ Zákon říká:

„Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.”



Fotografovat a natáčet můžeš osoby jen s jejich souhlasem. Výjimkou jsou fotografie nebo videa vytvořené tak, že se dotyční lidé nedají identifikovat. Třeba ze zadu tak, že jim nelze vidět do obličeje, nebo se jedná o skupinu osob například na náměstí, stadionu apod.

Svolení nepotřebuješ, pokud fotografii nebo video vytváříš pro **úřední výkon** nebo ve **veřejném zájmu**. Například si natočíš autonehodu, vyfotografuješ zloděje, podvodníka apod.

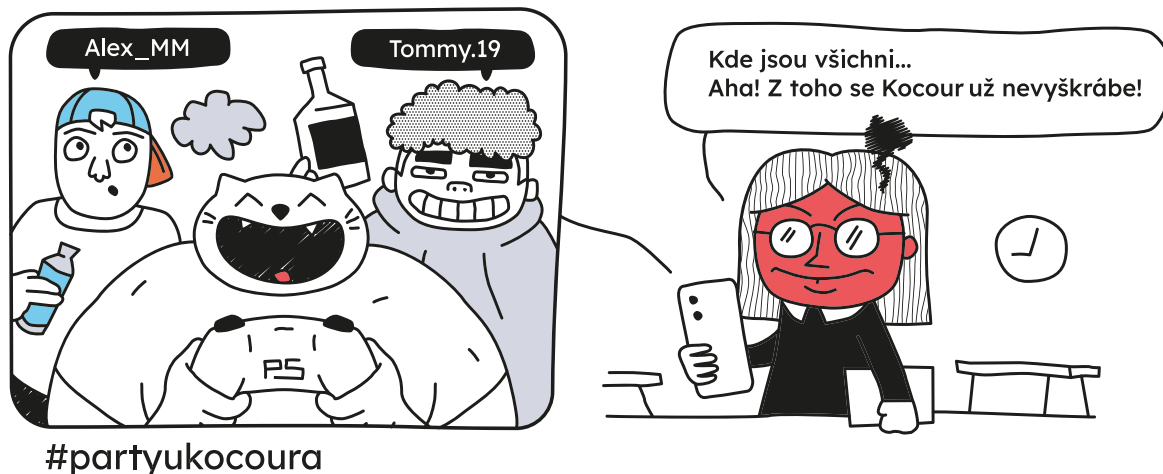
Pokud budeš používat nějaké obrázky z internetu, ověř si, zda je můžeš šířit. Například služba Google Obrázky ti nabízí možnost si zvolit v Nástrojích, Práva k užití: Licence Creative Commons.



Bez souhlasu nesmíš fotografovat, natáčet ani streamovat svého učitele. Totéž platí, pokud jsi u někoho na návštěvě. Zakázáno je také natáčet filmy v kině.

Kapitola 051 – Označování uživatelů

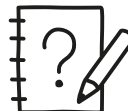
K příspěvkům na internetu můžeš přidat nejen místo, kde vznikly, ale také můžeš označit osoby, které se na nich nacházejí. Co když ale nechceš, aby tě na fotografii někdo poznal? Podívej se na následující situaci.



Obsah, kde je zobrazeno něco zajímavého, se může velice rychle šířit a stát se virálním. Pokud ho odstraníš, není zaručeno, že si již někdo nevytvořil kopii. Časem se fotografie nebo video může někde objevit a způsobit ti nepříjemnosti.



Označování si můžeš na sociálních sítích vypnout.



Zkusíš vymyslet nějaké situace, které tě mohou přivést do problémů?

Kapitola 052 – Nikdy bez oblečení!

Jedna z věcí, která ti může na internetu opravdu hodně ublížit, je zveřejňování citlivého, intimního obsahu. Nikdy nemáš jistotu, že ten, komu pošleš tyto materiály, si je nechá jen pro sebe.



Pokud se dostaneš kvůli citlivému nebo intimnímu obsahu do úzkých, neboj se svěřit. I když může situace vypadat složitě, vždy je nějaké řešení.

Pomoci ti mohou tyto služby:

- **Linka bezpečí** – zavolej na bezplatné číslo 116 111 (kdykoli) nebo chatuj na www.linkabezpeci.cz
- **Hotlinka STOPonline.cz** – zde můžeš anonymně nahlásit závadný obsah, který hotlinka rychle odstraní
- **Linka důvěry** – svěř se se svým problémem, www.ditekrize.cz, Rizika kyberprostoru (telefon 778 510 510)

Kapitola 053 – Streamování

Kdo by nechtěl ve svém životě něco dokázat nebo získat slávu? V tom skutečném světě to stojí spousty dřiny a úsilí. V tom virtuálním jen pár kliků. Ale je to opravdu tak jednoduché?

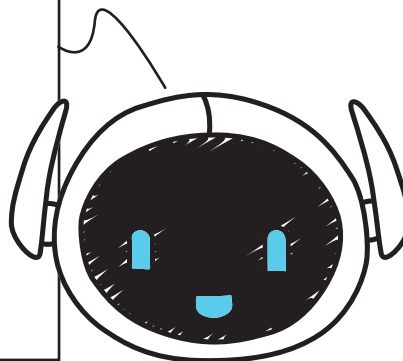


Když na sebe na live streamu vyleju jogurt, budu slavná?

Ne, jen budeš chvílku virálně kolovat internetem



- Neukazuj místo, kde bydlíš, a nesděluj své osobní údaje
- Pokud chceš používat obsah, který ti nepatří, požádej nej dřív o souhlas autora
- Slušnost nebolí - slávu nezískáš vulgaritami
- Nedělej nic, za co se budeš v budoucnu stydět
- Vše, co pustíš do světa, tam zůstane, tak na to pamatuj



Připrav se na to, že ne každému se tvoje tvorba bude líbit. Mohou tě „hejtit“ zcela neznámí lidé. Na urážlivé, negativní nebo výhrůžné zprávy nereaguj.



Máš nějakého oblíbeného streamera?

Kapitola 054 – Nebud'te lhostejní

Pokud na internetu narazíš na obsah, který se ti nelíbí, někomu ubližuje, nebo si myslíš, že by to na internetu nemělo být, nenech si to pro sebe s tím, že to třeba nahlásí někdo jiný. Tím, že se někomu svěříš nebo závadný obsah nahlásiš, můžeš i někoho zachránit.

Jak řešit nevhodný obsah

- Předtím, než začneš situaci řešit, si vytvoř důkaz. Tím může být screenshot, vytisknutá stránka, nesmazané zprávy nebo SMS
- Pamatuj si, kdy a kde se to stalo. Ideální je znát přesnou www stránku
- Svěř se někomu, komu důvěřuješ (kamarádům, učitelům, rodičům...)
- Nevhodný obsah nahlas provozovateli služby nebo na linku STOPonline.cz



Nevhodný obsah můžeš na internetu nahlásit i anonymně. Důležité ale je, aby oznámení kromě důkazů obsahovalo i dostatek informací. Zkus se rozepsat jako při psaní povídky.



Když si nebudeš vědět rady, obrať se (klidně i anonymně) na tyto profiky:

Linka bezpečí

Zavolej na Linku bezpečí. Je zdarma 24 hodin, 7 dní v týdnu na čísle 116 111

Když se necítíš na hovor, můžeš si s nimi chatovat nebo napsat e-mail

Linka důvěry

Zavolej na číslo 241 484 149 nebo 777 715 215, využít můžeš také Skype hovor, chat nebo e-mail. Všechny kontakty najdeš na www.ditekrize.cz

STOPonline.cz

Posoudí závadnost obsahu na internetu a případně ho odstraní.

Napiš jim na www.stoponline.cz

Kapitola 055 – Testíček

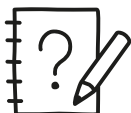


Na internetu je tolik pravidel, která si mám pamatovat...

A to ještě nejsme u konce



Teď se podíváme na další obsah, který není dobré sdílet



O tom, co sdílet, nebo nesdílet, už víš docela dost. Co říkáš na malý test? Zkus u každé situace popřemýšlet nad tím, jak by se dala zneužít.

KONCERT

LETENKA OK125 10:20 15 11C Praha USA

DŮM Game key 1235 6667 9523 1156

#NoveKolo

Mia F xx xx xxx Vinohradská 1 CZ

Zloděj bude vědět, že nejsi doma

Útočník může zjistit, kde bydlíš, nebo doklad zneužít

Někdo cizí použije kód na fotce a na koncert půjde místo tebe

Aktivaci hry udělá někdo cizí a tobě zůstane jen krabice a oči pro pláč

Cizí lidé budou vědět, že máš drahou věc. Pokud budeš sdílet další osobní údaje nebo to, kdy nebudeš doma nebo kam s tou drahou věcí jezdíš, mohou ti ji ukrást



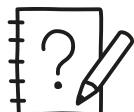
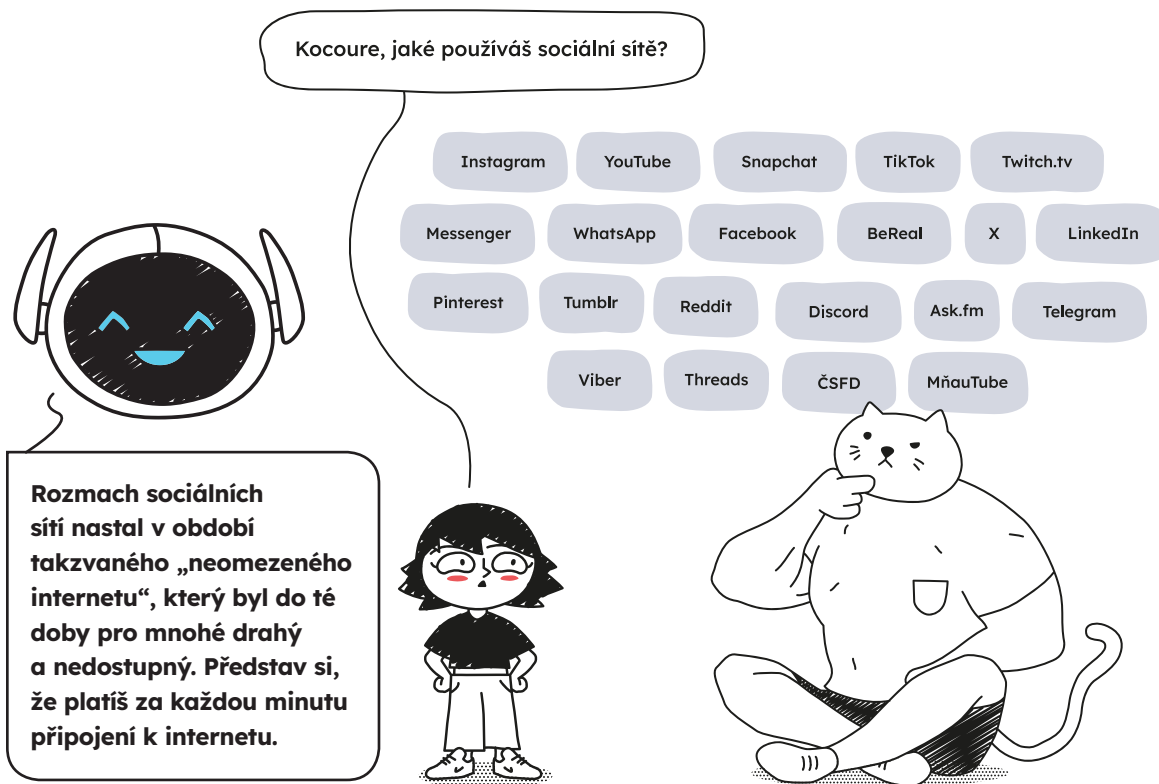
Část 5

Sociální média

Kapitola 056 – Co je sociální síť?



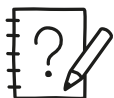
Sociální síť je internetová služba, která ti umožňuje vytvářet veřejné, uzavřené nebo i firemní profily, prezentace, diskuzní fóra a nabízí ti prostor pro sdílení fotek, videí, obsahu a dalších aktivit. Většinu obsahu sociálních sítí vytvářejí jejich uživatelé. Nejčastějším důvodem, proč lidé používají sítě, je navázání kontaktu, komunikace, zábava a prezentace vlastní osoby.



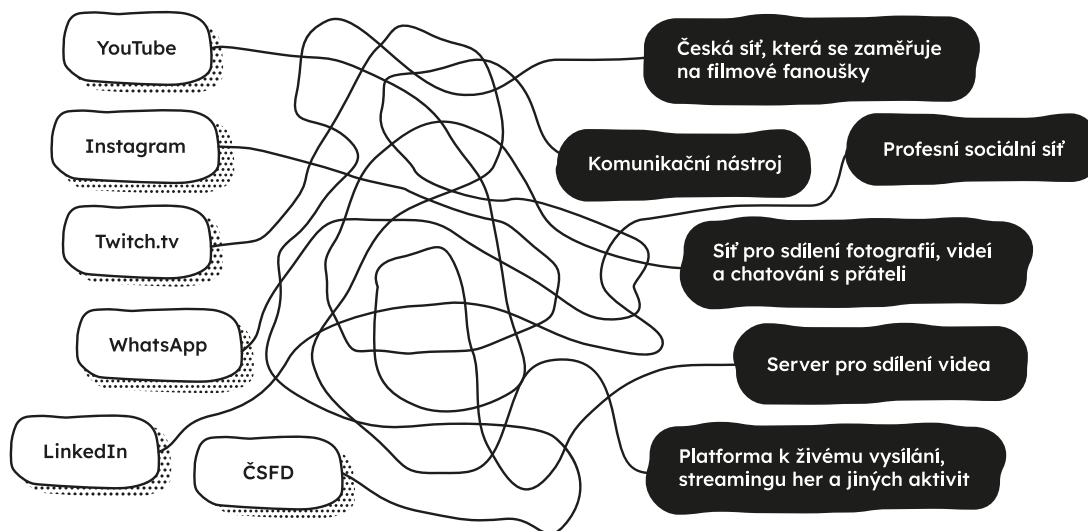
Je mezi sociálními sítěmi, které používá Kocour, i nějaká tvoje oblíbená?
Znáš nějakou další?

Kapitola 057 – Typy sociálních sítí

Kolik existuje sociálních sítí, nikdo neví, každý den vznikají desítky nových. Na celém světě používají alespoň jednu z nich téměř 4,8 miliardy lidí. Velká část slouží k sebeprezentaci nebo zábavě, ale jsou i sítě profesní, seznamky nebo sítě určené konkrétní skupině lidí – cyklistům, sběratelům a podobně. Máš pejska a chceš potkat někoho podobného na společné venčení? I taková síť existuje!



Dokážeš určit, čemu se věnují tyto sítě?



Mnoho sociálních sítí je přeloženo do českého jazyka, ale to z nich nedělá českou službu. Pamatuj, že v případě problémů na této síti se podmínky užívání řídí právem a zvyklostmi státu, ve kterém je zaregistrována. To ale neznamená, že si případný problém necháš pro sebe.

Kapitola 058 – Jaký obsah sdílet na síti

V části 4 o sdílení obsahu na internetu jsme si řekli, co vkládat na internet, a co na něj naopak nepatří. První věcí, kterou je po založení profilu na síti potřeba udělat, je nastavení soukromí. Aby tvůj obsah viděli jen tví kamarádi, rodina a blízcí. Pokud se v budoucnu rozhodneš sdílet svůj obsah se všemi na internetu, odstraň z něj citlivé a osobní údaje.



Sociální sítě jsou v Česku povolené zákonem až od 15 let.

Toto omezení je zavedeno proto, že se na nich může vyskytovat nevhodný obsah.



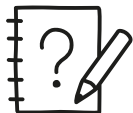
Na síti nevyplňuj všechny položky, které po tobě chce. Nikdo nemusí vědět, kolik měříš, jakou máš velikost nohy nebo jakou jíš zmrzlinu.

„Velikost Vašeho ocasu“



Pokud budeš sdílet osobní a citlivé informace, je větší pravděpodobnost, že ti budou psát lidé, o které nestojíš

Pokud nebudeš mít nastavený soukromý profil, ale budeš sdílet velké množství fotek, videí nebo storíček, může se stát, že si někdo tvůj obsah stáhne, zneužije ho nebo se za tebe bude vydávat. Internetoví predátoři často používají ukradený obsah k vytváření falešných profilů.



Které z těchto údajů není dobré mít veřejně na profilu? A víš proč?



Adresa bydliště ✕

Fotografie v plavkách ✕

Datum narození ✕

Můj stav: hledám flirt ✕

Výška, váha a barva vlasů ✕

Jméno mého domácího mazlíčka ✕

Fotografie sourozenců ✕

Informace o mém těle ✕

Moje nejoblíbenější jídlo ✕

Jména mých nejlepších kamarádů ✕

Číslo telefonu ✕

Moje zájmy ✕

Kapitola 059 – Lajky

Slyšet pochvalu nebo potlesk je krásný pocit a je to zcela přirozené. Stejně tak i na internetu. Po získání lajku nebo jiném uznání vyplavuje náš mozek látku, která se nazývá dopamin. Náš mozek má tuto látku moc rád a chce tento pocit vzrušení nebo radost stále opakovat.



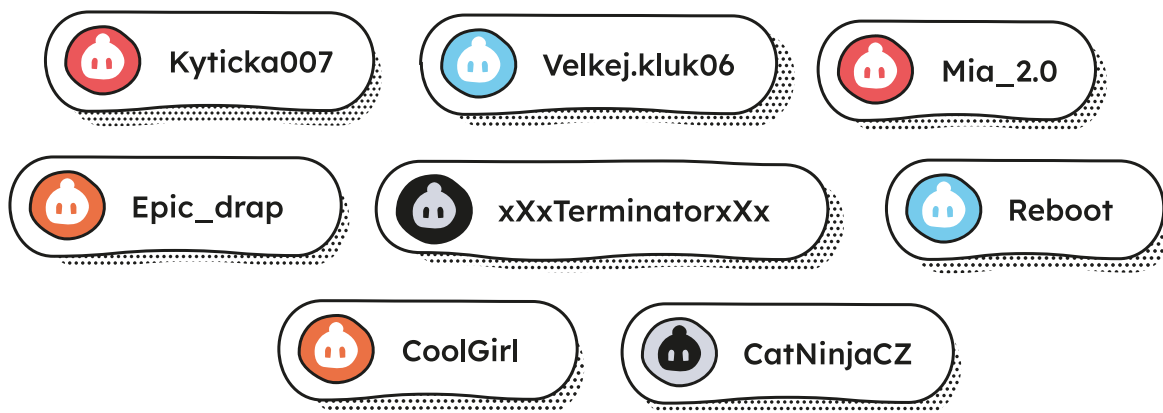
Zažívání virtuální pochvaly nebo slávy může být návykové. Když lajky nebo ocenění ustanou, můžeme cítit smutek, strach, nejistotu nebo mít pocit selhání. Mít hodně lajků ale neznamená, že jsme slavní nebo že jsme lepší než někdo druhý.

Chceš si o tom popovídat?
Zavolej na Linku bezpečí na telefon 116 111.



Kapitola 060 – Přezdívky

Většina sociálních sítí nevyžaduje vyplnění tvého skutečného jména. Vystupovat na nich můžeš pod přezdívkou (nickem). V případě zveřejnění jména zvyšuješ šanci, že tě najdou tví kamarádi. Pokud zvolíš přezdívku, zamysli se nad jejím zněním. Neměla by být vulgární, zesměšňující nebo útočná.



Pokud budeš volit název účtu, se kterým budeš vystupovat veřejně (ve škole a v budoucnu i v zaměstnání), je lepší používat účet s vlastním jménem než například GTA Killer.

To, že se uživatel skryje za přezdívku, neznamená, že ho v případě porušení zákonů nelze dohledat. Pokud zvolíš nevhodnou přezdívku, může tě správce služby zablokovat.



Kapitola 061 – Falešné profily a jak je odhalit

Každý pátý profil na internetu obsahuje nepravdivé informace. Lidé například zkreslují svůj věk, váhu nebo vkládají cizí či upravené fotky. My ti ukážeme několik tipů, které jsou velmi účinné. Počítej ale s tím, že internetoví podvodníci jsou vždy o krok napřed.

Ověření pomocí fotografie

Pokud máš podezření, že člověk, se kterým si píšeš, se vydává za někoho jiného nebo jsou jeho fotky až moc dokonalé, popros ho o jednu laskavost.



The illustration depicts a chat interface with a light blue background and a pattern of small blue dots and zig-zags. On the left, a grey circle with a black question mark represents the user. On the right, a character with black hair and glasses represents the person being questioned. The chat bubbles are as follows:

- Grey bubble (User): Chci, abys mi vyfotil svoji fotku, jak v ruce držíš cedulku, na které je napsáno moje jméno a dnešní datum. Tu fotku chci do pěti minut!
- Grey bubble (Person): Ty mi nevěříš? Chodím ještě do školy a líbí se mi
- Grey bubble (User): Nefunguje mi foťák :/
- Grey bubble (Person): Rodiče už spí, nechci je vzbudit...
- Grey bubble (User): Nejde mi to odeslat:((
- Grey bubble (Person): Mám vybitý telefon, vyfotím se ti jindy
- Grey bubble (User): ...
- Red bubble (User): Tak a dost! Takovou fotku dnes dokáže udělat každý! Když se někdo začne vymlouvat, že to nejde, je to vždy podezřelé!

Additional elements include a blue speech bubble on the right stating: "Pět minut je důležitých, fotka za tu dobu nejde upravit nebo zfalšovat." and a small white cat icon at the bottom right.

Ověření pomocí videohovoru

Jedná se o nejspolehlivější metodu ověření. Mysli ale na to, že si videohovor může kdokoliv nahrávat. Ukazuj proto jenom obličej. Jak se dá videohovor zneužít, nalezneš v kapitole 077 – Podvod s webkamerou.



Při videohovoru si dej pozor na pár věcí

Obráz by se neměl sekát a neměl by být bez zvuku. Na tvoje otázky by člověk (nebo kočka) na druhé straně měl odpovídat plynule



To je velmi důležité, podvodníci ti totiž mohou pustit videosmyčku někoho jiného.

Ověření pomocí vyhledávače obrázků

Někteří podvodníci si do profilů dávají fotografie celebrit nebo jiných lidí, které někomu ukradli.



Zkus fotografii vyhledat pomocí vyhledávačů obrázků. Třeba Google Lens nebo Tineye.com

Vyhledávač ti může napovědět, jestli byla fotografie někde zveřejněna



Pozor, vyhledávače neumějí vyhledávat v uzamčených profilech nebo soukromé komunikaci. Pokud se ti nezobrazí žádné výsledky, neznamená to, že je člověk na druhé straně tím, za koho se vydává.

Najdi si digitální stopu

Zkopíruj si přezdívku nebo jméno toho, s kým si píšeš, a zkus ho zadat do vyhledávače. Výsledky by ti měly ukázat jeho digitální stopu. Můžeš zjistit více informací. Pokud nenajdeš žádné výsledky, je to podezřelé.

**Při komunikaci
a ověřování si neposílejte
žádné kopie dokladů!**

Kapitola 062 – Více o falešných profilech

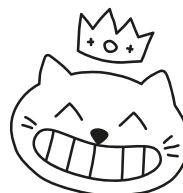
Téměř třetina všech profilů na sociálních sítích neobsahuje fotografie. To ale neznamená, že jsou falešné. Někdo se prostě nechce ukazovat. Stejně tak může mít jen málo přátel.



Mezi největší mýty o tom, jak poznat falešné profily, patří to, že:

- Byly založeny nedávno
- Mají málo fotek nebo žádnou fotku
- Mají málo přátel

Zkušení podvodníci, kteří to dělají opravdu dlouho, mají profily se spoustou přátel nebo mají hromadu fotek. Jednou jsem odhalil falešnou kočku. Psala mi, jak mě miluje, a poslala mi svoje fotky. Za ní ale byly dveře s kulatou klikou. A ty u nás nejsou. Dostal jsem ji!



Podívej se na síť, kterou používáš, a zkus najít ověřené uživatele.

Zahraj si na detektiva a všímej si detailů na fotkách. Některé fotografie nebo videa nemusejí pocházet z českého prostředí. Místo paneláků budou na fotkách mrakodrapy, v knihovnách budou tituly na hřbetech knih v jiném jazyce nebo budou na fotkách věci, které nepoznáváš.



Velká část služeb na internetu umožňuje svým uživatelům ověření. U jejich jména je pak označení pravosti. Tito lidé jsou skuteční. I ty se můžeš nechat ověřit a u tvého jména pak bude fajfka nebo jiný symbol, který slouží k označení ověřeného profilu.

Kapitola 063 – Co mám dělat, když narazím na fejk?

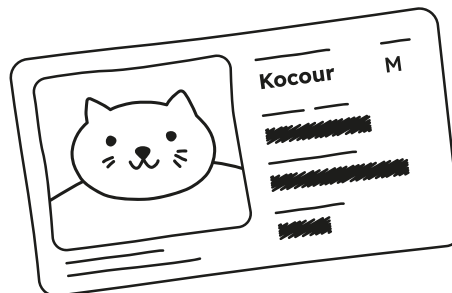
Pokud na internetu objevíš profil, který se za někoho vydává, nenech si to pro sebe. Profil se dá nahlásit přes odkazy (Nápověda, Kontakt, Technická podpora...) nebo přes tlačítko na profilu. Můžeš se také svěřit kamarádům, rodičům nebo učitelům či využít některou z linek pomoci.



Do formuláře uveď co nejvíce informací o tom, proč si myslíš, že je profil falešný. Pokud to bude možné, uveď jméno nebo odkaz na pravého majitele nebo přilož nějaký důkaz, například screenshot. Pokud profil nahlásí víc lidí (třeba kamarádů), je větší šance, že bude smazán.



Když se za tebe někdo vydává, mohou některé sítě vyžadovat kopii některého z dokladů. Pokud se rozhodneš situaci řešit touto cestou, zkus některé údaje z dokladu zakrýt.



Kapitola 064 – Osobní údaje jsou velmi cenné, opatruj je!

Víš, jak oslovují internetoví predátoři své oběti? Hledají profily na sociálních sítích, které se jim nejvíce líbí a splňují určité požadavky. Ty potom cíleně osloví.



Najdi mi holku ve věku 15 let, blond, v okolí místa, kde bydlím, a chci, aby se zajímala o koně



Vášim požadavkům vyhovuje 23 dívek, chcete jim napsat?

Nové hledání





Pokud do svého profilu veřejně napíšeš, že hledáš flirt, nebo do něj vložíš fotografie v plavkách, do půl těla nebo další fotografie či citlivé údaje, je pravděpodobnost, že tě osloví nějaký predátor, až padesátinásobně vyšší.



Profil si uzamkni před cizími lidmi. Pokud tě osloví někdo neznámý, nejprve si ho ověř, než si ho přidáš do přátel.

Kapitola 065 – Ignorace/Blokace



Pamatuj si, že se nikdy nemusíš na internetu bavit s každým, kdo ti napíše

Já mám v ignoraci asi 20 koček a kocourů



Já jenom jednoho kocoura. Schválně, jestli uhodneš jeho jméno :)))

Tak si mě odblokuj, protože ti jinak nebudu moct posílat memečka



No tak jo...

Pokud si někoho blokuješ z důvodu, že ti posílá nevhodné zprávy nebo obrázky, že ti vyhrožuje, nebo tě dokonce přímo vydírá, vytvoř si nejprve důkaz. Tím může být obrázek konverzace (screenshot) nebo nevymazané zprávy ve tvém telefonu nebo počítači. S důkazy, které prokazují, co se ti stalo, se někomu svěří.



Pokud zvolíš trvalou blokaci, dotyčný tě už nemůže kontaktovat. Bude odebrán i z přátel a zmizí i odkaz na jeho profil. Předtím, než to uděláš, si vše zazálohuj.

Když si s někým nebudeš chtít psát, můžeš si na sociální síti nastavit, zda ho trvale zablokuješ, nebo jen omezíš přijímání zpráv od něj. U některých sítí si můžeš nastavit, že ti budou moct psát pouze přátelé. Blokaci lze i zrušit.



Představ si, že by ti přišly tyto zprávy. Jaká by byla tvoje reakce?

Jestli mi to neřekneš, tak si najdu, kde bydlíš, a uvidíš!

Chceš vidět, co mám pod spodním prádlem?

Máš pět minut, jinak to všichni uvidí a bude ostuda!!



1. Nebudu odpovídat
2. Odpovím a zeptám se, co chce
3. Poprosím, aby mě nechal na pokoji
4. Udělám si důkaz
5. Všechno vymažu a budu dělat, že se nic nestalo
6. Svěřím se někomu
7. Odpovím mu a budu mu také vyhrožovat
8. Nahlásím tyto zprávy sociální síti

Píše mi nějaký Mikeš, že jsem ošklivý, vypelichanej kocour... Odpovídat mu nebudu, rovnou si ho zablokuj!



Možná má pravdu, ale raději mu vůbec neodpovídej a udělej si screenshot



Screenshot si děláš i pro případ, kdyby se situace zhoršila. To je ten nejlepší důkaz, který můžeš mít.



Kapitola 066 – Chladná hlava

Na internetu je dnes celý svět. Pokud do tohoto světa vstoupíš, musíš počítat s tím, že ne každý se k tobě bude chovat hezky, dávat ti srdíčka, palečky, lajky a kladná hodnocení nebo komentáře. I když tě může mrzet, že se někomu nelíbilo tebou vytvořené video nebo bude hejtit tvoji fotku, zachovej chladnou hlavu.



Já si to s tebou vyřídím!

Největší chybou, kterou můžeš udělat, je, že na tyto zprávy budeš odpovídat. Někteří lidé jen čekají na to, až se s tebou budou moct hádat



Která z těchto reakcí je správná?



Jestli mi teď hned neodepišeš, tak to pošlu tvým rodičům!



Dělej!!!



Jak myslíš, teď to uvidí všichni!

✗ Neznámý vám nemůže psát, je zablokován



Znám tvoje tajemství a řeknu ho všem!

Jaké tajemství???



Co se stalo na školním výletě

Prosím, nedělej to! Udělám cokoliv...



Jsi obyčejná socka!



Ani mi neumíš odeslat, protože máš určité tlačítkové mobil!

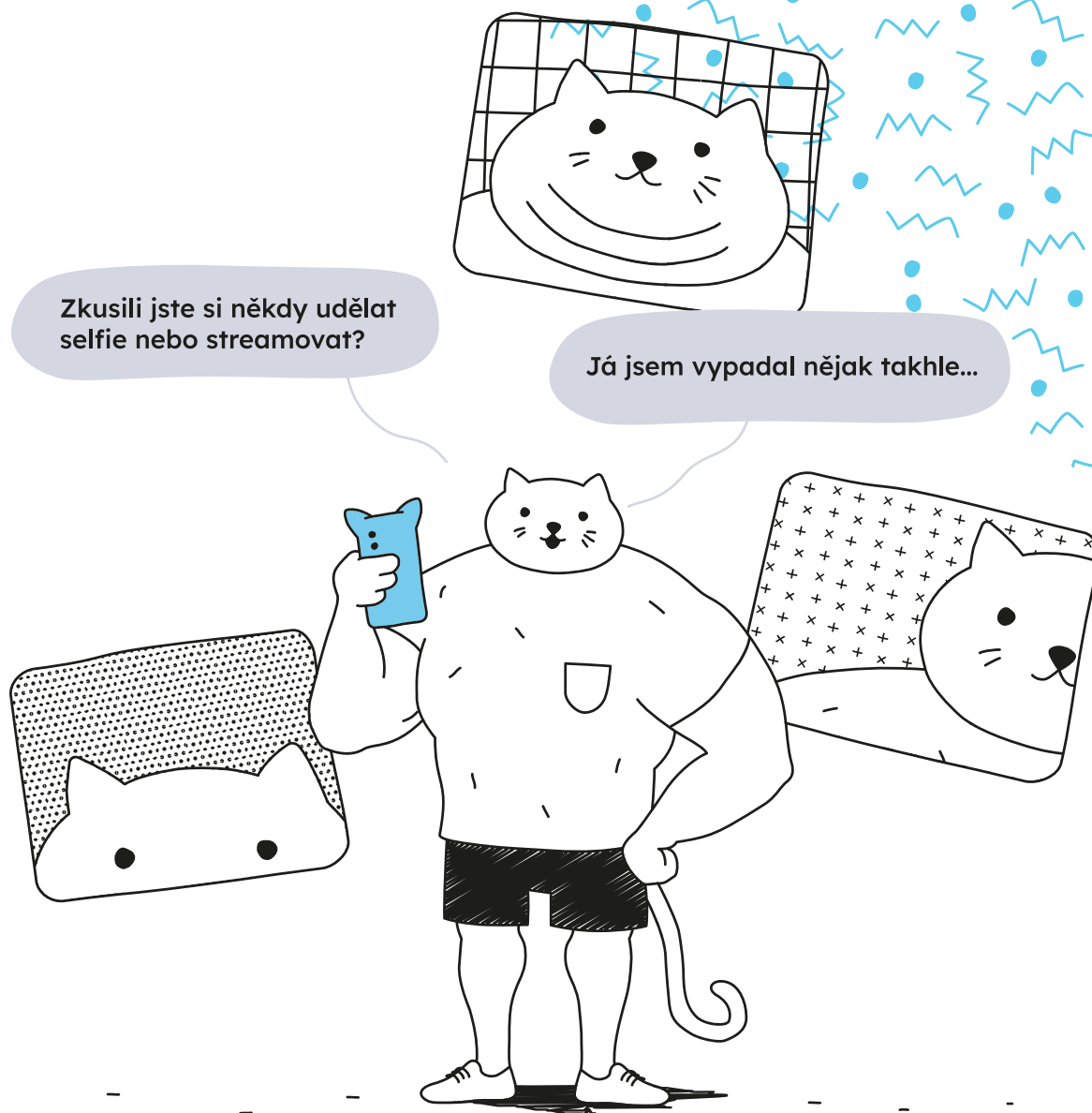


Hej!!! Dělej, odepiš mi!

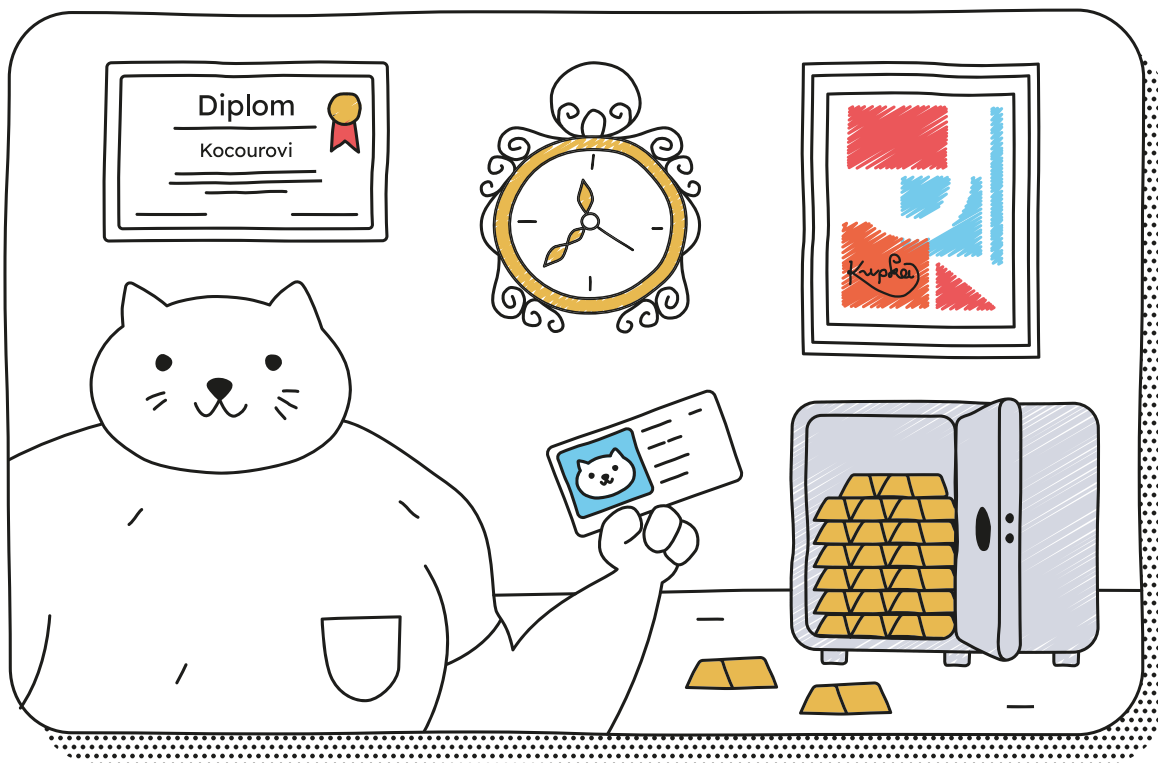


Hej!!! Dělej, odepiš mi!

Kapitola 067 – Selfie



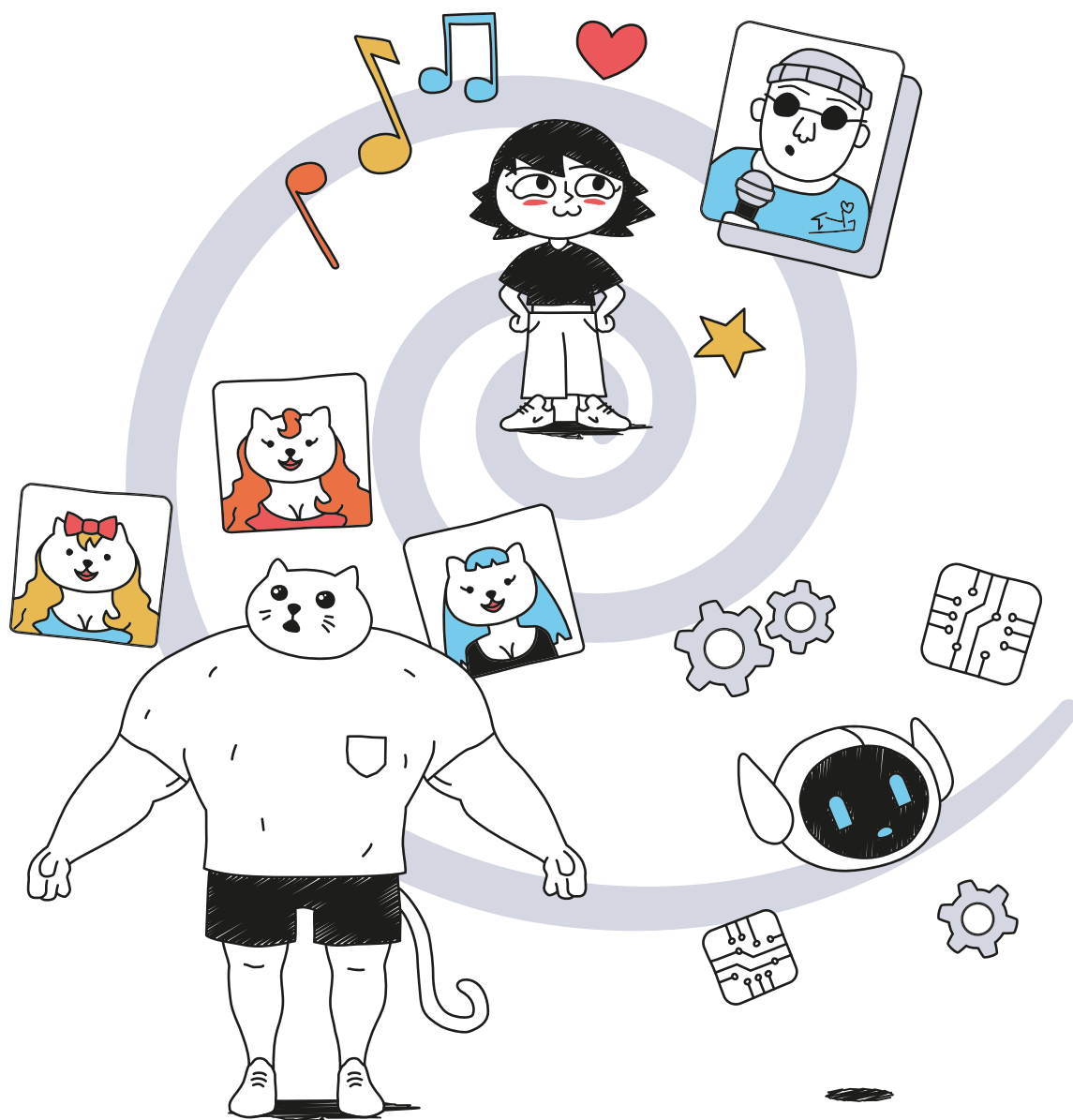
Není důležité, jak na selfie vypadáš, ale co se z té fotografie nebo videa dá zjistit. Podívej se na obrázek. Která z věcí o Kocourovi něco prozrazuje?



Podvodníci si mohou o tobě zjistit mnoho věcí. O tom, co máš doma, kde bydlíš, nebo další informace. Pak už si může podvodník dát jedna a jedna dohromady a může ti třeba vykrást byt. Před zveřejněním fotografie se ujisti, že neobsahuje cenné informace.

.....
Obraz - Na stěně mu visí drahý obraz, Občanka - Zjistiš osobní údaje, adresu nebo jméno, Diplom - Je vidět jméno a adresa
Zlaté cihly - Kocour má v bytě hodně peněz, Hodiny - Viš, kdy je Kocour doma,

Kapitola 068 – Králiči nory



Představ si, že jsi nový uživatel sociální sítě. Síť o tobě nic neví a ve snaze tě zabavit ti ukazuje virální obsah, který je oblíbený jinými uživateli. Uvidíš tak třeba vtipná videa, pejsky, zvířátka, motorky, přírodu nebo různé pranky. Podle toho, jak na ně reaguješ, zjistí síť to, co tě baví, a bude ti tento obsah nabízet přednostně.

To, že ti síť nabízí určitý obsah, se ti bude líbit, a budeš tak na ní trávit hodně času. Čím více času na ní strávíš, tím více ti může síť nabízet reklamy, a roste tak její zisk.



To, co mi síť nabízí, se mi docela líbí. Ale co je vlastně ta králíčí nora?

Když se ti z nějakého důvodu přestane vybraný obsah líbit, přestaneš ho lajkovat a sdílet, nabídne ti síť podobný obsah, ale ne tak virální. A ten nemusí být tak v pohodě...



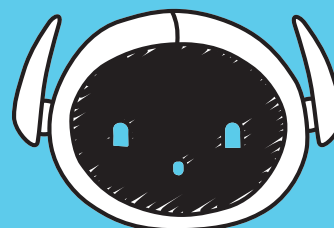
Tento obsah ti pak může přivodit různé psychické problémy, nespavost, zhoršení soustředění ve škole a spousty dalších nepříjemností...



Pokud se nebudeš při používání sociálních sítí cítit dobře nebo máš jiné obavy, neboj se říct si o pomoc. Zavolej na Linku bezpečí nebo na Linku důvěry.



Sociální sítě netrvá ani hodinu, aby o tobě zjistila téměř všechno. Chceš vědět víc o králíčích norách i to, jak fungují různé algoritmy? Podívej se na video od Kovyho: www.youtube.com/watch?v=IARByMNIpsw



Kapitola 069 – Bubliny

Na sociálních sítích se budeš chtít obklopovat lidmi, kteří mají stejné názory, koníčky nebo podobný pohled na svět. Budeš také více sledovat takový obsah, který tě zajímá a baví. Toho si brzy všimne sociální síť a bude ti všechny tyto věci nabízet přednostně. Postupně tak neuvidíš lidi s jiným názorem nebo videa, která se ti nebudou líbit. Můžeš se uzavřít do sociální bubliny.



Obsah, který vidíš, ti nabízejí algoritmy sociálních sítí. Příspěvky se už neřadí podle času, ale podle toho, jak si sociální síť myslí, že by se ti mohly líbit.



Vojna by měla být povinná

Zbraně patří do každé rodiny!

Poslal bych tam armádu

Střelení by mělo být povoleno od 15 let!



Zbraně jsou největší zlo!

Nechceme válku!

Chceme lásku a mír

Zakázala bych vojáky i zelenou barvu!

Uvnitř našich bublin se mohou objevovat nepravdy, zkreslené informace, můžeš se ve svých názorech utvrzovat nebo se v nich stále více radikalizovat.



Nevidíš dlouho žádný příspěvek svého kamaráda? Navštiv jeho profil a podívej se, jak se mu daří. Pokud ti chybí, ozvi se mu.

Kapitola 070 – Třetí strany

Určitě to znáš. Než založíš účet nebo si zahraješ nějakou hru, musíš potvrdit, že souhlasíš s podmínkami používání. A ty bývají opravdu hodně dlouhé.



Pozorně si přečti licenční podmínky služby, kterou chceš používat. Mohou obsahovat i informace, které se ti nemusejí líbit. Může jít o práva k obsahu, předplatné, pokuty, sledování nebo oprávnění využívat další části tvého zařízení. Zamysli se a nepotvrzuj každou možnost, která je ti nabídnuta.



Existují různé služby, které ti pomohou zjistit, jaké informace se o tobě sbírají. Tuto možnost nabízejí i některé sociální sítě.

Kapitola 071 – Jak odejít ze sítě, která mě už nebaví



Může se ti stát, že tě nějaká služba na internetu omrzí a už ji nebudeš chtít používat. Nestačí se z ní jen odhlásit nebo smazat ikonku na ploše telefonu. Údaje, které do ní jednou vložíš (fotky, videa nebo psaní s kamarády), v ní stále zůstávají.



Před opuštěním sítě z ní vymaž citlivé údaje

Fotky, videa nebo komunikaci...



Většina sítí má v nastavení možnost profil smazat nebo deaktivovat, tak se na to podívej

U každé sítě to najdeš pod jiným názvem



Úplné smazání účtu bývá ale pořádně schované, budeš možná muset déle hledat nebo si najít návod na internetu

Svůj účet na síti můžeš i jen dočasně deaktivovat, profil tak zmizí a nebude se zobrazovat. Po nějaké době ale půjde zas obnovit. Všechny údaje a obsah na něm zůstanou.

Část 6

Seznamování na internetu

Kapitola 072 – Seznamky

Říká se, že internet je bezpečný, nebezpeční jsou na něm jen lidé. Na každé službě potkáš podivné lidi, podvodníky, fejkky nebo ty, kteří se ukazují v lepším světle. Na seznamkách jich je ale statisticky ze všech sociálních sítí nejvíc.



Seznamování na internetu je dneska úplně normální. Jen si musíš ověřit, s kým si píšeš, a hodně věcí brát s rezervou. V následujících kapitolách ti ukážeme pár triků, které používají útočníci nejčastěji.



Kapitola 073 – Zrcadlení, metoda podvodníků



Když o tobě zjistí informace, napíše ti většinou pod falešným profilem



O tom, jak si ověřit profil, jsme ti už povídali



Pokusí se tě oslovit pod nějakou záminkou



Většinou to bude nějaká nenápadná narážka, kterou o tobě útočník zjistil



Zaujme tě to, budeš chtít vědět víc a začnete si psát

Ahoj, nebyla jsi náhodou loni na táboře u Mácháče? Mám pocit, že tě znám...

Jéé, ty máš ale hezkýho retrívrá, já mám úplně stejného!

Nejsi náhodou z Plzně?

Čauky, ty chodíš na ZŠ U Parku, vid?

Ahoj, taky mám rád FC Barcelona, chceš se kamarádit?

Jak může vypadat celá konverzace, kde útočník jen kopíruje (zrcadlí)?

?

Ahoj, promiň, že otravuju, ale neznáme se náhodou?

Ahoj, nevím, odkud?



?

Nechodíš náhodou na gympl ve Lhotě? Mám pocit, že tě tam potkávám...

Jo, chodím, ty taky?



?

Jj taky máte na tělák starýho Růžičku?

Máme no, ten je strašnej, co xDD



?

Je, ale já mám fakt rád sport a tenis mě mega baví

Fakt? Já ho hraju závodně



?

Nekecej. A kolik ti vlastně je? Mně 14

Vážně? Tak to jsme stejně starý...



?

A kde bydlíš?



Po čase opadne počáteční nedůvěra, a můžete si tak začít psát i o citlivějších tématech. Celou dobu s tebou může útočník manipulovat, aby zjistil více informací, tvoje poměry nebo další údaje. Ty pak ale může zneužít.

Kapitola 074 – Oslovení útočníků – Rychle na věc

Někteří útočníci si s tebou nebudou chtít psát týdný nebo měsíce. Pokusí se hned na začátku psaní zeptat na citlivé věci. Když je odmítneš, nejspíš ti přestanou psát. Nebudou s tebou chtít ztrácet čas a osloví někoho dalšího.



Už jenom to, že se ti někdo pokusil psát citlivé věci, někomu řekni

Ty to sice můžeš přejít mávnutím ruky, ale útočník osloví někoho dalšího a ten nemusí být tak v obraze jako ty!



Všiměj si, kam konverzace s novým kamarádem směřuje. Pokud se bude velice rychle stáčet na citlivá témata, můžeš mít jistotu, že to s tebou nemyslí dobře.

Podívej se na tyto dvě konverzace. Která z nich je v pořádku a která ne? Dokážeš říct proč?

?

Ahoj!

Čauky, známe se?



?

Jj z tábora

Fakt? Si tě nevybavuju



?

To nevadí, pokecáme?

O čem?



?

Nevím, třeba co máš na sobě, nebo můžeme vyměnit nějaký fotečky

Fotečky? Jaký?



?

Klídne lechtivý .)

?

Ahoj, moc se mi líbíš, nechceš si psát?

Ahoj. Napišeš mi něco o sobě?



?

Mám rád holky jako ty

A to je všechno?



?

Co bys řekla na to, že bych ti poslal svoji nahou fotku? Poslala bys pak svoji?

Ne



✗ Uživatel Neznámý byl zablokován

Kapitola 075 – Neodolatelné nabídky

Další možností, jak tě může někdo oslovit, je, že ti útočník rovnou napíše, co chce a co ti za to nabízí. Většinou to bude nějaká hodně drahá věc nebo hromada peněz. Cílem je tě zaujmout a vzbudit dojem, že se ti to vyplatí.

Ukážeš se mi nahý? Pošlu ti nový telefon

Zapni si na pět minut webku a pošlu ti tisíc korun

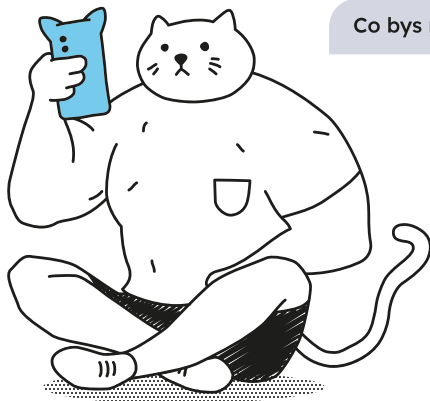
Když se se mnou sejdeš, můžeš si vydělat víc než na brigádě za půl roku. A neboj, nikdo se to nedozví.

Chtěla by sis vydělat?

Když se mi ukážeš, koupím ti tu novou hru

Co bys řikala na to, kdybych tě rozmazloval?

NIKDY, opravdu NIKDY na podobné, jakkoli lákavé nabídky nepřistupuj a okamžitě se někomu svěř. Jak na to, jsme ti vyprávěli v kapitole 054.



Pokud se necháš nalákat na možnost výdělku, ztrácíš nad tím, co bylo zasláno, kontrolu.

Kapitola 076 – Snaha tě izolovat od ostatních

Máš na internetu nového kamaráda a je ti s ním dobře. Po nějaké době si můžete povídat o citlivých věcech, které se svými skutečnými kamarády neřešíš. Budeš se svěřovat s tím, co tě trápí doma nebo ve škole. Toho může nový kamarád zneužít.



A jak to poznám, že je něco špatně?

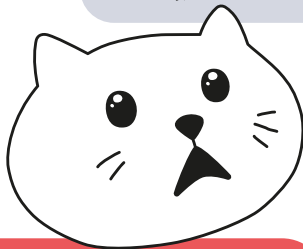
Kamarád tě bude ujišťovat o tom, že to, o čem si povídáte, zůstane jen mezi vámi. Že jde o tajemství, které nikomu neprozradí... A když zjistí, že tě má omotaného okolo prstu, tak na tebe může zaútočit



Jejda! Já už jsem asi někomu něco prozradil...

Za tohle se ti budou všichni ve třídě smát!

Počkej, až to táta zjistí!



Co říkáš na to, kdyby to bylo na internetu?

Když mi nepošleš, co chci, všichni to uvidí!

Mám to, co jsme si napsali, zveřejnit?



Nikdy na výhrůžky nereaguj a nesnaž se vykoupit. Situace se ještě může zhoršit. Když si nebudeš vědět rady, napiš nebo zavolej na linku, kde ti pomohou

Linka bezpečí – zavolej na bezplatné číslo 116 111 (kdykoli) nebo chatuj na www.linkabezpeci.cz

Linka důvěry – svěř se se svým problémem, www.ditekrize.cz, Rizika kyberprostoru (telefon 778 510 510)

Kapitola 077 – Podvod s webkamerou



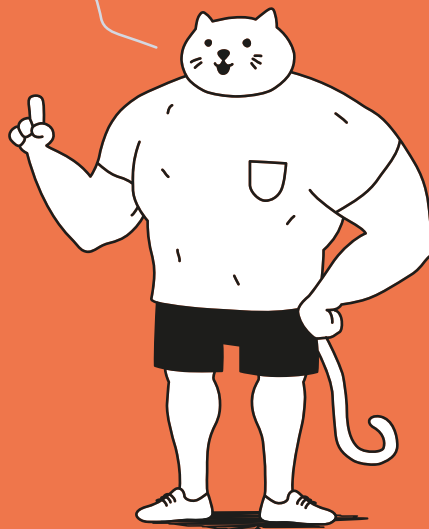
Webcam trolling je druh podvodu, který se používá k oklamání při videohovoru. Jde o podvržený videozáznam, na kterém ti osoba na druhé straně místo sebe bude pouštět videosmyčku, na které je někdo jiný.

Vynalézavost podvodníků nezná mezí. Víš, že se dá podvádět i s videohovory?

Webcam trolling původně vznikl jako žert. Volající chtěl napálit kamaráda a pustil mu místo sebe opičku, která psala na klávesnici. Brzy toho ale začali zneužívat podvodníci.

Psal jsem si se super číťou, ale bylo mi divný, že nejde zvuk a pořád se to divně sekalo. Svlékala se a chtěla po mně, abych udělal to samé...

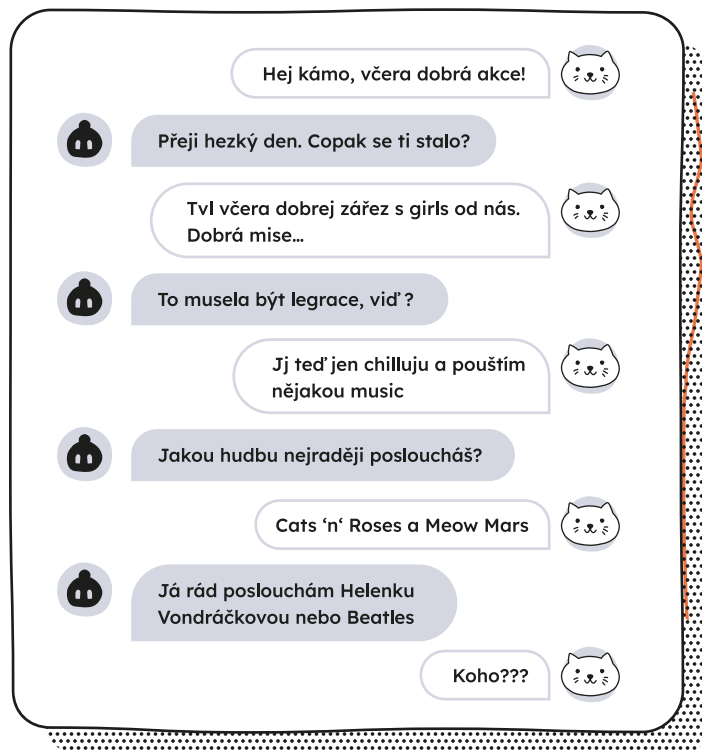
U videohovoru by měl vždy fungovat zvuk. Můžeš také požádat volajícího, aby udělal něco konkrétního, netradičního. Třeba si dal pravou ruku na levé ucho. Tím si ověříš, že nejde o předtočenou videosmyčku.



Webcam trolling je nebezpečný v tom, že si tě může útočník skrze něj nahrávat. Ukazovat bys měl jen ty věci, které nejsou citlivé. Určitě se neodhaluj!

Kapitola 078 – Mluvíš jako můj děda

Při seznamování a psaní s neznámými lidmi byste si měli všimnout více věcí. Jednou z nich je to, jak vám kámoš nebo kámoška z internetu píše. Když si budete psát o hrách, oblíbených streamerech nebo o hudbě, tak se nemusí vůbec chytat. Je možné, že za monitorem bude sedět někdo jiný a starší...



Když si nebudete jisti, zda ten, s kým si píšete, je tím, za koho ho máte, nebo zda se za něj jen vydává, ověřte si to (kapitola 061).

Kapitola 079 – Seznámení naživo

Pokud na internetu potkáš kamaráda, kterého budeš chtít potkat i osobně, je důležité dodržet pár pravidel.

Nescházej se okamžitě

Nepodlehni nátlaku ani pocitu, že když teď hned za kamarádem nepůjdeš, přijdeš o něj.



Schůzku si domluv přes den



Ve tmě může kámoš nebo kámoška vypadat jinak. Vím, o čem mluvím...

Veřejné místo



Schůzku si naplánuj na veřejném místě, kde je co nejvíce lidí. Ideální jsou náměstí nebo obchodní centra. Ta mají i kamery nebo ostrahu.

Pozor na uzavřené prostory!

Nikdy se nescházej na místě, ze kterého se nedá lehce odejít. Nechoď k neznámým lidem do bytu ani nastupuj do aut.





Dej si „rande“ ve třech

Na první schůzku s někým z internetu, koho dobře neznáš, vezmi s sebou někoho dalšího.



Dej někomu vědět

To, že půjdeš na schůzku, někomu řekni.

Zahraj si na detektiva

Než na schůzku vyrazíš, ověř si, že je kamarád skutečný!



Vyžádej si více fotek nebo jdi na videohovor

Nespokoj se jen s tím, co ti online kamarád povídá.



Můžeš odejít

Když ti bude schůzka nepříjemná, vždy můžeš odejít. Není podmínkou, že na ní zůstaneš jen ze slušnosti.



Alarm

Pokud tě bude nový kamarád nutit do věcí, které nechceš, udělej hluk nebo jdi k nejbližším lidem.

Osobní údaje

Na první schůzce nesděluj nic osobního, třeba kde bydlíš.



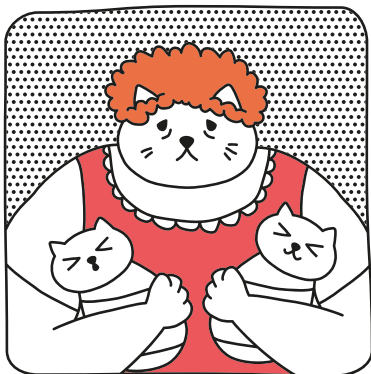
A co ty? Vymyslíš ještě nějaké další pravidlo?

Jo! A neplať za všechny xD



Kapitola 080 – Ptej se na podrobnosti

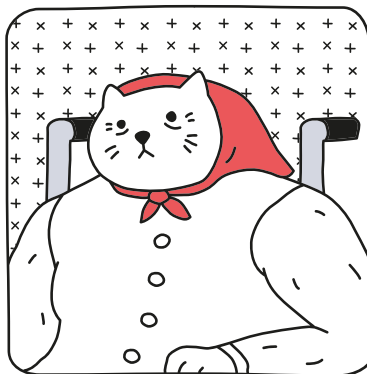
Na seznamkách se pohybuje celá řada lidí, kteří mají seznamování jako zábavu a ve skutečnosti se nikdy nechtějí potkat naživo. Žijí ve svém světě, ve kterém mohou být kýmkoliv. Třeba ředitelem banky. Nebo se mohou vydávat za nemocného, aby vzbudili soucit.



Jsem svobodná matka sedmi dětí, mám tři zaměstnání, abych je uživila. Abych ušetřila, svítíme doma svíčkou.



Hi! Jsem americký voják na misi v Africe a chtěl bych bydlet v Česku a ty se mi moc líbíš. I love you!



Děti mě opustily a z důchodu mi nezbývá na jídlo. Pomůže mi někdo? Stačí pár korunek na chleba...

I když mají podvodníci svoje příběhy promyšlené, čas od času se chytí do vlastní lži. Stačí se opakovaně ptát na podrobnosti. Třeba na to, jaké mají auto. Jednou bude modré, a podruhé žluté.



**Neposílej peníze
neznámým lidem
z internetu.**

Kapitola 081 – Jména

Poznat falešný profil je už pro tebe hračka. Poradíme ti ale ještě jednu vychytávku, jak poznat na internetu podvodníka. Podle jména.



Kocoure, kdyby sis založil falešný profil na seznamce, jaké bys mu dal jméno?

Asi Karolínka Zkušená nebo Nadrženkyně001



To je ale pěkně hloupé jméno a takové přezdívky si holky nedávají! Tebe bych odhalila hned.

Zkopíruj si jméno a zadej ho do vyhledávače. Zahraj si na detektiva. Pravděpodobně zjistíš, že pod tímto jménem neexistuje žádná digitální stopa.



Nejčastějšími falešnými jmény na seznamkách jsou:

Karolínka
Kristýnka
Lucka
Vojta
Patrik
Matyáš (Maty)

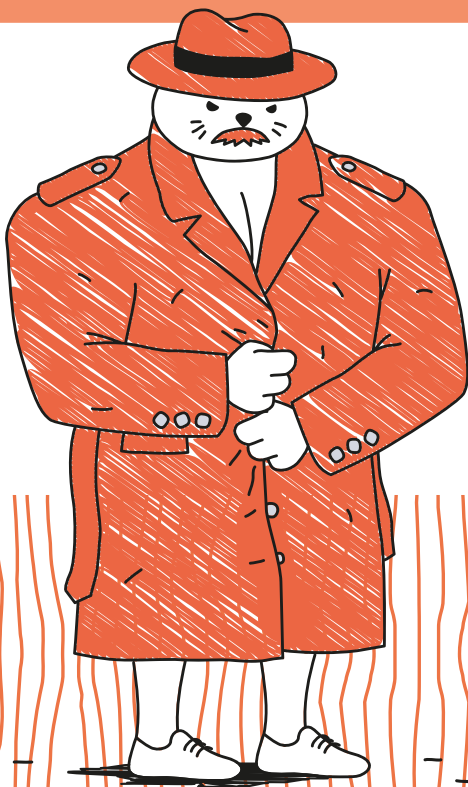
Jak nenaletět a jak si ověřit, jestli není profil falešný, nalezneš v kapitole 061.

Kapitola 082 – Predátoři

Už jste slyšeli o internetových predátorech? To jsou lidé, kteří tě mohou zneužít nejen online na internetu, ale i fyzicky. Tyto útočníky také označujeme jako kybergroomery. K tomu, aby dosáhli svých cílů, používají celou řadu manipulačních technik.



Kybergrooming je manipulace útočníka s obětí prostřednictvím moderních technologií s cílem získat její důvěru a pak ji vylákat na schůzku a zneužít.



Mylná představa je ta, že je predátor starší osoba. Většinou jsou útočníci v podobném nebo jen lehce starším věku než ty. Díky tomu dobře ovládají technologie, pohybují se na internetu jako ryba ve vodě a dokážou se s tebou bavit o spoustě věcí.

Shrneme si pár rad, jak se bránit predátorům:

- Ověř si, s kým na internetu mluvíš (**kapitola 061, 062, 081**)
- Nikomu nesděluj osobní údaje. Platí to o celém jméně, adrese i telefonu (**kapitola 049, 058**)
- Nikdy neposílej intimní informace, fotky nebo videa
- Dej si pozor i na online streamy (**kapitola 053, 077**)
- Nenech se nalákat na peníze (**kapitola 075**)
- Bavte se jen o tom, o čem byste se byli schopni bavit osobně
- Pozor na manipulaci (**kapitola 073, 074, 076**)
- Pokud se s někým nechceš bavit, nebav se
- Pokud je ti jednání druhé strany nepříjemné, nepřistupuj na ně
- Neboj se svěřit, můžeš tím zachránit někoho dalšího
- Nesnaž se „lovit“ predátory, je to velmi nebezpečné!
- I když už uděláš chybu, nikdy nepřistupuj na výhrůžky a vydírání
- Každá situace se dá řešit



Pokud kybergroomer udělá chybu, poučí se z ní a jeho příští útok bude zase o něco dokonalejší.

Pokud na kybergroomera narazíš, nenech si to pro sebe:

Linka bezpečí – zavolej na bezplatné číslo 116 111 (kdykoli) nebo chatuj na www.linkabezpeci.cz

Hotlinka STOPonline.cz – zde můžeš anonymně nahlásit závadný obsah, který hotlinka rychle odstraní

Linka důvěry – svěř se se svým problémem, www.ditekrize.cz, Rizika kyberprostoru (telefon 778 510 510)

Poradna Napiš nám: www.napisnam.cz

Kapitola 083 – Další testíček!



Odet' se zkusím na internetu seznamovat podle pravidel

Tak schválně, dokážeš správně odpovědět na pár otázek?



Správné odpovědi najdeš na konci stránky



1. Když ti na internetu někdo nabídne peníze za fotky, videa nebo osobní setkání, tak:

- a) Na nabídku kývnu, ale řeknu si o víc peněz
- b) Zeptám se na podrobnosti
- c) Nebudu odpovídat, udělám si screenshot a někomu to řeknu



2. Když ti bude někdo vyhrožovat nebo tě vydírat, jak se zachováš?

- a) Nebudu reagovat a někomu se svěřím
- b) Raději útočníkovi vyhovím, aby se to nikdo nedozvěděl
- c) Pokusím se smlouvat



3. Jak by měla probíhat první schůzka s kamarádem z internetu?

- a) Domluví si ji ve dne a půjdu na ni sám
- b) Nejlepší schůzka je tam, kde nás nikdo neuvidí
- c) Půjdu na ni s někým dalším ve dne a proběhne na místě plném lidí



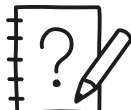
4. Když s někým budu mluvit přes webkameru, pohlídám si:

- a) Aby mi to na videu slušelo
- b) Nebudu ukazovat, co mám za sebou, nebudu v citlivé situaci a pohlídám si, aby osoba, se kterou se bavím, měla funkční zvuk a obraz
- c) Nastavím si video tak, aby bylo vidět co nejvíc, ideálně celý pokoj v HD kvalitě



5. Pokud mě osloví někdo z internetu, tak:

- a) Si ho hned přidám do přátel a zjistím, kdo to je
- b) Zkusím si o něm nejprve zjistit co nejvíc informací
- c) Dám si ho do ignore



Zkus vymyslet pět dalších otázek a udělej si test se svým kamarádem nebo sourozencem. Nebo zkusíš otestovat rovnou rodiče?

Část 7

Kyberšikana

Kapitola 084 – Co je kyberšikana

Kyberšikana (Cyberbullying) je jakékoliv chování, jehož záměrem je oběť vyvést z rovnováhy, ublížit ji, zastrašit ji nebo ji jinak ohrožit, a to za pomoci moderních informačních technologií (zejména pak internetu nebo mobilního telefonu)



Takže když mi na internetu někdo řekne, že jsem hloupá, je to kyberšikana?

Aby bylo možné hovořit o kyberšikaně, je nutné, aby byla oběť napadána cíleně a **opakovaně** jedincem nebo skupinou.



Kyberšikana má několik forem útoku. Mezi ty nejčastější patří:



Verbální útoky



Ztrapňování šířením fotografie, videa nebo zvukové nahrávky



Vyhrožování a zastrašování



Obtěžování vyzváněním nebo prozváněním



Krádež identity



Průnik na účet s cílem oběti ublížit, zesměšnit ji nebo ji dehonestovat



Vydirání



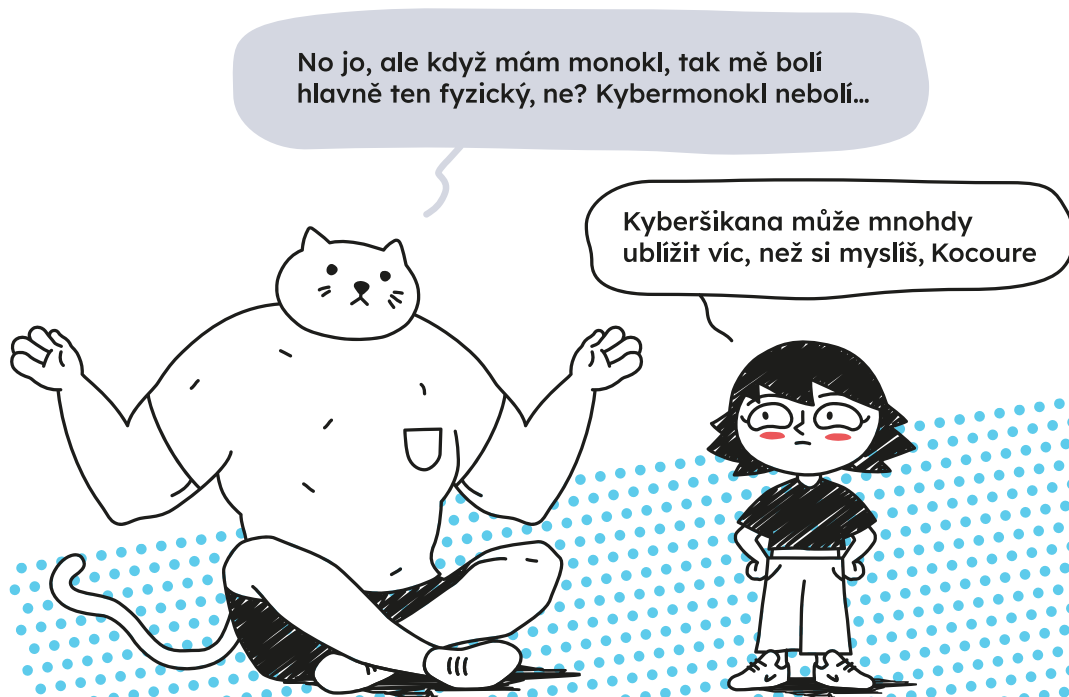
Stalking




Kyberšikana maže nepoměr sil mezi agresorem a obětí. Ve virtuálním světě mohou lidé využívat svoji anonymitu, komunikovat bez ohledu na svoje nedostatky (fyzické, psychické) a svoji převahu získávat technickou zdatností.

Kapitola 085 – Rozdíl mezi šikanou a kyberšikanou

Pokud víš o někom, kdo zažívá kyberšikanu, je pravděpodobně šikanovaný i fyzicky. Mnohdy je totiž kyberšikana spojená s klasickou šikanou, která zahrnuje například fyzické útoky, slovní nadávky, pomlavy nebo ponižování.



Na rozdíl od klasické šikany je mnohdy její virtuální forma čtenější, stupňuje se a oběť nemá šanci ji předvídat.



Už to chápu. Když jdu ze školy, tak asi vím, že dostanu přes kožich, ale na internetu nevím, kdy ten útok přijde.

Kapitola 086 – Kyberšikana jako nepovedený žert

Kyberšikana může začít na první pohled zcela nevinně. Třeba jako nepovedený vtip, sázka nebo jen obyčejné hecování mezi kamarády. Někdy se ale stane, že špatně odhadneš situaci a z obyčejné legrace to přeroste do pořádného průšvihů a velkého trápení.

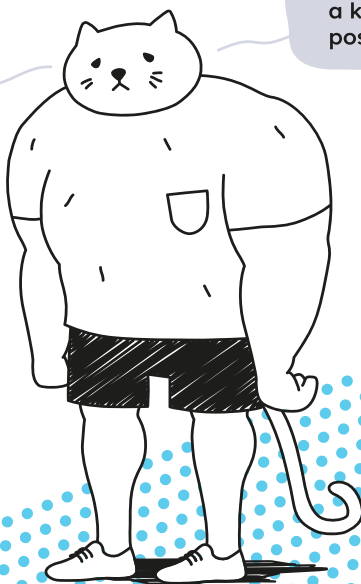


Každý máme jinak nastavenou citlivost. Co by tebe nerozházelo, může někomu jinému hodně ublížit. A víš, co je největší průšvih? Když to na začátku vypadá jako legrace, tak se k šikaně nakonec můžou přidat i ti, kteří by to jinak nedělali.

Vytvořil jsem fotomontáž Miciny, kde jsem jí přimaloval obří uši... (má je i tak velký)



Nechtěl jsem Micině ublížit, bral jsem to jako srandu a poslal jsem to do třídní skupiny...



Celá třída se tomu smála a kamarádi to ještě poslali všem do školy

Micina se tím moc trápila, nechtěla ani chodit do školy a všude si mě blokla. Fakt mě to mrzí, chci se jí omluvit hned, jak ji potkám.

Kapitola 087 – Kyberšikana „v dobrém úmyslu“

Mezi časté případy kyberšikany patří situace, kdy „budoucí“ oběť zveřejní v dobrém úmyslu na internetu video, vlog nebo jiný obsah, který se svým obsahem stane úspěšně virálním (v tom negativním smyslu slova). Autor obsahu se pak stává terčem posměšků, navíc s malou šancí smazat již rozšířené kopie videa.



Učím se jezdit na bruslích, moje první pády

200 tis. zhlédnutí

@Pepa1

Když neumiš bruslit, tak na ten led nelez!!!

👍 357

@KingOfTheBongo

Všimli jste si, že pokaždý, když spadne, tak se v ledu udělá díra?

👍 210

@BrnoGirlXoXo

Měla bys zhubnout a možná se na těch bruslích udržíš xDDD

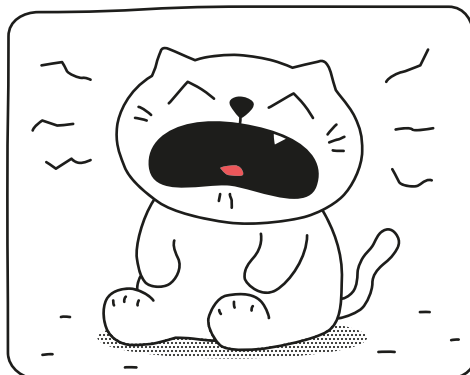
👍 87



Pamatuj si, na výhrůžné, vulgární nebo posměšné zprávy nereaguj! Někteří se tě budou snažit jen vyprovokovat a čekají na tvou reakci.

Kapitola 088 – Kyberšikana kvůli digitální stopě

Když přicházíš do nového kolektivu, třeba do nové třídy, chtějí spolužáci o tobě vědět víc informací. Může je napadnout si projít tvoje profily na internetu nebo profily tvých kamarádů a rodičů. Objevit tak mohou fotografie, které mohou být citlivé a kvůli kterým se můžeš stát obětí posměchu nebo kyberšikany.



První slůvka našeho chlupáčka
[#kocourek](#) [#nasemiminko](#)



K tomu, aby k podobným situacím docházelo co nejméně, je dobré pohlídat si svou digitální stopu. O tom jsme ti pověděli v kapitole 048-054.



Pokud se ti nějaký obsah, který je spojený s tebou, nelíbí, požádej jeho autory o jeho odstranění.

Kapitola 089 – Proč zrovna já?

Oběť kyberšikany nemusí být vybrána náhodně. Útočník si ji může vytipovat na základě jejího chování na internetu nebo ji může znát z reálného života. Podnětem pro kyberšikanu tak mohou být odlišné názory, chování, neúspěšný pokus o seznámení s obětí, ale také zveřejnění nějakého obsahu.

Zeptali jsme se těch, kteří v minulosti někoho šikanovali, proč to dělali:



Pamatujte si, nikdy na to nejste sami. Nebojte se svěřit!

✕ Linka bezpečí

Zavolej na Linku bezpečí. Je zdarma 24 hodin, 7 dní v týdnu na čísle 116 111
Když se necítíš na hovor, můžeš si s nimi chatovat nebo napsat e-mail

✕ Linka důvěry

Zavolej na číslo 241 484 149 nebo 777 715 215, využít můžeš také Skype hovor, chat nebo e-mail. Všechny kontakty najdeš na www.ditekrize.cz

Kapitola 090 – Když budu anonymní, nikdo mě neodhalí!

Pro mnohé útočníky je pocit určité anonymity spouštěcím faktorem. Falešný pocit bezpečí, pokud se schová za přezdívku (nick), předplacenou SMS kartu nebo e-mailový účet, může v útočnickovi posílit odvahu k využití nových metod a nárůstu agrese. Dobrou zprávou ale je, že jde útočníka vždycky dohledat, i když se schovává za falešné účty, předplacené karty nebo anonymní připojení.



Někdy to může vypadat, jako by ti psaly desítky lidí. Za mnoha účty ale může stát i jen jediný člověk.



Odesílatele zpráv si můžeš zablokovat v telefonu nebo přímo u operátora. Důležité je na tyto zprávy nereagovat. Když zachováš chladnou hlavu a dáš najevo, že tě útoky nerozházejí, brzy přestanou útočníka bavit.



Kapitola 091 – Verbální útoky



Ty jsi ale hloupá



A taky smrdíš



Huso!



Já nejsem osel, já jsem kocour!



Tak se všichni uklidníme



Škádlení a pošťuchování mezi kamarády,
kde jsou vyrovnané síly, není kyberšikana



Kdyby nadávky byly dlouhodobé, intenzivní, s cílem ti ublížit

Ne, ty jsi hloupej!



Ty smrdíš víc!



Osle!



To je snad ještě horší :D :D



Já se uklidňovat nebudu, Kocour mě šikanuje!



A kdy už by to byla kyberšikana?



Lidé mají právo vyjadřovat i své negativní názory. Je rozdíl mezi škádlením, jednorázovou agresí a intenzivním, opakovaným jednáním s cílem oběti ublížit. V každém případě dodrž následující postup:

Neodpovídej



Na ošklivé nebo výhrůžné zprávy neodpovídej. A to ani tehdy, pokud v nich útočník vyhrožuje, že něco zveřejní (třeba nějaké tajemství nebo citlivý obsah).

Vytvoř si důkaz



Umiš udělat screenshot? Když dostaneš podobné zprávy, vytvoř si důkaz. Ten pak můžeš ukázat kamarádům, rodičům nebo se s ním poradit v některé z poraden (jejich seznam nalezneš v kapitole 054).

Vlož si útočníka do ignore



Nikde není psáno, že se na internetu musíš bavit s každým. Zkus se podívat, jak na službě, kterou používáš, funguje ignore. Někdy stačí jen odesílatele umlčet na pár dní. Dej si ale pozor na to, když zvolíš trvalou blokadu. Po jejím zvolení se může smazat vše – zprávy i profil.

Zprávy si pro jistotu nemaž



Zprávy si nepromazávej a vytvoř si jejich kopii. Uchované zprávy pak můžeš někomu ukázat. Třeba i policii, kdyby se situace zhoršila.

Svěř se



Ta nejdůležitější rada na konec. I když můžeš mít pocit, že se už nedá nic dělat, vždycky ti může někdo pomoci!

Kapitola 092 – Rozliš, zda jde o kyberšikanu

Podívej se na následujících pět situací a zkus uhodnout, zda se jedná o kyberšikanu.



Kocour mi napsal, že jsem pihatej prcek!



Spolužáci si založili veřejný chat, kde o mně tvrdí, že jsem z útulku, a další lži a pomluvy!



Učitelka nám zakázala používat mobil v hodině!



Do recenze v e-shopu o mně napsali, že jsem nevýkonný a drahý křáp!



Chodí mi zprávy z několika cizích účtů a vyhrožují mi, že zveřejní moje tajemství. Už to trvá několik týdnů!

Kdo nesnáší Kocoura, tak se přidá!!!

● @Alfréd

Tuhle skupinu jsem založil, aby mohl každý říct Kocourovi, co si o něm myslí!

● @Kocka.Modroocka

Je to trapák. Pozval mě na rande a ani za mě nezaplatil tuňáka!

● @PanTlapka

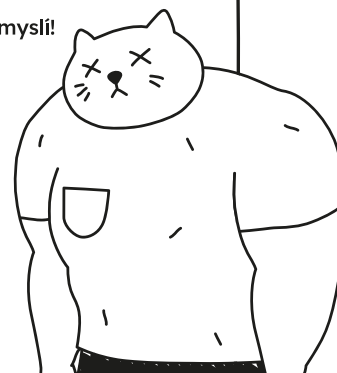
Slyšel jsem, že je z útulku...

● @MicinaxD

Určitě není papírovej jak já. Občejnej kříženec kocoura a prasete!

● @Zrzek066

Co kdybychom ho zabili?

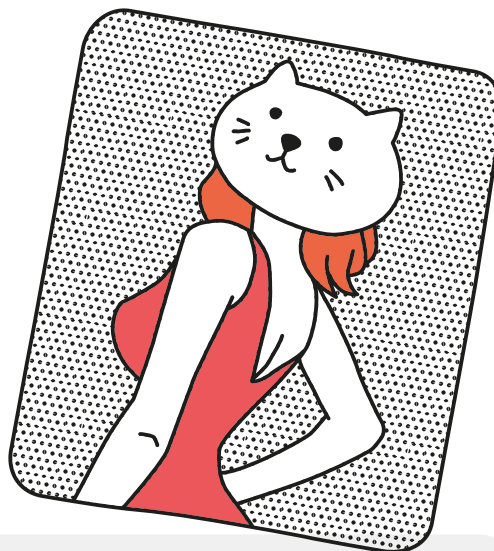


**Pokud uvidíš podobnou skupinu, nenech si to pro sebe.
Vytvoř si důkaz a někomu se svěř. Můžeš tím někoho
zachránit.**

Kapitola 093 – Ztrapňování šířením fotografie nebo fotomontáže

Co na začátku může vypadat jako legrace, se může časem zvrhnout v pořádný malér.

Představ si, že někdo vytvoří tvoji fotomontáž a pak to nasdílí do třídní skupiny. Nebo tě někdo vyfotí, když se převlékáš na tělocvik nebo jsi na záchodcích. Jde o jednu z forem kyberšikany a my tě naučíme, jak se bránit.



No, Kocoure, moc ti to sluší

Vůbec se mi to nelíbí, co mám dělat?

Už to viděla celá třída a bojím se, že se to dostane i do vedlejší třídy



Zachovej chladnou hlavu a dej najevo, že tě tato situace nerozhází
Slušně požádej tvůrce fotomontáže o odstranění

A když to neudělá? Já bych mu to nejradši nějak vrátil.
Mám vytvořit jejich fotomontáže?



To vůbec nedělej! Jestli se bojíš to řešit, zajdu za někým. Jsem ráda, že ses mi svěřil. Mám u tebe zmrzku!

Pokud se obsah nachází na nějakém veřejném serveru, kontaktuj jeho administrátora s žádostí o odstranění.



Kapitola 094 – Ztrapňování šířením fotografie nebo fotomontáže (příběh)

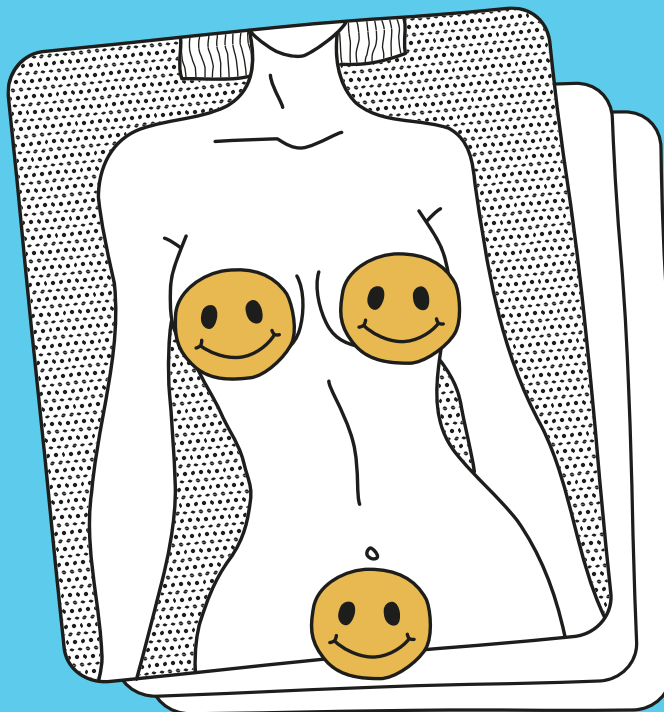
Přečti si jeden z příběhů, který se stal na základní škole.

Třináctiletá dívka (řijeme jí Jitka) se zamilovala do Pepy z vedlejší třídy. Ze začátku byla ostýchavá ho oslovit, proto mu nejprve lajkovala jeho příspěvky ve školní skupině na sociální síti. On si toho brzy všiml a napsal jí zprávu, ve které jí poděkoval. Začali si psát a trávili spolu psaním opravdu mnoho času. Čas od času si zašli ven a brzy přeskočila jiskra.

Jitka ale sportovala a její tatínek nebyl rád, že se s chlapcem schází, protože se její sportovní výkony zhoršily. Protože už se nemohli tak často vidat, rozhodla se Jitka svému chlapci posílat svoje fotografie, aby mu nebylo smutno. Protože do něj byla zamilovaná, ve slabé chvíli mu poslala i ty, na kterých byla nahá do půl těla. Její chlapec na ni naléhal a sliboval, že tyto fotografie nikomu nepoše. Také jí slíbil, že fotografie ihned smaže. To ale nedodržel a fotky si uložil mezi ostatní.

Jednoho dne začalo Jitce chodit velké množství zpráv, které byly posměšné, vulgární a jejichž mnoho autorů ani neznala. Začala pátrat, co se stalo, a objevila svoji nahou fotografii ve školní skupině, která byla pojmenovaná „Drby a úlovky z naší školy“. Okamžitě psala Pepovi, ale ten přísahal, že ji nikomu nedal.

Případ vyšetřovala policie, která zjistila, že se chlapci do telefonu dostali spolužáci, protože ho neměl uzamčený. Fotky i s vulgárním popiskem a Jitčíným číslem zveřejnili do této skupiny. I když byly fotky ze skupiny odstraněny, nikdo dodnes neví, kolik kopií fotek vzniklo.



Kapitola 095 – Ztrapňování šířením videa nebo zvukové nahrávky

Když vytváříš obsah na internetu, musíš počítat nejen s kladnou odezvou, ale také s tím, že ho může šířit nebo různě upravovat někdo další. Nemusí jít vždy o někoho cizího, dost často se stává, že za únikem obsahu může být tvůj blízký kamarád.



Pokud je obsah umístěný na veřejném místě, můžeš požádat administrátora stránky o vymazání. Pokud nebude stránka reagovat, můžeš se obrátit na specializovanou poradnu.



Audiohovory nebo videohovory si může druhá strana nahrávat. Dej si proto pozor, jaké informace sděluješ, a případně i na to, co ukazuješ. Informace o tom, co (ne)sdílet, nalezneš v kapitole 4. Nejvíc ti může ublížit obsah, který je citlivý. Přečti si o něm v kapitole 077 – Podvod s webkamerou.

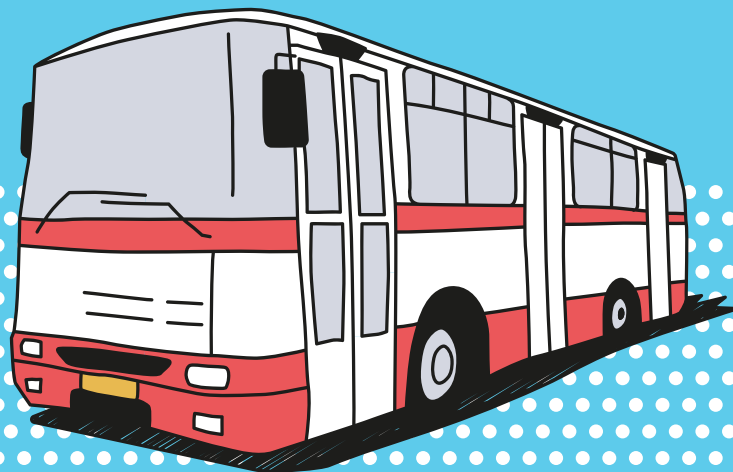
Kapitola 096 – Dívka z autobusu (příběh)

Na začátku byla jen touha se seznámit.

Elišce bylo deset let a vyrůstala v pěstounské rodině. K narozeninám si moc přála nový mobil. Ten, který doposud měla, dostala po své tetě. Uměl jen posílat SMS a byl pořádně těžký. Chtěla takový telefon, který umí nejen fotit a natáčet videa, ale hlavně se umí připojit k internetu. Ve třídě byla poslední, kdo ho ještě nemá, a spolužáci se jí občas kvůli tomu posmívali. K narozeninám ho skutečně dostala a byla z něj nadšená. Zkoušela si natáčet různá videa, která umísťovala na YouTube kanál.

Ze školy jezdila autobusem. Jen pár zastávek, ale vždycky se do autobusu těšila, protože v něm jezdil chlapec, který se jí líbil. Neznala jeho jméno, ani odkud je, ale byla do něj zamilovaná. Eliška byla trošku stydlivá a bála se ho oslovit. Když se vrátila ze školy, sebrala odvalu a natočila video, kde mu vyznala lásku. Chtěla, aby jí lidé pomohli s hledáním a napsali jí jeho jméno. Na konci videa pak zveřejnila svoje telefonní číslo.

Nedlouho poté, co video zveřejnila, se začalo virálně šířit, mělo dokonce několik set tisíc přehrání a lidé se jí vysmívali. Na uvedené telefonní číslo jí posílali stovky urážlivých SMS. Video si dokonce všimli youtubeři, kteří začali vytvářet parodie. Eliška musela kvůli kyberšikaně změnit telefonní číslo i školu. Tento příběh se stal před deseti lety, a videa jsou stále na internetu, i když se je Eliška moc snažila odstranit.



Kapitola 097 – Vyhrožování a zastrašování

Zná někdo vaše tajemství a vyhrožuje vám, že ho zveřejní? Nebo jste byli svědkem něčeho špatného a někdo po vás chce, ať to nikomu neříkáte? Anebo už jste se dostali do problémů na internetu, když jste si psali s někým cizím? Situací, kdy může dojít k vyhrožování nebo zastrašování, je opravdu mnoho.

Jak byste se zachovali, kdyby vám přišla podobná zpráva?



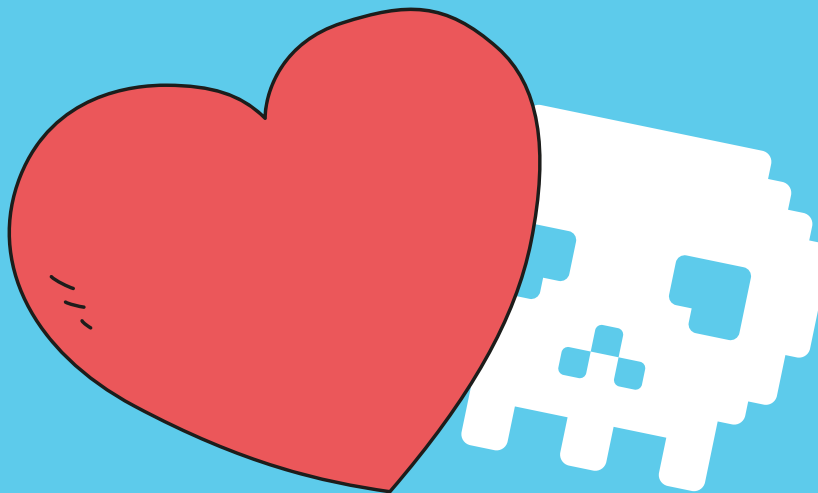
I kdyby ti ve zprávách vyhrožovali, chtěli okamžitou odpověď nebo ti dali určitý limit pro nějakou akci, neodpovídej. Svěř se někomu blízkému nebo se porad' na lince pomoci.

Kapitola 098 – Vyhrůžování a zastrašování (příběh)

Lucie a Karolína byly opravdu dlouho nejlepší kamarádky. Měly podobné zájmy, jezdily na skejtu, a ve škole seděly dokonce v jedné lavici. Lucie byla neřízená střela a čas od času si přilepšila tím, že své mamince ukradla nějaké peníze. Karolína to věděla, ale nechtěla svoji kamarádku prozradit, měla ji moc ráda.

V září přišel do jejich třídy nový spolužák Ondra, který se oběma líbil. Nejdříve si o něm jen povídaly, ale později si slíbily, že ani jedna s ním nebude chodit, protože by to rozbilo jejich přátelství. Uplynul nějaký čas a Karolína měla pocit, že se jí Lucie vyhýbá. Ve škole s ní moc nemluvila a už ani nechtěla chodit ven jezdit na skejtu.

Když se Karolína projížděla novou trasou po městě, uviděla svoji kamarádku, jak se s Ondrou vedou za ruce. Celou cestu domů byla Karolína smutná, a čím víc se blížila k cíli, i naštvaná. Jak jí to mohla udělat? Takhle to přece nenechá! „Jestli se s Ondrou nerozejdeš, tak se tvoje mamka dozví, že ji kradeš peníze!“



Jak byste vyřešili
tuto situaci?

Kapitola 099 – Krádež identity

Pokud budeš na internetu sdílet velké množství informací nebo budeš mít svoje profily na sociálních sítích přístupné i neznámým lidem, může se stát, že si někdo „vypůjčí“ tvoji identitu. Bránit se můžeš tak, že falešný profil nahlásíš.



Čas od času využij některý z nástrojů pro rozpoznávání fotek ke zjištění, zda se za tebe někdo nevydává. Třeba Google Lens nebo TinEye.



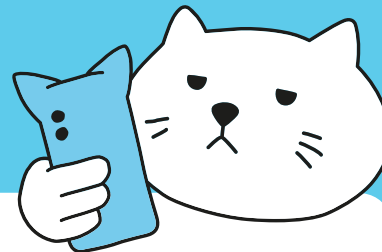
Nejlepší variantou je mít zamčený profil, přístupný pouze pro blízké. Když se ale rozhodneš mít profil veřejný, počítej s tím, že si obsah může stáhnout kdokoli. Nezobrazuj na něm citlivé věci. Více se dozvíš v Části 4 – Sdílení obsahu na internetu.

Kapitola 100 – Krádež identity (příběh)

Světлана měla mnoho účtů na sociálních sítích se stovkami sledujících. Trávila na nich většinu dne tím, že se jim snažila zprostředkovat svoje každodenní zážitky. Byla to docela náročná práce, protože postování začalo už ráno fotografií z postele s popiskem „Nový den je tu“ a pokračovalo pravidelným streamem cestou do školy. Denně Světлана vyprodukovala desítky storiček a fotek. O víkendu pak dělala speciální live stream, ve kterém nechala běžet kameru se záběrem na to, jak spí.

Bylo pro ni velkým překvapením, když jí začalo psát několik lidí s tím, že je ubohý fejk, který se jen za někoho vydává. Vůbec nechápala, co se děje, a začala pátrat po tom, co se stalo. Objevila svoje fotky na profilu dívky, která se jmenovala Kristýna. Pod fotkami měla dokonce příspěvky lidí, kteří tvrdili, že ji znají a chodí s ní do školy. Ale v jiném městě.

Kristýna byla ve skutečnosti muž, který ukradl Světlaně identitu a pod falešným profilem lákal z chlapců jejich fotografie.



Postování/Postnout

odeslat/publikovat příspěvek (např. na sociální síti)

Storičko/Storýčko

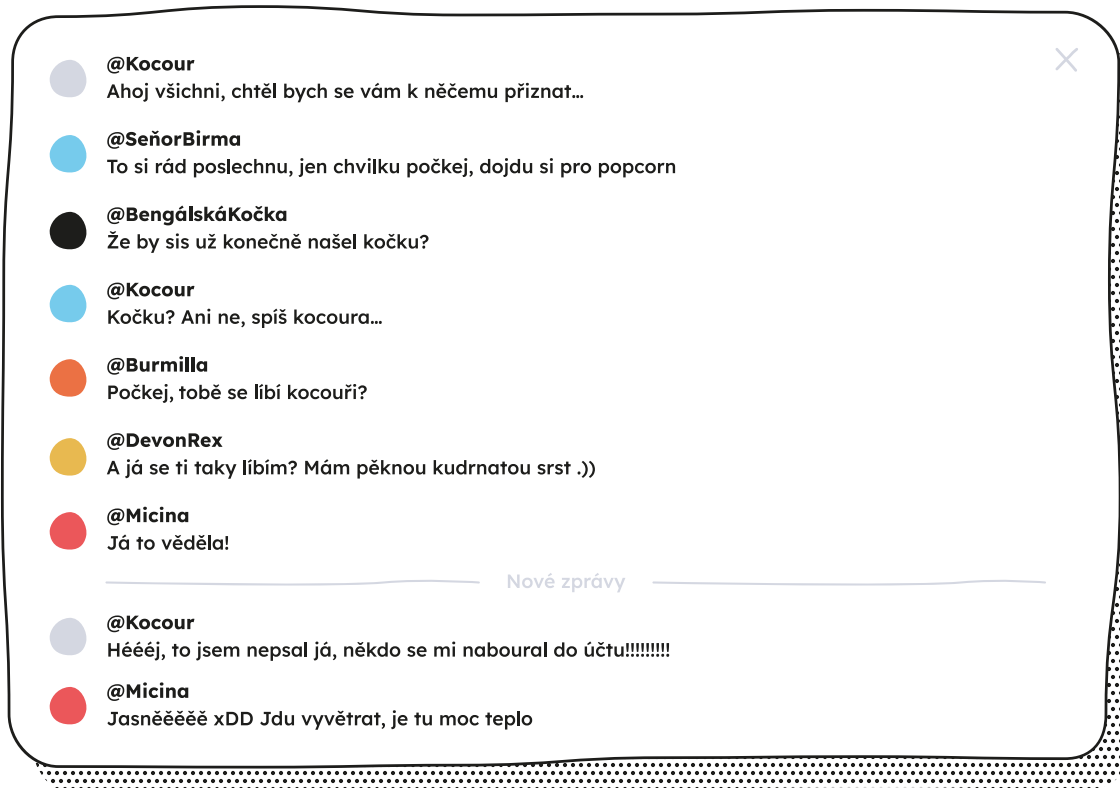
příspěvek v podobě fotografie nebo videa, který zůstane, dokud ho nesmažete, zveřejněný na vašem profilu



Co dělat, když narazíš na fejk?
Přečti si kapitulu 063.

Kapitola 101 – Průnik na účet s cílem oběť zesměšnit

Svoje účty nebo telefon byste měli poctivě chránit. Pokud se do nich někdo dostane, přijde velice snadno k citlivým informacím. Nebo může účet zneužít a vydávat se za vás, což nemusí být zrovna příjemné.



Nejčastější cesta, jak se ti někdo dostane do účtu, je skrze nezabezpečený mobilní telefon. Jak si ho zabezpečit, to najdeš v Části 2 – Ochrana mobilního telefonu.

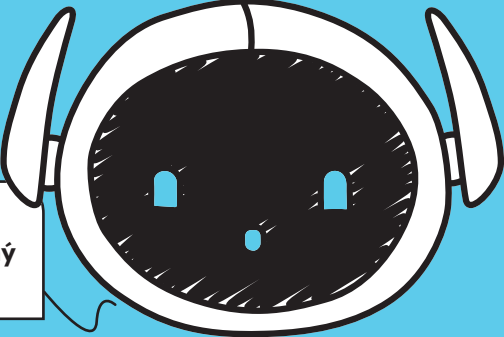
Kapitola 102 – Průnik na účet s cílem obět' zesměšnit (příběh)

S kyberšikanou se setkávají i dospělí, přečti si příběh o výpovědi z práce.

Jsem zaměstnaný sedm let ve firmě, která vede účetnictví firmám. Často jezdím na služební cesty, kde prezentuji zákazníkům svoji práci. Jednou se mi stalo, že se mi někdo naboural do mých účtů a změnil mi všechna přístupová data. Možná jsem se jen připojil na chvílku na nezabezpečenou Wi-Fi, ale teď se nedostanu ani na e-mail, ani na žádnou sociální síť. Nevím, co mám dělat, mám tam spousty fotek, ale i konverzace se svojí manželkou nebo šéfem.

Minulý týden se mi stalo, že někdo mým jménem z e-mailu odeslal výpověď mému nadřízenému. Ten to vzal nejspíš vážně, protože jsem měl již vyklizený stůl, když jsem přišel do práce. Ve dveřích jsem ho potkal a on jen utrousil, že měl o mně lepší mínění a že jsem za ním měl přijít dřív, když jsem s ním měl problém. Vysvětlil jsem mu to a snad pochopil, že si ze mě jen někdo udělal legraci.

Horší to ale bude s mou manželkou, té jsem údajně napsal na sociální síti, že ji podvádím a že se chci rozvést. Vůbec netuším, kdo za tím stojí a komu všemu jsem „já“ ještě napsal.



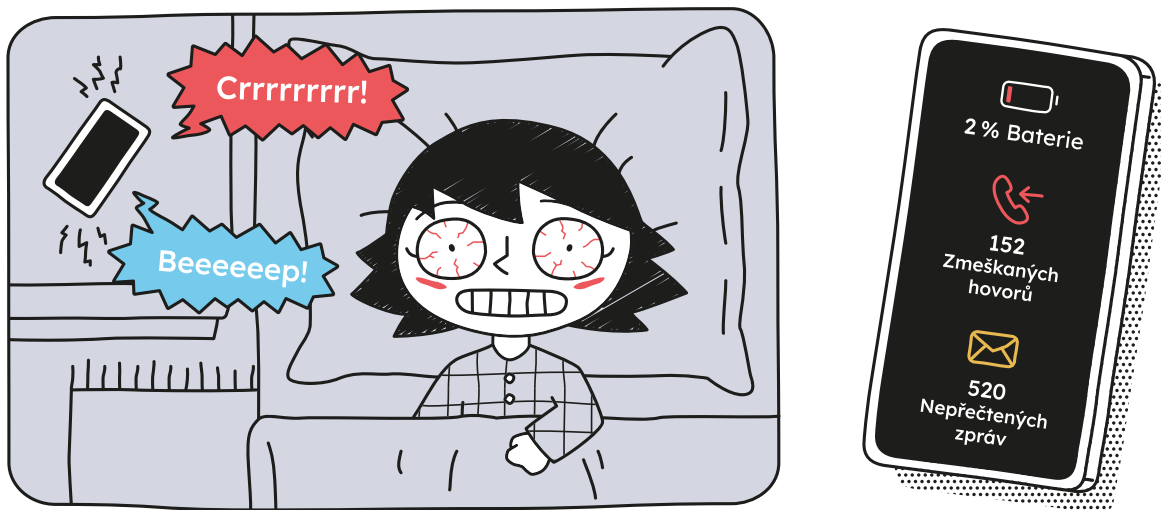
Neoprávněný přístup
k cizímu účtu je trestný
čin.



Dokážeš si představit, co dalšího by se mohlo stát a do jakých situací se můžeš v případe zneužití účtu dostat?

Kapitola 103 – Obtěžování prozváněním

Některé formy kyberšikany nemusejí na první pohled vypadat tak nebezpečně. Pokud ale nebudeš záležitost řešit okamžitě, může se situace změnit.



V nastavení telefonu si můžeš upravit, kdo všechno ti může psát a volat. Můžeš si nastavit i různé typy režimů. Telefon ti pak omezí upozornění na zprávy nebo volání. Když nepomůže omezení nastavené v telefonu, neváhej se obrátit na svého operátora.



Někdy může za intenzivní prozvánění jen legrace kamarádů. Nikdy to ale nepodceňuj, někdy může být útočníkem nějaký stalker.

Kapitola 104 – Obtěžování prozváněním (příběh)

Na sociální sítě moc nechodím, nemám na ně kvůli svému koníčku moc čas. Jezdím totiž závodně na koni a trénink mi zabere většinu dne. V okrese na závodech většinou vyhrávám. Na druhém místě je za mnou vždycky Adéla, která mě už musí nenávidět. Taky bych nechtěla být pořád druhá.

Možná to byla ona, možná někdo jiný, ale od minulého měsíce mi telefon jen vyzvání a chodí mi stovky zpráv. Když už se to nedalo vydržet, začala jsem pátrat po tom, kde je moje číslo uvedeno. Jeden z těch volajících mi řekl, že mám inzerát na seznamce. Druhý mi zase napsal, že prodávám levně auto, a třetí, že někde nabízím přívýdělek.

Když jsem si vyhledávala svoje číslo na internetu, našla jsem desítky různých inzerátů. Snažila jsem se inzeráty odstranit a zablokovala si hovory z cizích čísel. Na chvíli mám klid, ale zajímalo by mě, komu ležím v žaludku...



Já bych si vsadil na Adélu

Kapitola 105 – Vydírání

Vydírání nebo jiná, podobná forma nátlaku je nejnebezpečnější forma kyberšikany. Dost často vzniká z důvodu, že na nás ví útočník nějaké citlivé informace nebo obsah. S nějakou formou nátlaku nebo s vydíráním má zkušenost 7 % dětí.



Zachoval se Kocour správně?

Každý děláme chyby. Pamatuj si, pokud jsi obětí vydírání, že máš vždycky pravdu, i když ti pachatel tvrdí, že s ním spolupracuješ. Nikdy nepodléhej výhrůžkám a nenech se vydírat. Každá situace, i ta zdánlivě bezvýchodná, se dá vyřešit.



**Vydírání je trestné podle
§ (paragrafu) 175 trestního
zákoníku.**

Kocour se nezachoval správně. Ani když ti útočník vyhrožuje časovým limitem, neodpovídej. Udělej si screenshot a někomu se svěť. I když to bude vzhledem k citlivosti obsahu náročné. Uvědom si, že útočník může vydírat další oběti. Tvoje odvaha je může zachránit!

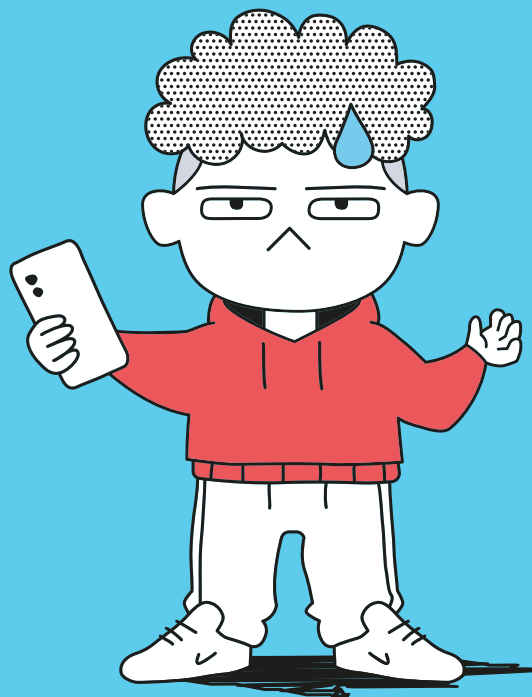
Kapitola 106 – Vydírání (příběh)

Na internetové seznamce jsem se seznámil s hezkou slečnou, která bydlela ve vedlejší městě. Protože na profilu neměla moc fotek a informací, napsal jsem jí, jestli by mi nenapsala něco o sobě a také neposlala víc fotek. Za dva dny jsem dostal zprávu i s fotkami. Ty byly ve spodním prádle, ale to mi vůbec nevadilo, protože byly opravdu nádherné. Abych nezůstal pozadu, poslal jsem jí také svoje polonahé fotografie.

Netrvalo dlouho a začali jsme si psát, plánovali jsme společné setkání a mě napadlo, jestli bychom si nemohli poslat i nějakou intimní fotku. Tím myslím úplně nahou. A to byla obrovská chyba. Poslal jsem sérii fotek jako první. Bylo na nich vidět úplně všechno. Dlouho se nic nedělo, ale pak mi přišla zpráva „Jestli nepošleš další nahé fotky do večera, tak vše, co jsi poslal, zveřejním na internetu“. Báł jsem se, že fotky zveřejní, a proto jsem jí nafotil další podle jejího přání. Před chvílkou mi přišla další zpráva „Máš deset minut na to, poslat mi svoji nahou fotku ze sprchy“.

Poradte mi, co mám dělat.

Matěj (14 let)

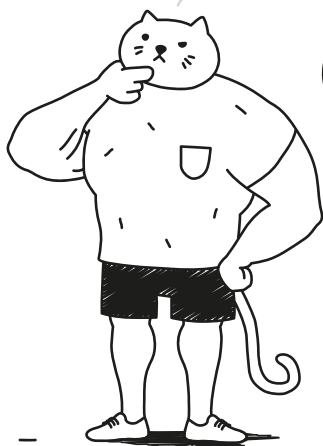


Co by měl Matěj udělat?
Poradíš mu?

Kapitola 107 – Nechtějí mě ve třídní skupině (digitální ostrakizace)

Určitě to znáš, máš pár dobrých kamarádů, povídáte si a možná máte nějakou společnou skupinu na WhatsAppu nebo v jiném kecálkovi. Co když má ale společnou skupinu celá třída, a tebe tam nechtějí? Jde o formu kyberšikany, kterou nazýváme digitální ostrakizace.

Ostra, Ostrov, Ostrekovat... To ani neumím vyslovit



Ostrakizace! Kocoure, kolik ti je, ty ani neumíš přečíst jedno slovo...



Ostrakizace znamená, že je oběť vyloučena z nějaké komunity, kam by měla nebo chtěla patřit.



Vyloučení z kolektivu není trestný čin, spíš to naráží na hranu slušného chování. Pokud máš s ostrakizací (i tou digitální) zkušenost, pověz o tom učitelům nebo rodičům. Nezapomeň, že ti mohou pomoci i profici z poraden na internetu.

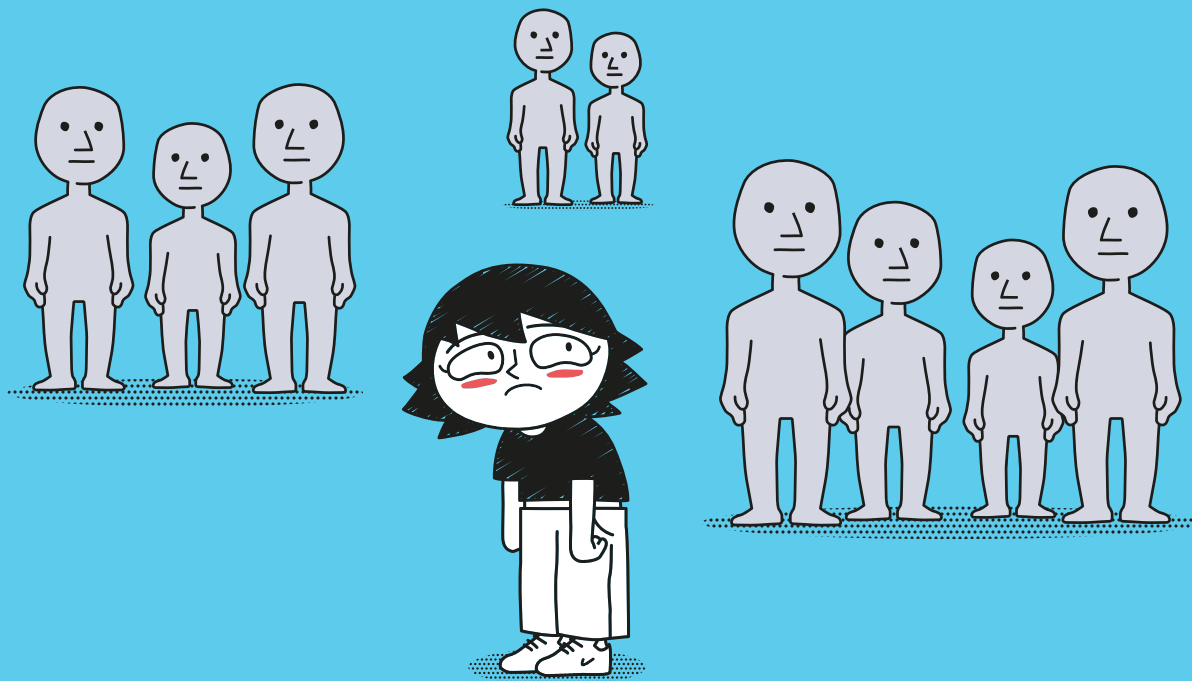


Pokud je někdo vyloučený ze skupiny, stává se z něj pohledu skupiny outsider. To může způsobit ztrátu dalších kamarádů, kteří se s ním mohou bát kamarádit, protože by se také mohli stát vyloučenými.

Kapitola 108 – Vyloučení z kolektivu (ostrakizace) příběh

Příběh z poradny:

Dobrý den, jmenuji se Zuzka a začala jsem chodit do páté třídy. Přestoupila jsem z naší malé vesnické školy a nikoho v naší třídě neznám. Bohužel se se mnou nikdo nebaví. O přestávce jsem zaslechla, jak si o mně šeptají spolužačky nějaké pomluvy. Taky jsem zaslechla, že jde celá třída odpoledne na nějakou oslavu a že místo a čas je ve třídní skupině. Já ale v žádné nejsem, nikdo mě tam nechce přidat, a dokonce dělají, že žádná neexistuje. Co mám dělat?



Dokážeš si z paměti vzpomenout na číslo Linky bezpečí? Měla by na něj Zuzka zavolat? Nebo máš jiné řešení, jak se z této nepříjemné situace dostat?

Kapitola 109 – Stalking

Za stalking lze považovat opětovné, systematické, dlouhodobé obtěžování nevyžádanými zprávami různého typu, telefonáty nebo i opakované cílené pronásledování. Obsah zpráv nemusí být urážející, může být příjemný, veselý, ale také zastrašující. Útočník u oběti vyvolává pocit strachu.

Moc se mi líbíš, pořád se dívám na tvoje fotky

Ještě se neznáme, ale už teď mi moc chybíš

Víš, že jsem tě včera viděl, jak jdeš ze školy?

Jestli mi neodepíšeš, tak si ublížím!

Jsi tam???

Proč se s ním bavíš, a se mnou ne?

Ty mi vážně nebudeš odepisovat?

Odpovíš mi konečně?

Napsal jsem ti za večer 100 zpráv, a ty ani jednu?

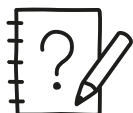
Kdy už natočíš nové video? To minulé jsem viděl snad tisíckrát!

Kdo je na té nové fotce? Proč se nechceš fotit se mnou?

Těším se, až tě zase zítra uvidím jít do školy!

Prosím, odepiš!!!

Včera večer jsem tě viděl online a neodepsala jsi mi!



Dokážeš na internetu zjistit, od jakého roku je stalking trestný v České republice?

Kapitola 110 – Stalking (příběh)

Tonda moc rád točil a stříhal videa, všechen volný čas věnoval přípravám scénářů a natáčení. Jeho kamarádi ho povzbuzovali, aby si založil veřejný kanál, na kterém by je zveřejňoval. Tonda ve svých videích vtipně popisoval život ve své rodině, komentoval aktuální kauzy z internetu a také dvakrát týdně zapíнал live stream pro své fanoušky.

Brzy měl na svém profilu sto tisíc sledujících, kteří ho povzbuzovali, aby streamoval častěji, a posílali mu i donáty. Lidé Tonda začali poznávat na ulici a občas chtěli autogram. Ze začátku to bylo příjemné, občas selfie s nějakým fanouškem, někdy podpis, čas od času i pozvánka na nějakou party.

Později se Tonda musel vyrovnat i s lidmi, kteří čekali před jeho domem a psali mu i ošklivé zprávy. Obzvláště vytrvalá byla jeho fanyнка Míša, která chodila na všechny jeho akce a měla pocit, že je Tonda součástí jejího života. Protože se jí nedostávalo takové odezvy, rozhodla se ho pronásledovat a zasílala mu stovky zpráv. To, kam chodí do školy, kde bydlí, jaké má číslo telefonu, i to, kde se nacházel, zjistila na internetu. A tak se rozhodla...



Donátovat

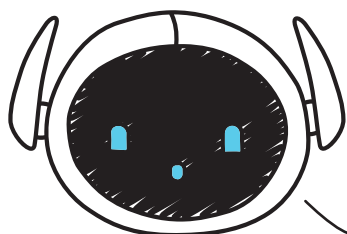
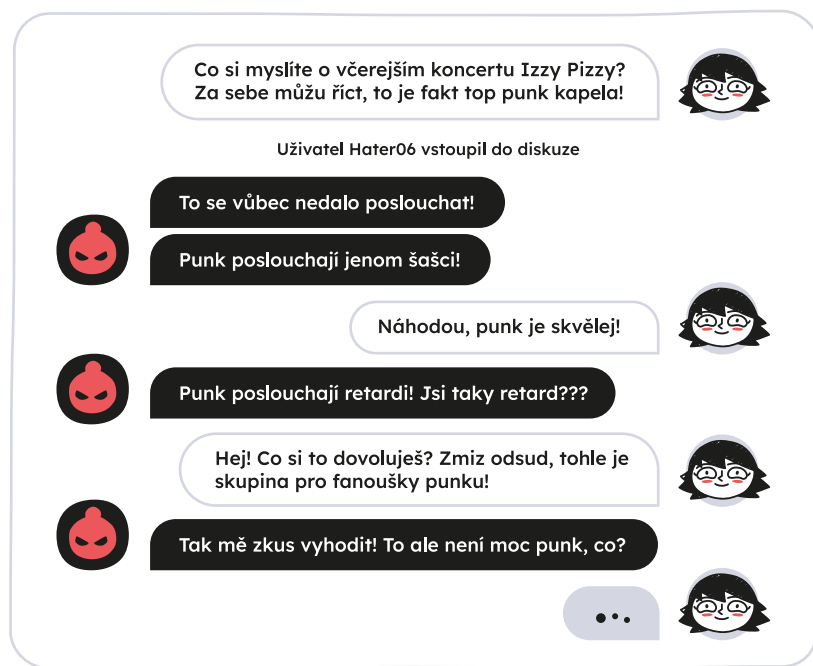
Podporovat, sponzorovat,
příspěvat na tvorbu



Příběh by mohl pokračovat a mohl mít několik konců. Jaký by mohl být dobrý konec?
Mohl dopadnout příběh i špatně?

Kapitola 111 – Trolling

Potkali jste někdy na internetu člověka, který rád provokuje, hádá se nebo někoho zesměšňuje? Tito lidé ve vás záměrně vyvolávají touhu na příspěvky zareagovat. Na to přesně čekají a baví je to. Může jít o jednotlivce nebo o organizovanou skupinu.



Troll (či trol) je v internetovém slangu účastník online diskusních fór, chatů či blogů, který začíná hádky, provokuje čtenáře na internetu a rozsévá neshody tím, že zveřejňuje záměrně provokativní, urážlivé nebo irelevantní (off-topic) příspěvky k citlivým tématům.

Kapitola 112 – Trolling (příběh)

Smutný příběh Michala K.

Michal chodil na střední průmyslovou školu. Bavily ho počítače, fyzika a vše okolo elektrotechniky. Jednoho dne se u něj v průběhu hodiny na škole projevila duševní choroba. Proskočil skleněnou výplň okna. Byla mu diagnostikována celá řada poruch, včetně schizofrenie, dostal mnoho léků a uzavřel se ve svém domově.

Z Michala se stal podle jeho okolí podivín a lidé se mu snažili vyhýbat. Kontakt s lidmi mu ale scházel, a proto se rozhodl s nimi komunikovat přes internet. Založil si YouTube kanál a začal pravidelně vysílat. Možná kvůli svému vzhledu a projevu si brzy získal pozornost tisíců lidí, kteří ho různě zesměšňovali. Michal to ale tak nevnímal a snažil se na jejich popichující zprávy slušně odpovídat.

Odpovídáním lidem strávil denně víc než osmnáct hodin, ale neuvědomoval si, že si z něj dělají jen legraci. Jeho nemoc, množství užívaných léků a špatná životospráva patrně stály za jeho úmrtím. Jeho „fanoušci“ si neuvědomovali, že utýrali psychicky nemocného člověka, a vtipy na jeho osobu kolují na internetu dodnes.



Pod názvem „Záznam divadelního představení #jsi_user“ ho nalezneš na internetu. Zajímavostí je, že 99,9 % textu v inscenaci tvoří autentický přepis mezi trolly a Michalem.



Víš, že byl Michal první český youtuber, a zároveň první oběť závislosti na internetu?

Kapitola 113 – Je kyberšikana trestná?

Slovo „kyberšikana“ český trestní zákoník nezná. To ale neznamená, že některé její projevy trestné nejsou. Třeba vydírání, stalking nebo neoprávněný průnik na účet trestné jsou.



To jsem z toho jelen. Tak je to trestné, nebo není?

Slovo kyberšikana sice v zákoníku není, ale je tam řada paragrafů, kterých se může týkat:

- § 175 Vydírání
- § 181 Poškození cizích práv
- § 182 Porušování tajemství dopravovaných zpráv
- § 184 Pomluva
- § 187 Pohlavní zneužívání
- § 345 Křivé obvinění
- § 353 Nebezpečné vyhrožování
- § 355 Hanobení...
- § 356 Podněcování k nenávisti...
- § 357 Šíření poplašné zprávy
- § 364 Podněcování k trestnému činu
- § 365 Schvalování trestného činu
- § 404 Projev sympatií k hnutí směřujícímu k potlačování práv a svobod člověka

...a mohl bych pokračovat



O výši trestu rozhoduje soud. Například za přečin vydírání hrozí trest odnětí svobody na šest měsíců až čtyři léta nebo peněžitý trest.

Kapitola 114 – Obrana proti kyberšikaně

Některé situace mohou působit bezvýchodně. Když ale dodržíš pár zásad, situaci určitě vyřešíš.

1

Řeš vzniklou situaci okamžitě.
Na nic nečekej!

2

Na vulgární, útočné nebo výhrůžné zprávy rozhodně nereaguj.

3

Kontaktuj technickou podporu služeb, kde se závadný obsah nachází, a žádej jeho smazání.

4

Pokud tě kontaktují neznámí lidé a obtěžují tě, vkládej si je do ignorace, nezvedej cizí čísla.

5

Snaž se působit klidně a v případě posměchu dávej najevo, že ti daná situace nevadí.

6

Svěř se blízké osobě (kamarádům, rodičům nebo učitelům) a popros je o pomoc.

7

Pokud se budou útoky stupňovat, je dobré mít důkaz (zálohu, screenshot...), můžeš se obrátit na specializované poradny.

8

V některých případech se můžeš obrátit na policii.

Nezapomeňte, nikdy na to nejste sami.
Každá situace má řešení!



Kapitola 115 – Filmy a seriály ke kyberšikaně

Poslední kapitoly nebyly zrovna veselé. O kyberšikaně se špatně mluví a mnohdy je potřeba velký kus odvahy se někomu svěřit. Je ale lepší na to nebýt sám. Zkus se podívat na filmy nebo seriály, které ti téma kyberšikany ukážou prostřednictvím příběhů jiných lidí.



#Martyisdead

Úspěšný český seriál o kyberšikaně. Hlavním hrdinou je Marty, který byl obětí kyberšikany a vydírání.



13 důvodů proč (13 reasons why)

Americký seriál o kyberšikaně. Tajemství. Lži. Pomsta. Na Liberty High mají všichni co skrývat... A pravda už má brzo vyjít na světlo.



Teror na síti (Cyberbully)

Casey čelí nejhorší noční můře každého teenagera. Anonymní hacker hodlá zveřejnit její soukromé fotografie na internetu a ona svádí boj s časem, aby mu jeho plány překazila.



Na hory

Příběh o tom, co dětem může způsobit obyčejné brouzdání po internetu. A jak může rodičům změnit život.



Hashtag

Seriál o jedné střední škole, partě spolužáků a jednom hashtagu, který mezi nimi všechno změnil.

Na filmy a seriály se sice můžete podívat sami, ale lepší je to s kamarády, rodiči nebo se na ně můžete podívat i ve škole.



Máš mladšího kamaráda nebo sourozence?

Těm nejmenším jsou určeny Kyberpohádky nebo projekt ON-LINE ZOO.

Kapitola 116 – Testíček

**Zkus si udělat malý test z vědomostí o kyberšikaně.
Dokážeš odpovědět na následující otázky?**

Pokud mě někdo začne urážet a opakovaně napadat, co udělám?

- A/ nenechám si to líbit a oplatím mu to
- B/ zavolám policii
- C/ svěřím se rodičům, učiteli nebo kamarádům a budu to řešit

Je kyberšikana trestným činem?

- A/ protože toto slovo není uvedeno v zákoně, tak se to neřeší
- B/ některé její projevy jsou trestné
- C/ není, na internetu můžu lidem ubližovat

Která z následujících činností není kyberšikana:

- A/ škádlení na sociální síti
- B/ vydírání
- C/ ztrapňování šířením fotografie, videa nebo audionahrávky

Co je kyberšikana?

- A/ pokud mě někdo fyzicky napadá
- B/ kyberšikana je pouze jiný název pro šikanu, jinak je to naprosto totéž
- C/ chování, jehož záměrem je oběť vyvést z rovnováhy, ublížit jí, zastrašit ji nebo ji jinak ohrožit, a to za pomoci moderních informačních technologií

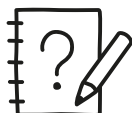
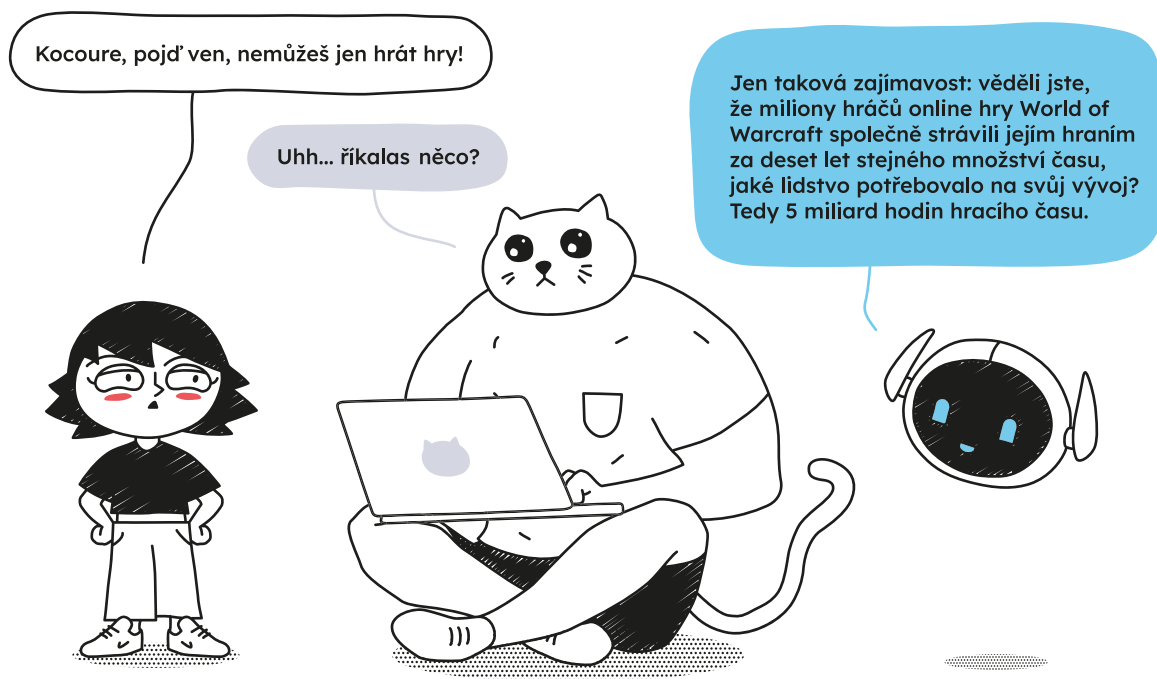


Část 8

Rizika spojená
s hrami

Kapitola 117 – Online hry

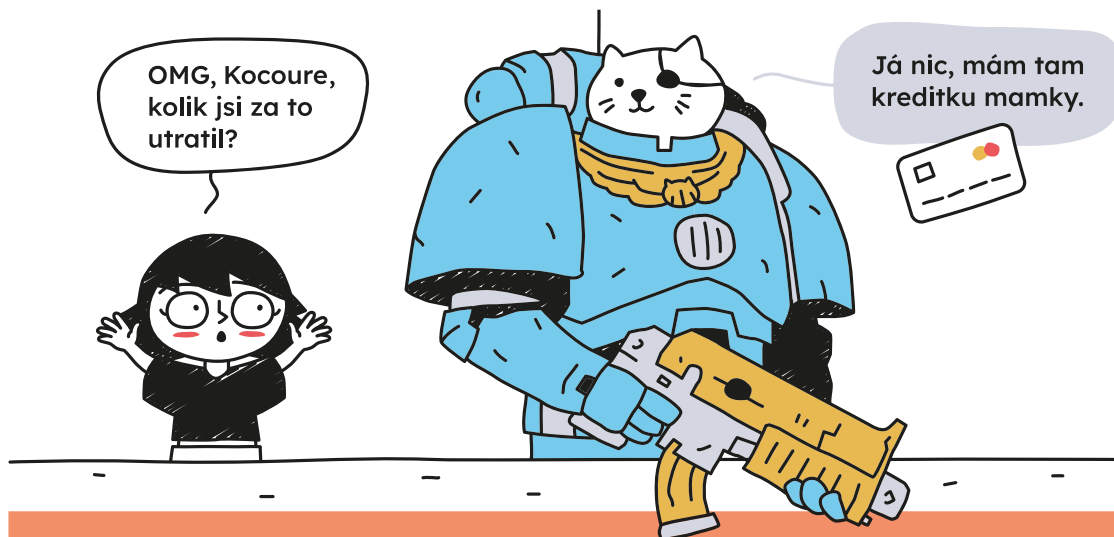
Hraní her je skvělá věc, při které se můžeš zabavit nebo si odpočinout. Je vědecky dokázáno, že některé hry mohou rozvíjet kreativitu, vnímání i schopnost rozhodování. Zjistilo se ale také to, že násilné videohry mohou pozměnit mozkové funkce už po pouhém týdnu hraní.



Hraješ hry?
Které jsou tvoje nejoblíbenější?

Kapitola 118 – Loot boxy

Pokud hrajete online hry, nejspíš jste narazili na loot boxy. Ty jsou ve hrách velmi oblíbené a většinou obsahují nějakou odměnu. Může jít o skin, předmět, herní měnu a další předměty, které si můžete ve hře i napřímo zakoupit.



Nevýhodou loot boxů je ale to, že nevíme, co je uvnitř ukryto, velkou roli zde hraje náhoda. Některé virtuální bedýnky jsou časově omezené nebo jsou označovány podle jejich exkluzivity. To nás může nutit je mít, s vidinou, že budeme mít něco, co ostatní hráči nemají, nebo že si můžeme prodejem vydělat nějaké peníze

Znáte to vzrušení z otevírání těchto předmětů? Někdo si na něm může vybudovat závislost stejně jako na výherních automatech.

Jakou máte zkušenost s loot boxy?
Získali jste někdy obsah, který byl vzácný?



Kapitola 119 – Krádeže herních účtů

Podvodníci na internetu kradou hesla nejen k účtům na sociálních sítích nebo k e-mailům, ale také k hráčským profilům. Některé z nich totiž mohou obsahovat něco cenného.



Vůbec nechápu, jak se může prodat nějaká virtuální věc za tolik peněz...



Protože s ní pak můžu flexit!



No a někdo to má jako investici. Dá se tím vydělat balík!



Věděla jsi, že majitel nejdražšího skinu do hry CS:GO za něj dostal nabídku přes 32 milionů korun?

Tak to si raději ten svůj účet pořádně ochraň, nebo ti ten tvůj zlatý dráp někdo ukradne!



\$ 1.500





Jak si zabezpečit účet si přečteš v Části 1 – Hesla a zabezpečení.



Flexit – vychloubat se nebo machrovat

Kapitola 120 – Čas strávený online

Jak vypadá tvůj den? Kolik hodin času trávíš ve škole, spaním, při volnočasových aktivitách nebo věnuješ zábavě na internetu?



Netolismus – závislostní chování na „virtuálních drogách“. Jde o nadměrnou aktivitu na internetu (sociální sítě, nakupování, sázení, hraní her apod.). Pokud těmto aktivitám věnuješ čas na úkor spánku nebo odpočinku, může jít o první příznaky.



Svůj čas strávený online můžeš ohlídat přes různé nástroje. Nezapomeň, že je dobré jej vyvážit nějakými jinými aktivitami, například sportem nebo jinými koníčky.

Kapitola 121 – Esport

Kdo si hraje, vydělává. Je tomu ale opravdu tak? Profesionální esportovci si mohou skutečně vydělat velké množství peněz. Musejí tomu ale obětovat spoustu času a svůj online trénink musejí vyvažovat jinými aktivitami.



Rozhodla jsem se, že budu slavná

A můžu se zeptat, v čem?



Budu hrát hry a vydělám si balík peněz

Jako Prší nebo Dámu?



Kocoure, nedělej si srandu, zjistila jsem, že mám na hry talent. Na Farmě už mám level 1.563!

To ale není esport



To nikdy nevíš, jednou budu určitě na olympiádě!

Jasně a vyhraješ bramborovou medaili



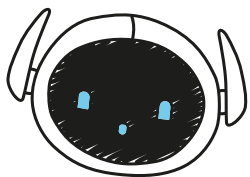
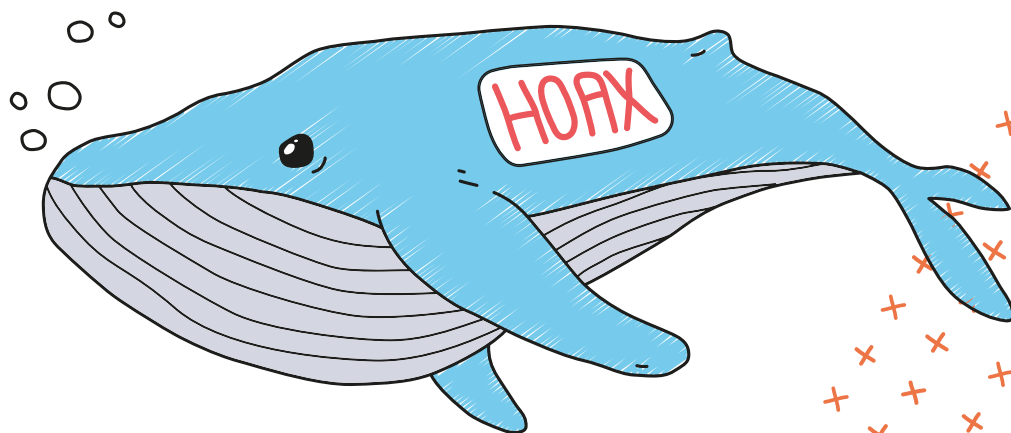
Esport je zkratka pro elektronický sport. Jde o organizované soutěžení hráčů nebo týmů, v jakékoliv hře, na jakékoliv platformě (PC, konzole, mobil).



Sleduješ nějaké streamy z hraní her nebo turnajů?
Baví tě esport?

Kapitola 122 – Modrá velryba

Hra Modrá velryba se v minulosti masově šířila mezi uživateli sociálních sítí a podle legendy měla prostřednictvím administrátorů (kurátorů) nutit děti plnit destruktivní úkoly. Brzy se ale zjistilo, že jde o vymyšlenou zprávu.



Hra Modrá velryba byla největším hoaxem v historii České republiky. O hoaxu jsme si povídali v kapitole 043.



Je důležité si ověřovat informace na internetu. Jak na to, se dozvíš na internetu ve videích od Kovyho. Vyhledej si „Kovyho mediální ring“.

Kapitola 123 – Online výzvy (Online challenges)

Různé typy výzev, sázek nebo hecování jsou s námi od počátku lidstva. Lidé se vždy v něčem předháněli a dělají to i dnes, jen se část těchto aktivit přesunula na sociální sítě. Bezhlavé napodobování online výzev může být velmi nebezpečné.



Která z těchto výzev je nebezpečná?

Spolkní lžici skořice

Vyfoť svoje rodiče, jak spí

Nalij si alkohol do očí

Přejdi se zavázanýma očima silnicí

Dej si na kůži sůl a na ni polož led

Dej na internet fotku z první třídy a označ pět dalších lidí, kteří ji musejí také zveřejnit

Vypij půl litru mléka na ex

Strč ruku do mraveniště

Stůj pět minut v ohni

Nech si tělo pevně oblepit lepicí páskou a pak se z ní pokus vyprostit

Spolkní chilli papričku

Každý den, sedm dní v týdnu, v 7:00 udělej sto kliků



Ice Bucket Challenge byla online výzva, při které si dotyčný na hlavu vyléval kbelík ledové vody se záměrem zvýšit povědomí o amyotrofické laterální skleróze. Virálnost výzvy měla za cíl podpořit výzkum této vzácné nemoci.



Ne každá online výzva je nebezpečná.

Před tím, než ji začneš plnit, si zjisti co nejvíce informací a zvaž rizika.

Kapitola 124 – Kocourovo desatero bezpečného hraní online her



Zkus si při hraní online her pohlídat pár věcí:

1

Hlídej si čas trávený hraním her, nehraj na úkor svého spánku, odpočinku nebo povinností.

2

Hraj jen hry, které odpovídají tvému věku, podívej se na PEGI rating.

3

Když s někým ve hře nechceš komunikovat, nemusíš.

4

Dávej si pozor! I v online hrách je prostor pro kyberšikanu nebo predátory.

5

Stahuj a hraj jen hry z ověřených zdrojů. Hry také mohou obsahovat viry!

6

U mobilních her si omez příjem oznámení v časech, kdy nechceš nebo nemůžeš hrát.

7

Když se ti nebude dařit, hru vypni.

8

Svoje herní účty si pořádně zabezpeč! Obsahují mnoho cenného.

9

Neutrácej velké množství peněz za loot boxy, dají se získat i zdarma.

10

Když se budeš cítit nepříjemně, neboj se obrátit na specializované linky pomoci.

Ale ze všeho nejdůležitější je vyvážit čas online nějakou fyzickou aktivitou.



Kapitola 125 – Závěrem

I když jsme tě upozornili na hodně rizik, internet a technologie jsou opravdu skvělé věci.



Všechno dobré se dá zneužít.
Jako to pořekadlo s ohněm.
Internet je dobrý sluha,
ale špatný pán.



Nikdy nezapomeň na to, že na ty
zlé věci nikdo není sám. Neboj se
svěřit, a když nebudeš vědět,
jak postupovat, napiš nám!



Linka bezpečí – zavolej na bezplatné číslo **116 111** (kdykoli) nebo chatuj na www.linkabezpeci.cz

Hotlinka STOPonline.cz – zde můžeš anonymně nahlásit závadný obsah,
který hotlinka rychle odstraní www.stoponline.cz

Linka důvěry – svěř se se svým problémem, www.ditekrize.cz, Rizika kyberprostoru (telefon **778 510 510**)

Poradna Napiš nám – když si nebudeš vědět rady, www.napisnam.cz

Sleduj náš **Instagram** [@no_net_drama](https://www.instagram.com/no_net_drama)

Strážci na internetu

Martin Kožíšek

Za tuto publikaci odpovídá pouze její autor.

Evropská unie nenese odpovědnost za jakékoli využití informací v ní obsažených.

Vydavatel:

CZ.NIC, z. s. p. o.

Milešovská 5, 130 00 Praha 3

Edice CZ.NIC

www.nic.cz

1. vydání, Praha 2024

Kniha vyšla jako 32. publikace v Edici CZ.NIC.

ISBN 978-80-88168-73-7

Tisk: Iva Vodáková – Durabo, Na Stráni 1301, 250 88, Čelákovice

Ilustrace: Jan Štěpánek

Grafický design a sazba: Michaela Spilková

Editor: Zuzana Krotílová

© 2024 Martin Kožíšek

Toto autorské dílo podléhá licenci Creative Commons BY-ND 4.0 (<https://creativecommons.org/licenses/by-nd/4.0/>). Dílo však může být překládáno a následně šířeno v písemné či elektronické formě, na území kteréhokoliv státu, za předpokladu, že nedojde ke změně díla a i nadále zůstane zachováno označení autora a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Překlad může být šířen pod licencí CC BY-ND 4.0.



Spolufinancováno
Evropskou unií

cz.nic | SPRÁVCE
DOMÉNY CZ

