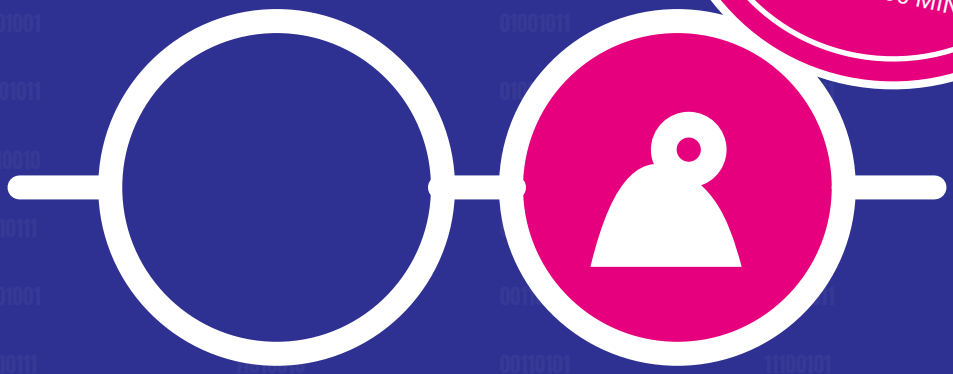
Rozhovory s AI
o kyberbezpečnosti

KYBER-BEZPEČNOST

LÍNÁ EDICE

ZDARMA · 30 MIN



PRO NEPOLÍBENÉ

Jakub Luptovec
& jane.comensky

Zkrácená verze 2. vydání knihy · 30 minut čtení · 7 kroků · Klid v duši

ÚVOD

Začneme nepříjemným faktem

Před chvílí jsem se vrátil z velké mezinárodní konference o kybernetické bezpečnosti. A jeden z řečníků nám naservíroval pár docela ostrých čísel:

1. Každý den je na světě zneužito přes 18,5 milionu datových záznamů.
2. Mnozí výrobci bezpečnostních technologií slavných jmen se sami stali cílem útoku a přišli o svá data.
3. Kybernetický zločin je dnes třetí největší ekonomikou světa, po Spojených státech a Číně, s ročními příjmy přes 8 bilionů dolarů.

A mám pro tebe ještě jednu zprávu, která tě nepotěší. Tím, na koho kyberzločinci nejraději útočí, jsi právě ty.

> **Vědění, znalost – života zbraň.**

Triky, které na nás kybernetičtí podvodníci zkoušejí, se dají často docela dobře rozpoznat. Stačí trocha tréninku a informací — a šance na výhru začnou docela slušně růst. K tomu je tahle příručka.

Co tě v LÍNÉ EDICI čeká

Jano, kdo bude tuhle Línou edici číst a co od ní může čekat?

Každý, kdo nemá čas číst celou 168stránkovou knihu. Zjistíš tu, jakých 7 hrozeb tě reálně ohrožuje a 7 konkrétních kroků, kterými se proti nim ochráníš. Pochopíš to, i kdyby ti bylo 75 a počítač jsi viděl/a poprvé před měsícem.

KAPITOLA 1

7 hrozeb, které musíš znát

Tahle kapitola je vlastně černou magií, jen v digitálním kabátku. Útočníci spoléhají na to, že lidé jednají rychle a bez rozmyslu. Pravidlo č. 1 zní: nech to chvíli vychladnout. Skoro nikdy se nestane nic, co by hodinu nepočkalo.

01 Phishing – falešný e-mail nebo SMS

CO TO JE. Zpráva, která vypadá jako od banky, pošty, Alzy nebo úřadu. Vyzývá tě k přihlášení, doplnění údajů nebo zaplacení drobného poplatku. Stránka, na kterou míříš, je ovšem podvrh — tvoje heslo nebo číslo karty putují přímo do rukou útočníka. Existuje i smishing (přes SMS) a vishing (přes telefon).

CO S TÍM. Nikdy neklikej na odkaz ve zprávě, která tě nutí jednat rychle. Otevři si web ručně nebo přes záložku. Pokud si nejsi jistý, zavolej do banky/instituce na oficiální číslo, které najdeš na jejich webu — ne to ze zprávy.

02 Sociální inženýrství a deepfake

CO TO JE. Útočník nepotřebuje hackovat počítač, když může „hacknout“ tebe. Vydává se za rodinu („babi, mám problém, pošli peníze“), kolegu, opraváře, policistu. Využívá naléhavost, autoritu, strach. Dnes umí AI vygenerovat i deepfake video či hlas tvého blízkého.

CO S TÍM. Při jakékoli žádosti o peníze, hesla nebo údaje vždy ověř druhým kanálem. Zavolej zpátky na známé číslo, napiš jiným způsobem, domluvte si v rodině heslo pro případ nouze.

Jano, a proč se vlastně říká PHISHING a ne FISHING, když se bavíme o rybaření?

Předpona „ph“ pochází z dob, kdy hackeři a phreakers (lidé manipulující s telefonními systémy) používali „ph“ místo „f“ ve svém žargonu. Slovo phishing metaforicky odkazuje na „lov“ uživatelů, kteří „kousnou“ do podvodné návnady.

Medailonek: Kevin Mitnick (1963-2023)

Jeden z nejznámějších hackerů světa. Proslavil se sociálním inženýrstvím — vydával se po telefonu za zaměstnance telekomunikačních firem a získával tak přístupové kódy. Po propuštění z vězení se stal etickým hackerem a konzultantem. Jeho techniky jsou považovány za ranou formu phishingu — tehdy se ale ještě nepoužíval internet, ale telefonní síť.

03 Malware, viry a ransomware

CO TO JE. Souhrnné označení škodlivých programů — dostanou se do počítače přes přílohu, pirátský software nebo aplikaci z neoficiálního zdroje. Můžou krást hesla (keyloggery), tajně sledovat (spyware), nebo zašifrovat všechna data a požadovat výkupné (ransomware).

CO S TÍM. Zapnutý a aktualizovaný antivirus (na Windows úplně stačí Windows Defender), instaluj jen z oficiálních zdrojů (App Store, Google Play, weby výrobců), nikdy neotvírej přílohy, které nečekáš. Hlavně zálohuj — krok 5.

04 Falešné e-shopy a podvodné weby

CO TO JE. Útočník zkopíruje vzhled známého e-shopu a změní v adrese jediné písmeno — třeba *alza.cz* vs. *alza-cz.shop*. Ty vyplníš platbu, peníze odejdou, zboží nikdy nedorazí. Často to přijde přes Facebook reklamy nebo phishingové e-maily („poslední kus, sleva 70 %“).

CO S TÍM. Adresu webu vždy zkontroluj v adresním řádku — kompletně. Při placení preferuj kreditní kartu nebo PayPal (umožňují reklamaci), vyhýbej se převodu na účet u neznámých e-shopů. Hledej recenze i mimo daný web.

Jano, hackeři mohou vytvořit falešné recenze i celé e-shopy, které vypadají jako originální?

Přesně tak, Jakube. Existoval třeba falešný e-shop „Big BBQ Warehouse“ — podvodníci vytvořili web na doméně .shop místo originální .com, vypadal úplně stejně. Nakupující na tomhle podvodném webu přišli o peníze a nikdy nedostali zboží.

05 Únik dat (data breach) a krádež identity

CO TO JE. Když firma, u které máš účet (e-shop, fórum, hra, banka), přijde o databáze, tvůj e-mail a heslo skončí na černém trhu. Útočník je pak zkouší v desítkách služeb a tam, kde používáš stejné heslo, se přihlásí. S dostatkem dat může převzít i tvou identitu — vyřídit si půjčku, založit firmu.

CO S TÍM. Pro každou službu jiné heslo (s pomocí správce hesel — krok 3). Pravidelně si zkontroluj e-mail na haveibeenpwned.com, zdarma ti řekne, v jakých únicích už figuruješ. Pokud ano: okamžitě tam změň heslo a všude jinde, kde jsi měl stejné.

06 Veřejné Wi-Fi a IoT zařízení

CO TO JE. Kavárna, letiště, hotel. Útočník na stejné síti může odposlouchávat tvou komunikaci. Stejně tak levné kamery, žárovky a chytré spotřebiče s továrním heslem — připojit se na cizí domácí kameru zvládne i desetiletý hacker. To samé platí pro bezklíčový přístup u aut: signál klíčenky uvnitř domu lze prodloužit „relay boxem“.

CO S TÍM. Na veřejné wifi nikdy internetbanking ani přihlášení k důležitým účtům — pokud nemáš VPN. Změň výchozí hesla na všech chytrých zařízeních, klíčenku auta ukládej do kovové krabičky (Faraday).

07 Seznamky a romantické podvody

CO TO JE. Ověřený profil není bezpečný profil — modrá fajfka potvrdí obličej, ne úmysl. Appka jen porovná tvoje selfie s fotkami na profilu; podvodník s vlastní tváří projde ověřením stejně snadno. Scénář má i jméno — pig butchering: oběť se nejdřív „vykrmí“ důvěrou, pak porazí. Jede to v krocích: rychlá intenzita (láska po pár dnech psaní), přesun z appky („pojď na WhatsApp“ — mimo appku tě nikdo nehlídá a profil nejde nahlásit), náhlá krize nebo „tip na krypto“, a nakonec peníze — grafy na falešné investiční appce rostou, dokud posíláš; pak web zmizí i s penězi. Varianta přes nahé fotky (sextortion): nejdřív intimní výměna, pak vydírání.

CO S TÍM. Chtěj živý videohovor — pravý člověk na pět minut kývne, tři výmluvy v řadě = konec. Hoď fotky do zpětného vyhledávání (Google Images, PimEyes, TinEye); stejná tvář pod víc jmény = ukradený profil. Žádné peníze a žádné doklady někomu, koho jsi neviděl naživo — bez výjimky. Přesun mimo appku, spěch a tajemství („neříkej to nikomu“) ber jako signál, ne náhodu.

Jano, fakt stačí chtít videohovor? Co když se ten člověk prostě stydí?

Stydlivost pět minut na kameru vydrží — podvod ne. Když přijdou tři výmluvy v řadě a stejná tvář sedí na víc profilech ve zpětném vyhledávání, máš odpověď. A pravá známost tě nikdy nepoprosí o peníze dřív, než jste se viděli naživo.

Když už visíš na háčku

Hlavně se nestyď a mlč co nejmíň — stud je důvod, proč většina obětí nikomu neřekne, a útočník přesně s tím počítá. Okamžitě přestaň posílat (i když slibují, že tahle platba je úplně poslední). Zavolej do banky — čerstvou platbu jde někdy ještě zastavit nebo reklamovat. Nemaž komunikaci — profil, zprávy a čísla účtů jsou důkaz. Nahlas to na linku 158 (nebo Policie ČR online); u sextortinu a u dětí pomůže poradna E-Bezpečí. U vydírání nahými fotkami neplať a neodpovídej — zaplacení vydírání nezastaví. Jedna naletěná platba není konec světa. Mlčení a druhá platba ano.

Pozor na sociální sítě. Co napíšeš na Facebook nebo Instagram, je veřejné — a útočníci to používají k cíleným útokům. Fotky letenek a oznámení „odjíždíme na dovolenou“ jsou pozvánka pro zloděje. Méně sdílení = lepší ochrana.

KAPITOLA 2

7 kroků k bezpečnému životu

Představ si, že jsi starověký rytíř stojící na hradbách své pevnosti. Nepřítel může zaútočit odkudkoli, ale ty máš silné hradby a propracované strategie. Sedm kroků v téhle kapitole jsou tvoje digitální hradby a brnění. Když si to dáš jeden volný večer, budeš na 90 % ochráněný.

1 Zapni dvoufaktorové ověření (2FA)

Tohle je nejdůležitější věc v celém guide. Kromě hesla potřebuješ druhý faktor — kód v aplikaci, SMS, otisk prstu. Útočník, který ti ukradne heslo, se pořád nedostane dovnitř.

Kde minimálně: e-mail (Google, Seznam, Outlook), banka, Facebook, Instagram, Apple ID, Microsoft. Aplikace jako Google Authenticator, Microsoft Authenticator nebo Authy jsou bezpečnější než SMS.

2 Vytvoř si silná hesla – frází, ne kudrlinkou

Zapomeň na *Pavel1985!*. Pravidlo zní: delší = lepší. Nejsilnější jsou dlouhé fráze ze 3–4 nesouvisejících slov, například: **Zeleny.Knedlik.Katastrofa6**

Snadno se pamatuje, prakticky se nedá uhodnout ani prolomit. Vyhni se jménům, datům narození, jménu psa nebo RZ auta — to vše se dá najít na sítích.

3 Začni používat správce hesel

Nezvládneš mít unikátní silné heslo pro 100 služeb v hlavě. Řešení je správce hesel — jedno hlavní heslo si pamatuješ, zbytek za tebe vyplní.

- Bitwarden — zdarma, otevřený kód, funguje všude. Pro většinu lidí ideál.
- 1Password — placený, profesionálně udělaný.
- iCloud Klíčenka — pokud žiješ v Apple, máš to zdarma a funguje samo.

A když zapomenu hlavní heslo? Budu muset zavolat hackera?

Většina správců má postupy pro obnovu — bezpečnostní otázky, záložní kódy nebo obnovu přes ověřený e-mail. Důležité je tyhle možnosti nastavit hned, jak začneš.

4 Zkontroluj antivirus a aktualizace

Většina lidí přemýšlí nad antivirem zbytečně dlouho. Pravda: Windows 10/11 už mají vestavěný Windows Defender, v testech srovnatelný s placenými. Pro 95 % lidí to úplně stačí.

Na Macu stačí vestavěná ochrana plus zdravý rozum. Na mobilu antivirus prakticky neřeš, pokud instaluješ jen z oficiálních obchodů.

Aktualizace nejsou otrava, ale záplaty bezpečnostních děr. Pravidelně instaluj operační systém, prohlížeč i aplikace.

5 Zálohuj – pravidlo 3-2-1

Tři kopie, dvě média, jedna mimo dům. Pravidlo, které si pamatují i profíci.

3× kopie: originál + 2 zálohy.
2× média: jedna na externím disku, druhá v cloudu.
1× mimo bydliště: kvůli požáru, krádeži. Cloud to splňuje automaticky.

Pro běžného člověka: Google Drive / iCloud / OneDrive + jednou ročně kopii na externí disk. Pro automatické zálohování použij *Time Machine* (Mac) nebo *Historie souborů* (Windows).

Když přijde ransomware, požár, krádež nebo „jen“ rozbitý disk — tvoje fotky dětí, dokumenty a vzpomínky jsou v bezpečí. Bez zálohy jsou pryč navždy.

6 Zabezpeč domácí Wi-Fi

46 % uživatelů si nikdy nezmění výchozí heslo routeru — a útočník ho najde na internetu během minuty.

- Změň heslo wifi i administrátorské do routeru (ne stejné).
- Nastav WPA3 (nebo WPA2). Nikdy WEP — ten je jako zámek z papíru.
- Pravidelně aktualizuj firmware routeru.

7 Zdravý kybernetický skepticismus

Krok, který nemá konec. Většinu útoků dnes nezachytí antivirus — protože míří na tebe, ne na tvůj počítač. Zlaté pravidlo: když tě někdo tlačí jednat RYCHLE, je to varovný signál.

Tři otázky, které si vždy pokládej: 1) Čekal/a jsem tuhle zprávu? 2) Sedí mi adresa odesílatele a webu? 3) Tlačí mě někdo k akci?

Rychlý checklist na lednici

- [ ] Zapnul/a jsem 2FA na e-mailu
- [ ] Zapnul/a jsem 2FA na bance a sítích
- [ ] Mám silné, unikátní heslo na e-mail
- [ ] Mám správce hesel a hlavní frázi
- [ ] Defender / antivirus je zapnutý a aktualizovaný
- [ ] OS, prohlížeč a aplikace jsou aktuální
- [ ] Zálohuji do cloudu — automaticky
- [ ] Mám i kopii na externím disku
- [ ] Změnil/a jsem heslo na wifi a do routeru
- [ ] Zkontroloval/a jsem se na haveibeenpwned.com

KAPITOLA 3

Mýty vs. realita

Mark Twain jednou řekl: *„V životě mě trápila spousta věcí, z nichž většina se nikdy nestala.“* V kyberbezpečnosti kolují polopravdy, které člověka buď zbytečně vyděsí, nebo naopak uspí. Tady jsou ty hlavní.

MÝTUS	Můj počítač nikoho nezajímá, na mě nikdo neútočí. Útočníci útočí v rozsahu — automaticky na miliony lidí. Máš e-mail, jsi cíl.
MÝTUS	Antivirus zaručuje 100% ochranu. Žádný antivirus nezachytí útok přes sociální inženýrství. Tam zachrání jen tvoje hlava.
MÝTUS	Silné heslo stačí — 2FA je pro paranoidy. Bez 2FA stačí jediný únik dat a útočník je v účtu. 2FA je dnes standard, ne luxus.
MÝTUS	Domácí wifi je bezpečná, protože používám heslo. Pokud máš výchozí heslo z routeru a starý šifrovací standard, nic to neznamená.
MÝTUS	Bezpečnostní záplaty mohou počkat. Většina aktualizací jsou opravy bezpečnostních děr. Den, kdy je odložíš, útočníci zjistí, co opravovat.
MÝTUS	Anonymní režim v prohlížeči mě ochrání před sledováním. Skryje historii v prohlížeči. Před zaměstnavatelem, ISP a stránkami neskryje nic.
PRAVDA	Každý může být cílem hackerů, bez ohledu na finance. Hackeři útočí v rozsahu — automaticky na miliony lidí.
PRAVDA	Většina útoků dnes míří na lidi, ne na technologie. Sociální inženýrství je nejúspěšnější typ útoku.

KAPITOLA 4

Algoritmus tě sleduje

Tvoje digitální stopa rozhoduje. Skrytě. Pořád. Co o tobě algoritmy ví, určuje cenu letenky, výši pojistky, výši úroku z hypotéky — i to, jaké reklamy uvidí tvoje děti. Tady je 5 reálných příkladů z roku 2026.

Není to konspirace. Je to byznys.

JetBlue zdražila letenku za den o 230 $

Andrew Phillips hledal letenku na pohřeb. Druhý den byla o 230 dolarů dražší. Když JetBlue zažaloval, sami mu radili: *„Vyčisti cookies, použij anonymní okno.“* Algoritmus sleduje tvoji IP, geolokaci a kolik času trávíš na stránce — a z toho spočítá, kolik nejvíc jsi ochotný zaplatit.

Pojišťovna ti měří, jak řídíš

Telematics aplikace v autech (a chytré hodinky pro životko) sledují, jak brzdíš, kdy řídíš v noci, kdy spíš. „Sleva za bezpečnou jízdu“ znamená v praxi penalizaci za to, že řídíš jako normální člověk. Stejné principy přicházejí do životního pojištění přes Apple Health a Garmin.

HR a banky scrapují tvé staré posty

Při pohovorech HR scrapery najdou každý tvůj starý komentář a lajk. V USA některé hypoteční firmy upravují úrok podle „lifestyle scoringu“ z Facebooku a Instagramu. Co jsi napsal/a v roce 2014 rozhoduje o tvé budoucnosti dnes.

Algoritmy cílí na děti v okamžiku zranitelnosti

TikTok, YouTube i Instagram cílí reklamy na děti podle dat: kdy bdí, kdy je smutné, kdy má kapesné. Interní studie Facebooku z roku 2017 ukázala, že algoritmus uměl rozpoznat teenagery v „okamžiku zranitelnosti“. Díky AI je dnes profilace 100× přesnější.

Data brokeři jsou byznys za 270 miliard ročně

Na světě je 5 000 data brokerů. Za 1 dolar si kdokoli koupí tvou aktuální adresu. Vědec v roce 2025 koupil milion seznamovacích profilů včetně 5 milionů fotek za 150 dolarů. V USA pro to není federální zákon. V EU GDPR pomáhá — ale musíš to udělat sám.

5 věcí, co můžeš udělat zítra ráno

Těmhle systémům se úplně vyhnout nemůžeš. Ale můžeš výrazně omezit, co o tobě algoritmy vědí — a tím přímo ovlivnit ceny, pojistky i úroky, které ti nabízejí.

1 Před nákupem letenky vyčisti cookies

Anonymní okno (Ctrl+Shift+N v Chrome, Cmd+Shift+N na Macu) před každým nákupem letenky, hotelu nebo pojištění. Porovnej s běžným oknem — rozdíly bývají v desítkách až stovkách procent.

2 Smaž (nebo skryj) staré sociální posty

Posty z roku 2014 dnes rozhodují o úrocích, pojistce, pohovorech. Projdi si chronologii na Facebooku a Instagramu. Smaž to, co bys už nepostnul/a. Nastav staré posty na „jen přátelé“.

3 Vypni telematics a fitness sdílení s pojišťovnou

V aplikaci pojišťovny a v Apple Health / Google Fit zkontroluj, komu sdílíš data o spánku, pulsu, řízení. Tahle data znamenají reálné peníze — tvoje, ne jejich.

4 Pošli data brokerům žádost o smazání (GDPR)

V EU máš právo na výmaz. Bezplatné služby jako YourDigitalRights.org nebo Mine ti pošlou žádosti na stovky data brokerů jedním kliknutím.

5 Změň prohlížeč na Brave nebo Firefox

Chrome a Edge tě sledují by default. Brave a Firefox mají vestavěné blokování trackerů a fingerprintingu. Když přesto chceš zůstat u Chrome, doplň si aspoň uBlock Origin + Privacy Badger a zakaž *third-party cookies*. V mobilu zapni *App Tracking Transparency* (iOS) nebo blokování v *Privacy Sandbox* (Android).

KAPITOLA 5

Co dělat, když se to už stalo

I když uděláš všechno správně, může se stát, že tě někdo přeci jen dostane. Tady je první pomoc pro nejčastější scénáře.

Klikl/a jsem na podezřelý odkaz a zadal/a heslo.

Jdi do služby ručně přes prohlížeč (ne přes ten odkaz!) a okamžitě změň heslo. Pokud používáš stejné heslo jinde, změň ho i tam. Zapni 2FA. Zkontroluj v účtu, jestli se z něj neposlaly podivné zprávy.

Přišel mi e-mail „pošli bitcoin nebo zveřejníme video“.

Klid. Tohle je masově rozesílaný podvod (*sextortion*). Útočník nic nemá. Pokud ve zprávě uvádí staré heslo, má ho z dávného úniku dat. Heslo si změň, 2FA zapni. Neplať. Neodpovídej. Smaž.

Někdo se dostal do mého e-mailu.

Nejhorší scénář — z e-mailu se obnovují hesla všude. Z bezpečného zařízení změň heslo a zapni 2FA. Odhlas všechna ostatní zařízení. Zkontroluj, jestli si někdo nepřesměroval poštu. Postupně změň hesla všude důležitě (banka, sítě).

Mám zašifrovaný počítač – ransomware.

Neplať výkupné — žádná záruka, že to pomůže, a financuješ útočníky. Odpoj počítač od sítě. Pokud máš zálohu (krok 5!), přeinstaluj a obnov ze zálohy. Případ nahlas Policii ČR (kybercrime@pcr.cz).

Babička volá, že banka po ní chce peníze „do bezpečí“.

Zhluboka se nadechněte všichni. Je to právě probíhající podvod. Ať nic nedělá, neposílá nic, neinstaluje žádnou aplikaci „na pomoc“ (pozor na *AnyDesk*!). Zavolej do banky na číslo z karty. Banky nikdy nepřesouvají peníze „do bezpečí“.

ZÁVĚR

Tahle stránka není konec.

Je to začátek. Pokud ti LÍNÁ EDICE otevřela oči, mám pro tebe ještě tři věci.

1. Plná verze knihy

Kyberbezpečnost pro nepolíbené
(168 stran, 2. vydání)

Najdeš v ní všechno detailněji — kompletní vysvětlení phishingu, sociálního inženýrství, ransomware, hesel, 2FA, zálohování. Plus kapitolu o tom, jak vypadá útok z pohledu útočníka, a „přídavek pro nenasytné“ o kvantových počítačích, kryptoměnách, XR realitě a autonomní dopravě.

2. Jane.comensky – tvoje AI asistentka

Jane je virtuální asistentka, která ti zodpoví otázky z téhle příručky i mimo ni — kdykoli a konkrétně. Můžeš jí poslat fotku podezřelé SMS, e-mailu nebo faktury a ona ti řekne, jestli je v pořádku.

Kde Jane najdeš

1. Otevři chatGPT.com · 2. Přihlas se · 3. V levém panelu klikni na *Prozkoumej modely GPT* · 4. V hledání napiš comensky · 5. Zvol Jane.Comensky a piš.

3. Pošli to dál

Pošli tenhle PDF tomu, kdo ho potřebuje — rodičům, prarodičům, kolegyni, sousedovi. Je to volně šiřitelná zkrácená verze. Kybernetické gramotnosti není nikdy dost.

Hodně štěstí v digitálním světě.

— Kuba & Jane

Každou minutu dochází ve světě ke 2 200 kyberútokům. Každou minutu se přes 40 lidí stává obětí. Buď mezi těmi, kdo to nezažijí.