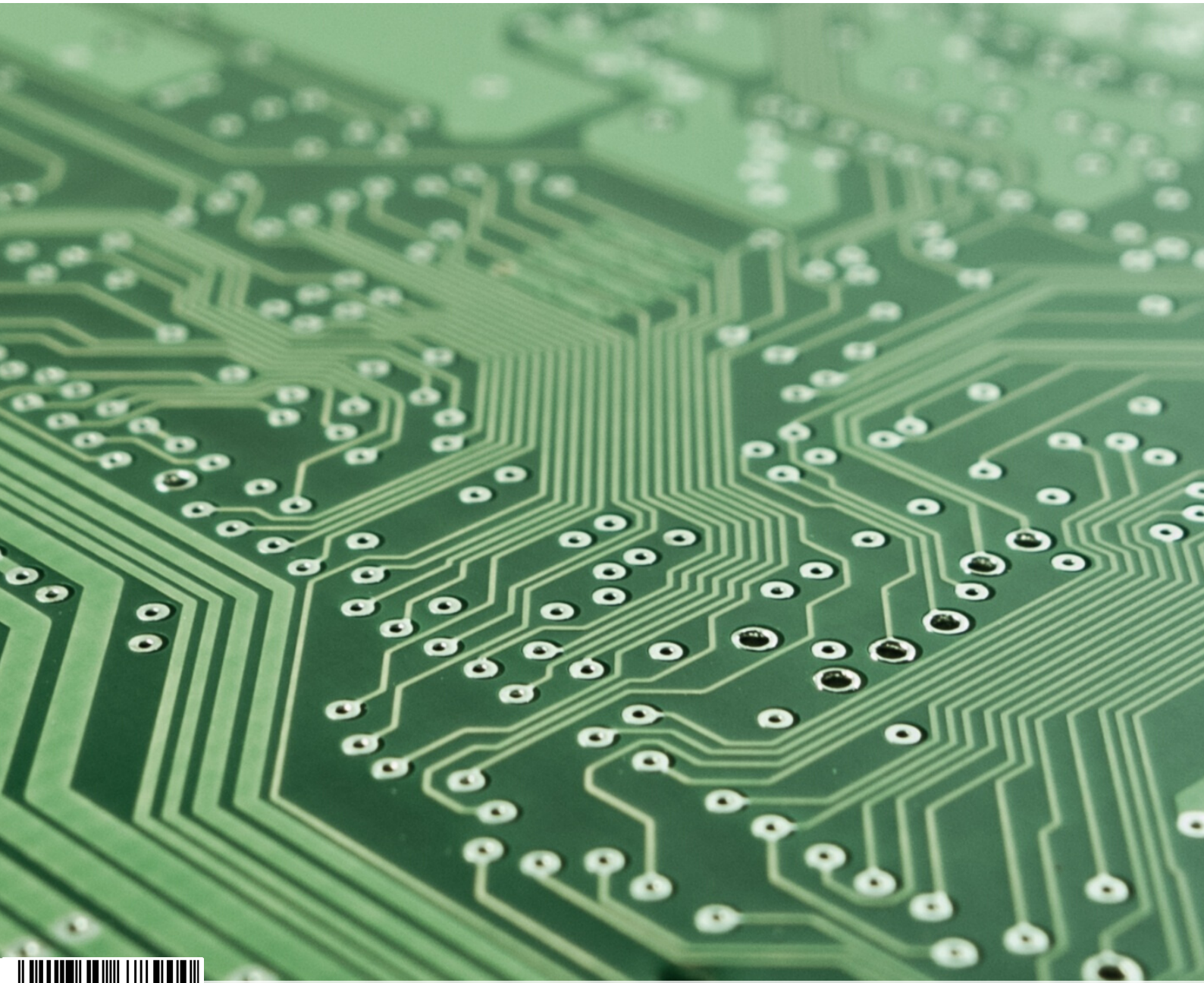
KVĚTEN 2020 | Č. 11
KČ 60,-

intervědomí



JAK SE NEZPEČNĚ CHOVAT NA INTERNETU/TIPY A RADY

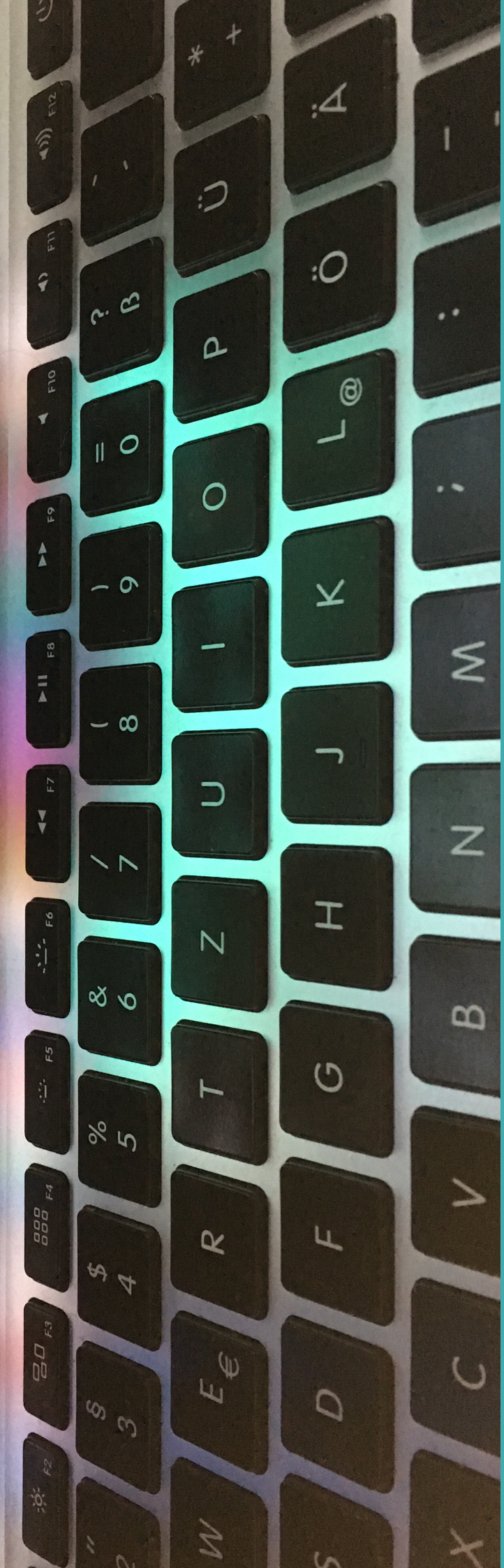
5 012345 678900

VÁŽENÍ ČTENÁŘI,

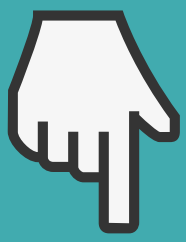
vítáme Vás u dalšího dílu časopisu Intervědomí. Tento díl časopisu jsme zaměřili na bezpečné chování na internetu. Jelikož věříme, že je v dnešní době velice důležité být informován a mít základní znalosti o tomto tématu. Myslíme si, že by tyto znalosti, měl mít každý, kdo se na internetu nějakým způsobem pohybuje, a proto prosíme o rozšíření tohoto čísla.

Vynález internetu je rozhodně pozitivní věc pro naše lidstvo. Už nemusíme chodit do knihoven, půjčovat si knihy a hledat v nich, abychom se dozvěděli o tématu, které nás zajímá. Dnes už stačí zapnout počítač, notebook, chytrý telefon či televizi, napsat dané téma a informace máte rovnou před sebou. Ale s internetem přichází také nebezpečí, ať už jsou to hackeři, kybešikana, viry. Špatné zabezpečení našich zařízení, může dokonce ovlivnit naše životy, či stavy bankovních kont. A proto jsme pro Vás připravili tento měsíc číslo tomuto věnované. A byste mohli v klidu trávit čas na internetu.

Redakce časopisu Intervědomí Vám přeje příjemné čtení.



OBSAH



SLOVNÍK
ZÁKLADNÍK POJMŮ

Hacker/cracker	člověk, který proniká do počítačů s úmyslem zničit data, vyřadit síť nebo získat citlivé informace
Pořítačový virus	program, který se spustí na vašem PC bez Vašeho svolení. Některé viry Vám pouze znepříjemňují život. Většina virů ale získá kontrolu nad vaším počítačem a provádí destruktivní akce
Firewall	software nebo hardwarové zařízení, které filtruje příchozí i odchozí komunikaci do vnitřní sítě. Zjednodušeně si funkci můžeme představit jako stráže vstupu do pevnosti, které rozhodují o tom, koho pustí dovnitř a ven
Adware	zobrazuje nevyžádanou reklamu, banery, časem zaplaví váš přístroj vyskakujícími okny
Malware	typ škodlivého softwaru, hackeři ho používají k získání osobních údajů, hesel nebo peněz nebo snižuje výkonnost počítače
Ransomware	zašifruje všechny data na počítači, hacker po oběti požaduje výkupné
Social Engineering	ukradení nebo vytvoření kopie účtu na sociálních sítích
Keylogger	zaznamenává vše, co píšete na klávesnici, i hesla!
Physing/rybaření	získání Vašich citlivých osobních informací, hesel, údajů o platebních kartách, rodných čísel nebo čísel bankovních účtů
Trojský kůň	vir, díky kterému může hacker sledovat, co na svém počítači děláte

CO NA NÁS NA INTERNETU ČÍHÁ

SEPSALI JSME PÁR JEVŮ, KTERÉ NÁS NA INTERNETU MOHOU POTKAT, JESTLIŽE SI NEBUDEME HLÍDAT NAŠE OSOBNÍ ÚDAJE.

Kyberšikana

Druh šikany, při které prostřednictvím elektronických médií, jako je internet a mobilní telefony dochází k záměrnému agresivnímu poškození uživatele těchto médií. Aktéry kyberšikany jsou Agresor – Oběť – Přihlížející.

OBĚŤ

Mezi nejčastějšími oběti kyberšikany patří děti a teenageři, které jsou odmítány kolektivem z důvodu osobní charakteristiky, jako je plachost, stydlivost, nejistota, fyzické atributy. Existují případy, ve kterých se sám agresor stane obětí, a to v případech, kdy se takto jeho oběť mstí nebo se proti jeho chování zvedne nepřiměřený odpor na internetu ze strany dalších lidí.

AGRESOR

Agresorům kyberšikany je společná nižší míra empatie v porovnání s ostatními dětmi, jelikož se neumějí vcítit do oběti a chápat, jaké zranění způsobují. Agresor svou oběť nevidí a nezná její reakce, tudíž nedokáže odhadnout, jak velkou újmu by ji mohl způsobit.

PŘIHLÍŽEJÍCÍ

Existuje několik druhů přihlížejících. Někteří jsou následovníci agresora, někteří jsou nezúčastnění a někteří jsou na straně oběti. Role těchto přihlížejících je velmi důležitá, pokud proti kyberšikaně otevřeně vystoupí, to se ale ve většině případů bohužel nestává.

Kyberstalking

Pronásledování v kyberprostoru nejčastější pomocí SMS, chatu, emailu, telefonu, sociálních sítí, Skypu apod. Oběti většinou pronásledovatele (stalkera) znají, často jde o bývalého milence/milenku, kamaráda, zrazeného přítele nebo milovníka. Stalker může být ale i neznámý, a to v případě, že si oběť vyhlédl náhodně na internetu. Pronásledované oběti hrozí naprostá ztráta soukromí, osobních údajů a pocitu bezpečí. Typickými příklady taktik kyberstalkerů mohou být:

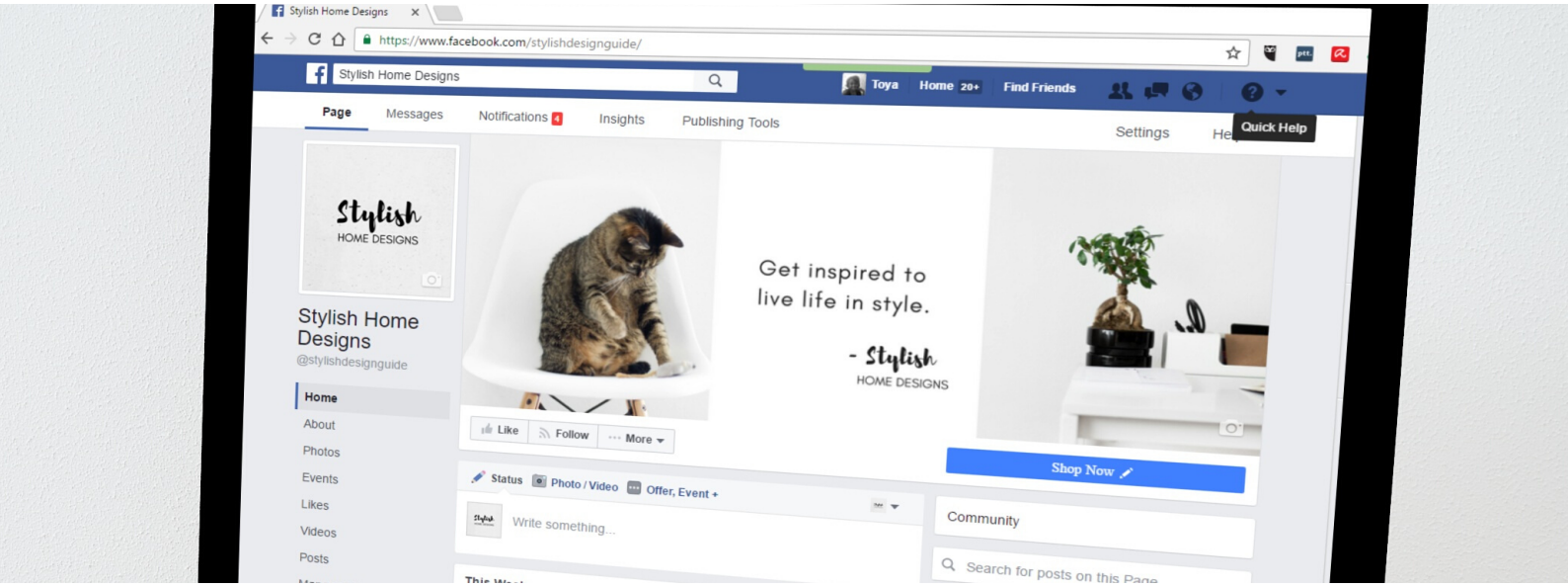
- posílání manipulativních, výhrůžných, obscénních nebo obtěžujících e- mailů
- nabourání se do on-line účtů oběti a změna nastavení nebo hesla
- vytváření falešných účtů na sociálních sítích a seznamkách, vydávání se za oběť nebo snaha o navázání kontaktu s obětí pod falešnou identitou
- zveřejňování soukromých informací o oběti na internetu například ve formě inzerátu (výsledkem je obtěžování mnoha lidmi, kteří si příspěvek přečetli)
- zneužití profilu oběti na sociálních sítích (získání informací, nabourání se do účtu atd.)
- monitorování e-mailové komunikace oběti nebo narušení e-mailové komunikace oběti zahlcením schránky nežádoucími e-maily nebo viry

Kyberharašení

Za kyberharašení lze označit opakované zprávy zasílané agresorem, které jsou oběti nepříjemné. Tato situace může vzniknout i ze vzájemné konverzace, ta se stane nepříjemnou a oběť není schopná ji ukončit. Agresor většinou oběť začne bombardovat zprávami ihned po připojení na internet nebo jí zasílá nežádoucí SMS.

Spam

Spam nebo také spamming lze nejjednodušeji vysvětlit jako zasílání nevyžádané elektronické pošty (email, messenger apod.). Jedná se o masové rozesílání e-mailů s převážně reklamním sdělením, avšak s příchodem diskusních fór a různých messengerů spamming přechází i na tyto kanály. Jedná se o masové zasílání reklamního sdělení, nikoliv o cílené. Všem těmto nebezpečím ze většinou předejít právě tím, že uživatel včas u emailové komunikace rozezná, že se jedná právě o SPAM, zprávu neotevře a ihned ji smaže.



Flaming - trolling

Jde o nepřátelské chování útočníka vůči oběti ve virtuálním světě. Je to výrazně vyhrocená a agresivní diskuze až hádka na internetu. Někteří uživatelé úmyslně podobné diskuze provokují vkládáním různých kontroverzních příspěvků, urážením účastníků diskuzí apod. Výzkumy ukazují, že slovní napadání je ve virtuálním prostředí až čtyřikrát častější než v reálném životě.

Flamer úmyslně vnáší do internetových diskusí vulgarismy a úmyslně napadá jiné uživatele. Své útoky vůči ostatním uživatelům, jež mají jiný názor, stupňuje, někdy eskalují až výhrůžkami.

Jak se bránit? V tomto případě zní rada jednoduše – daných diskusí se neúčastnit nebo v nich dále nepokračovat.

Sexsting

Zasílání textů, fotografií a videí a se sexuální tématikou prostřednictvím elektronických médií. Tyto materiály pak často končí na internetu a můžou mít pro oběť fatální důsledky, jelikož jsou často použity jako prostředek k vydírání. Některé případy mohou skončit až smrtí oběti. Útočník se v případě, že je oběť mladší 18 let, dopouští trestné činnosti v oblasti šíření dětské pornografie.

Rizika: Potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít. V případě zveřejnění citlivého materiálu na internetu je prakticky nemožné tento materiál „smazat“ – může být zneužit i po velice dlouhé době od zvěřejnění. Trestní odpovědnost za šíření sexstingu.

JAK SE CHRÁNIT NA INTERNETU?

Každou chvíli můžeme sledovat únik osobních fotografií slavných jmen. Policie dennodenně zaznamenává případy odcizení peněz prostřednictvím internetu, a když si k tomu připočtete, kolik zařízení už chytilo ransomware, tedy virus, který doslova žádá výkupné, jinak vám vymaže celý obsah harddisku, tak zjistíte, že všechna ta varovná oznámení o kvalitním zabezpečení skutečně nejsou na škodu. I když si myslíte, že vám se nic podobného stát nemůže, dávejte si pozor a přečtěte si několik dobře mířených rad pro bezpečnější surfování na internetu.

JEDEN WEB - JEDNO HESLO A ŽÁDNÉ UKLÁDÁNÍ

V posledních letech se stále více společností spravujících desítky milionů hesel přiznalo, že jejich servery a datová střediska byly úspěšně napadeny. Ano, drtivá většina těchto informací je zašifrována, a tedy pro crackera zbytečná, ale vyskytly se i případy, kdy hesla nebyla dostatečně kryptovaná a uživatelům hrozily problémy, zvláště pokud totéž heslo využívali na dalších ne-li všech webech. Facebook, Instagram a další služby se snaží kradená hesla co nejdříve vypátrat, porovnat a upozornit daný účet na nebezpečnou shodu, ale i tak bystesi měli pro každý důležitější registrační formulář vybírat jiné, ideálně nijak spolu nesouvisející heslo. Upozorňovat na kombinaci malých, velkých písmen spolu s čísly snad nemusíme.

SAMOSTATNÁ KREDITNÍ KARTA PRO ONLINE PLATBY

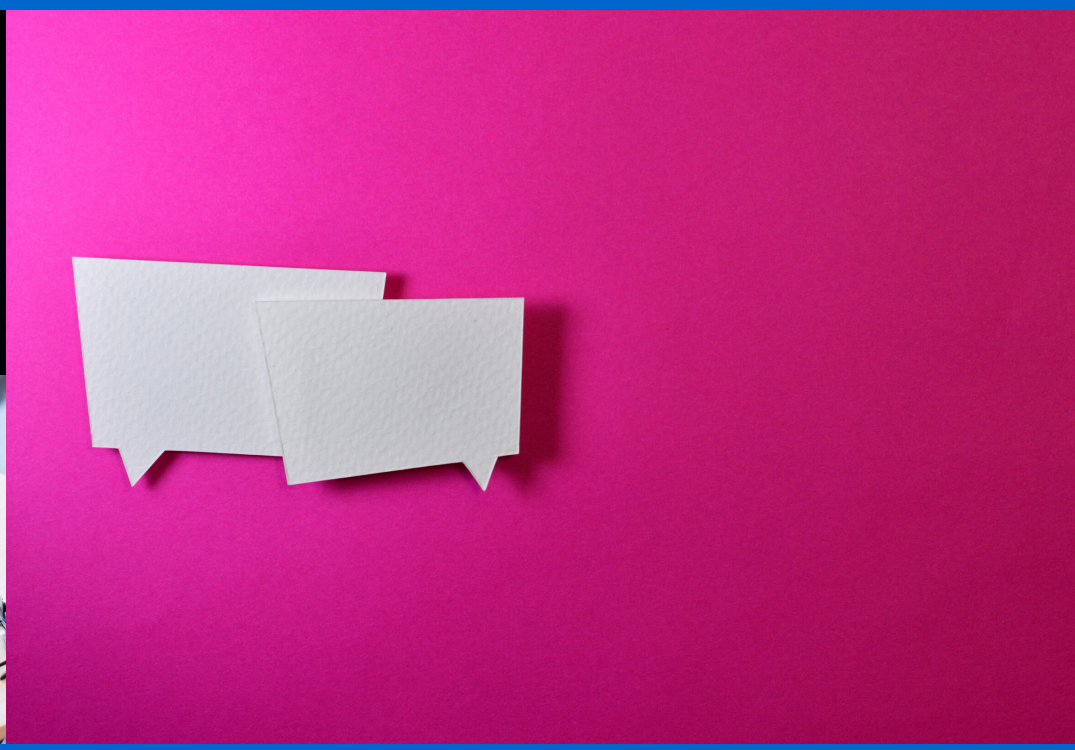
Spořit si finance na bankovním účtu a zároveň stejným účtem platit na internetu je do jisté míry riziko. Především, pokud zadáváte údaje z platební karty všude možně a nebojíte se ukládat informace o kartě na webech (pro pohodlnější a rychlejší platby bez nutnosti opakovaného zadávání).
Ideálním řešením je v tomto případě pořízení kreditní karty, která nebude provázána s vaším účtem a na rozdíl od debetní karty z ní nebude možné vybírat peníze po přečerpání. Při platbách si pokaždé všímejte, zda má daná stránka šifrování (zelený zámek) a pokud si stále nejste jisti, prověřte si daný web přes Google zadáním názvu webu a známého slovíčka „scam“.

NIKDY NEOTEVÍRAT PODEZŘELÉ ODKAZY!

Když už jsme v úvodu nakousli ten Ransomware, v listopadu 2016 obletěla svět informace o rozšíření škodlivých obrázků na Facebooku, které automaticky zablokovaly váš počítač po otevření konkrétní stažené fotografie. Pouze jediné kliknutí tak dokáže odpálit všechny vaše údaje. Statistika mluvící o napadení virem za rok 2015 ukazuje, že proběhlo 3,8 milionu útoků. Šílené číslo jen zdůrazňuje, jak jednoduše lze využívat zvědavosti a nevědomosti uživatelů ve svůj prospěch. Prosíme vás, neklikejte, nestahujte a neotvírejte nic, o čem nejste 100 % přesvědčeni, že je bezpečné. Ušetříte si kopec starostí.

ZABEZPEČENÍ KONVERZACÍ

Snad všechny sociální sítě zaměřené na chatování, tedy Messenger, Viber, Whatsapp či Google Allo, aktuálně disponují možností konverzovat prostřednictvím end-to-end šifrování. Konverzaci můžete vidět pouze vy a osoba, se kterou komunikujete. V případě WhatsAppu, Viberu a Google Allo je end-to-end šifrování aplikováno na všechny chatovací okna, na Messengeru ho lze využívat jen pomocí tajných konverzací. Po tom, co zprávy odstraníte, ať už ručně nebo destrukčním časovačem (Messenger), je nelze žádným způsobem získat zpět. Ani vy, ani Facebook. Samozřejmě, teoreticky je možné i takovou komunikaci rozšifrovat, avšak klidně by to mohlo trvat i několik let.



DVOUFÁZOVÁ AUTENTIFIKACE

Důvěra v přihlašování „jen“ jménem a heslem nemusí být natolik velká jako v případě použití dvou faktorů. Přeci jen, vždy jste o něco klidnější, když se přihlašujete do internet-bankingu jméno heslem a kódem z SMSky nebo jiným doplňkovým způsobem. Může to být například otisk prstu nebo klíč nahraný na externím zařízení (USB). Možností je mnoho a je jen na vás zkontrolovat si daný web, či neposkytuje uživatelům přihlašování přes dvoufaktorovou autentizaci. Vpřípadě Facebooku najdete takovou formu přihlašování v Nastavení -> Bezpečnost -> Setting Up Extra Security.

AKTUALIZUJTE MOBILNÍ ZAŘÍZENÍ

Nejednou se stává, že nejnovější aktualizace mobilního operačního systému v sobě skrývá kritickou díru, kterou vás může třetí strana s lehkostí napadnout. Pokud zahlédnete na internetu článek o objevení podobné chyby, zbytečně neváhejte a bezprostředně po příchodu aktualizace (určitě vás na ni upozorní notifikace) ji nainstalujte. Aby Google zajistil co možná nejvíce neprůstřelný software, odměňuje nálezce softwarových chyb částkami až do výšky několika desítek tisíc dolarů. Hledat chyby se jednoznačně vyplatí.

ZÁLOHUJTE SI DATA

Na závěr rada, kterou většina uživatelů podceňuje. Zejména v posledních měsících řádí ransomware stále více a nemyslete si, že vám se něco takového přihodit nemůže. Požadavek několika stovek až tisíců korun za odblokování celého obsahu počítače může být pořádný škrt přes rozpočet, avšak s vlastnictvím aktuální zálohy počítače na externím úložišti vám může být nějaký virus ukradený a přeinstalací operačního systému spolu s formátováním disku se ho jednoduše zbavíte. Nezanedbávejte zálohu důležitých dat.

ŠIFROVANÝ EMAIL

Věděli jste, že Google, Microsoft nebo Yahoo v rámci zlepšování cílené reklamy spolu s dalšími důvody mají přístup k obsahu vašich mailových schránek? Ne, že by reálné někdo seděl za obrazovkou a četl si vaše osobní zprávy a prohlížel fotografie z dovolené, ale pokud si chcete být 100 % jisti, že veškerá vaše mailová komunikace je bezpečně zašifrovaná i před správci serverů, využijte někteří z bezplatných šifrovaných emailů, například ProtonMail. Kromě webové verze nechybí ani ty mobilní, ať už jste na Androidu nebo iOS. V případě, že odesíláte zprávu na prostý mail, můžete si vybrat, zda adresátovi přijde pouze odkaz na šifrovanou zprávu spolu s nutností zadat heslo nebo půjde o běžnou, nekryptovanou zprávu.

VYUŽÍVÁNÍ VPN SÍTĚ

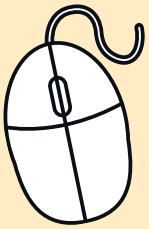
Přistupovat na internet z veřejných, často nezajištěných sítí, může mít v krajních případech fatální následky na vaši bezpečnost. Pokud by byl na stejnou wi-fi připojen hacker odposlouchávající bezdrátový přenos a vy se připojíte k webu bez zabezpečovacího protokolu HTTPS, může získat například vaše přihlašovací údaje a vyzkoušet, zda se se stejným heslem nepřipojí i k vašemu Facebooku, Gmailu nebo jiné službě. Pokud však použijete VPN, tedy budete surfovat prostřednictvím bezpečného serveru, hacker nemá šanci zjistit nic o vaší internetové identitě. S VPN sítí dokážete obejít i geografické omezení a rovněž vám zajistí anonymní stahování torrentů.

ZDROJ: Refresher.cz

RADY PRO BEZPEČNÉ POUŽÍVÁNÍ SOCIÁLNÍCH SÍTÍ

10 TIPŮ A RAD

Co dělat, ale i co nedělat na sociálních sítích.



1. Neuvádějte na veřejném profilu telefonní číslo nebo adresu-
2. Neposílejte nikomu svoji intimní fotografii, nikdy nevíte, kde se může objevit.
3. Udržujte hesla (k e-mailu i jiná) v tajnosti, nesdělujte je ani osobě blízké či kolegovi v práci.
4. Nikdy neodpovídejte na neslušné, hrubé nebo vulgární maily a vzkazy.
5. Nedomlouvejte si schůzku přes internet, aniž byste o tom neřekli někomu jinému.
6. Nevěřte každé informaci, kterou na internetu získáte.
7. Když s někým nechcete komunikovat, nekomunikujte.
8. Nesdělujte informace typu, kdy jedete na dovolenou, po návratu by vás mohlo čekat překvapení.
9. Při používání webové kamery buďte obezřetní, kdokoli může na druhé straně hovor nahrávat.
10. Než cokoli potvrdíte, přečtěte si podmínky užívání.

A TEĎ JE ČAS NA ZÁBAVU!

Zkuste OSMISMĚRKU! Najděte slova, která se týkají rizik online komunikace

B	M	B	Z	V	X	R	P	G	B
P	O	M	L	O	U	V	Á	N	Í
J	B	Y	J	Y	J	K	L	D	M
I	Y	B	T	N	W	S	E	H	W
S	E	X	T	I	N	G	H	T	R
X	H	H	K	W	W	X	P	D	N
K	H	P	R	H	N	X	Z	L	T
O	U	O	O	B	K	B	P	V	T
G	V	U	V	N	H	R	K	B	S
D	I	A	A	S	R	Y	H	Q	L

kyberšikana

sexting

kybergrooming

kyberstalking

pomlouvání

pořizování záznamů

happy slapping

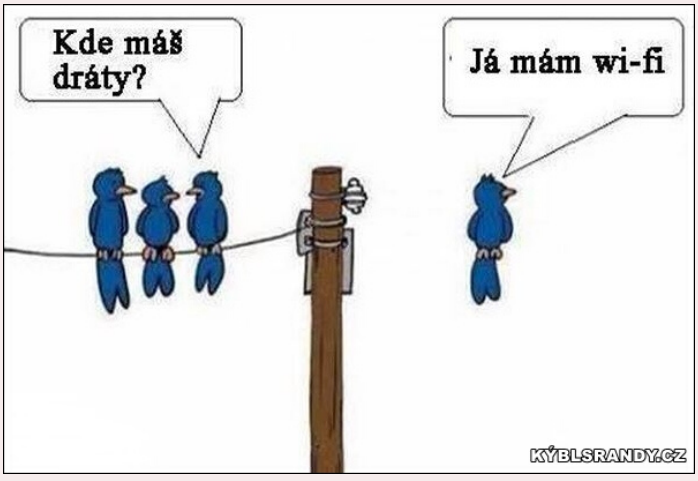
krádež identity

odhalování tajemství

online

vydírání

Hádají se:
Wikipedie: „Já vím všechno!“
Google: „Já najdu všechno!“
Facebook: „Já znám všechny!“
Internet: "„Beze mě jste všichni namydlení!“
Elektřina: „A tak se uklidníme, jo?!“



Dnes mi na 45 minut vypadl internet. Šel jsem tedy za mámou do obýváku a zjistil jsem, že je to vcelku pohodová ženská.

Nečtěte počítačové vtipy z počítače:
Mohl by se urazit a vypnout se!

SUDOKU!

			9		2			
	4						5	
		2				3		
2								7
			4	5	6			
6								9
		7				8		
	3						4	
			2		7			

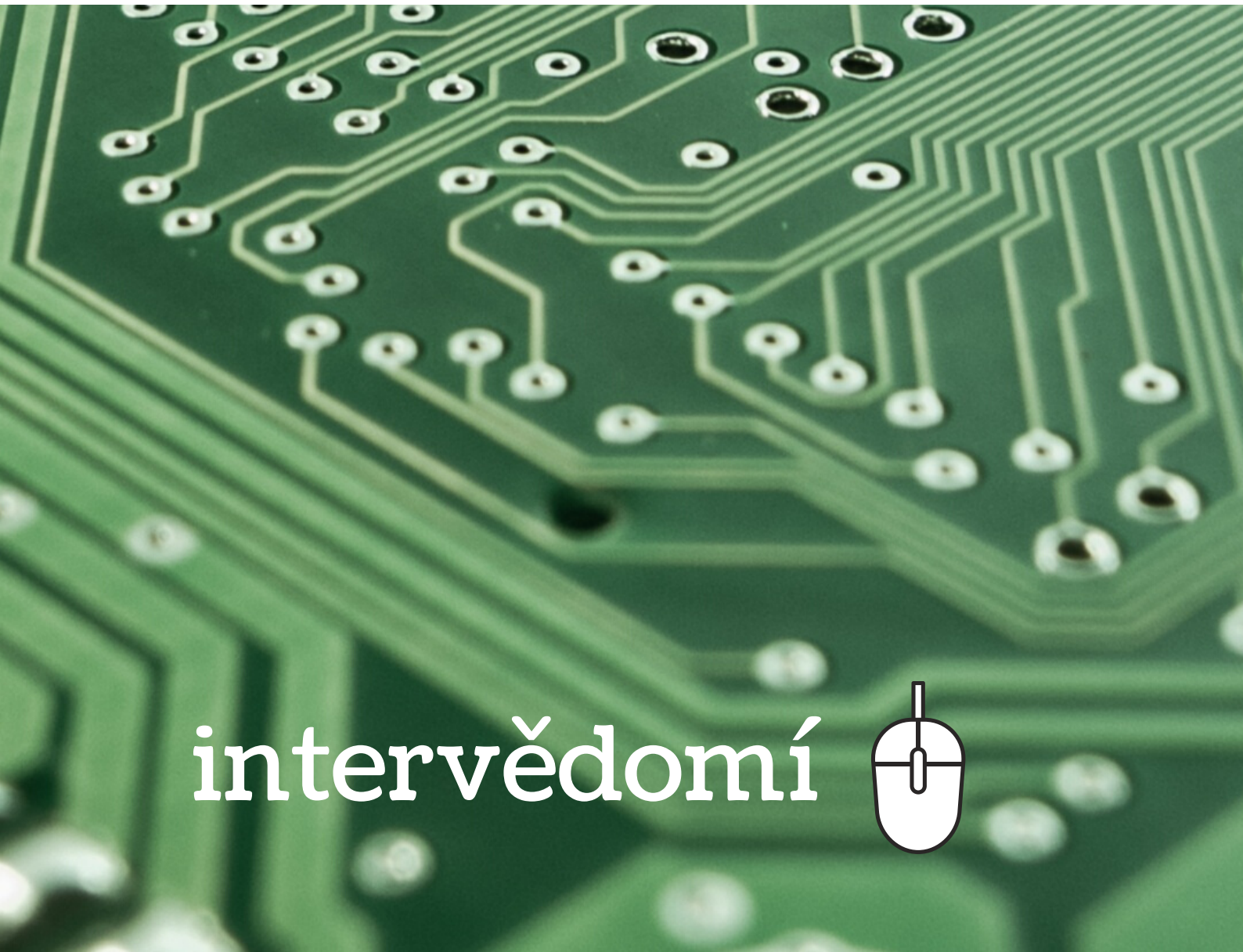
	6			2				
7			8	4				6
	5		1			7		
3		8				1		
		1				2		4
		6			2		4	
				7	1			9
				9			3	

DĚKUJEME,
ŽE NÁS PODPORUJETE.
Těšíme se na Vás u dalšího čísla, již za měsíc.

V tomto čísle nám inspirací byly:
internetembezpecne.cz
bezpecnyinternet.cz
refresher.cz

Další vydání již za měsíc
1.6. 2020

Natálie Navrátilová
Simona Tesařová
Marie Veselá



intervědomí