"To se mně stát rozhodně nemůže."

Tenhle velký mýtus z oblasti kyberbezpečnosti používáme, když se nechceme svou bezpečností zabývat: nemáme na to čas, nevíme jak nebo nás prostě nenapadlo, že by bylo dobré se při práci s vlastními technologiemi chránit. Než se v dalších modulech společně podrobněji podíváme na jednotlivé oblasti kyberbezpečnosti, budeme si vyprávět příběhy. Jména osmi hrdinů těchto příběhů jsou sice smyšlená, jejich útrapy se ale v mnoha obměnách odehrávají dnes a denně na celém světě.

Jsou to příběhy **obyčejných lidí jako jsme my**, kteří si ale na vlastní kůži zažili narušení svého osobního kyberbezpečnostního prostoru: od prolomení hesla, přes sociální inženýrství až po ransomware. Záporáky příběhů jsou kyberkriminálníci z celého světa, kteří chtějí on-line prostor a technologie využít pro svůj zisk: někdy jde o peníze, někdy o naše data a naše soukromí; někteří využívají sofistikované metody a jiní jednoduché postupy, staré jako lidstvo samo. **Ostražitost** je tedy na místě vždy.

Tento e-learning existuje proto, že chceme v říši kyberbezpečnosti vyprávět už jen pozitivní příběhy – nebo alespoň takové příběhy, které budou mít vždy dobrý konec. Proto se dnes zamyslíme i nad rychlými a jednoduchými kroky a tipy, jak se nestát hrdiny podobných příběhů. V dalších modulech tato doporučení a tipy podrobněji rozebereme.

# Petr, vyučující na Pedagogické fakultě

Petr je ve svých přednáškách zvyklý zkoušet mnoho nových on-line služeb a nástrojů, kterými svou výuku zatraktivňuje. Často se proto registruje k různým službám a často také využívá jedno a totéž heslo pro všechny stránky: kdo si je má jinak všechna pamatovat? Petrovi dnes přišel znepokojivý e-mail: ze služby pro tvorbu studentských kvízů unikla data – a jeho e-mail i heslo v nezašifrované podobě teď prý lítá někde po internetech. Kdokoliv tak může jeho kombinaci e-mailu a hesla využít pro přihlášení k jakékoliv další službě, kde je Petr použil. Útočník, který Petrovy údaje dostal do ruky, se je pokusil zadat do Facebooku. Kombinace byla bohužel správná, Facebook ovšem útočníka ani přes to dál nepustil. Petr totiž naštěstí u těch nejzásadnějších služeb (jako je jeho e-mail, Facebook a školní systém) využívá vícefaktorové ověřování. Kromě zadání hesla se tak musí při přihlašování ověřit ještě potvrzením na svém telefonu. To bylo Petrovo jediné štěstí. I tak ho čeká odpoledne strávené měněním hesel na mnoha dalších webech.

Dnes už není otázkou, zda z některé služby data uniknou, ale spíše kdy. Každý týden vídáme zprávy o větších či menších únicích. Jakmile se přihlašovací údaje z jedné služby dostanou na veřejnost (*v horším případě nijak nechráněné a čitelné*), zkouší je útočníci automatizovaně předhazovat různým dalším webům a službám – a u části z nich se stejnou kombinací uspějí. Této praxi se říká *credential stuffing* a útočníci zneužívají té hrozivé skutečnosti, že přes 65 % uživatelů používá stejná hesla opakovaně pro různé služby.

Stejná hesla většinou používáme, protože je to jednoduché: nemůžeme si pro každou službu pamatovat unikátní heslo. Tím ale velmi dramaticky ohrožujeme své kyberbezpečí! Vaše heslo není jen řetězec znaků, který vám umožňuje přístup do konkrétního účtu. Heslo v kyberprostoru představuje polovinu vašeho soukromí.

Dobrým řešením je správce hesel, který si hesla bezpečně pamatuje za nás. U zásadních služeb, jako je e-mail nebo sociální síť, je pak unikátní heslo spolu s vícefaktorovým ověřením rozumnou a rychlou cestou, jak je ochránit. Aby se útočník do Petrova Facebooku dostal, nestačilo mu jen znát heslo – musel by ještě Petra fyzicky okrást o jeho telefon. A to už rozhodně není tak jednoduché, jako vytahovat uniklá hesla z temných zákoutí internetu.

|  |
| --- |
| **Vyzkoušejte si,** zda jste také už někdy nebyli součástí nějakého úniku dat. Vsaďte se, že pravděpodobně ano? Vložte svou pracovní a pak i svou osobní e-mailovou adresu do služby [Have I Been Pwned](https://haveibeenpwned.com/) a ihned zjistíte, zda se vaše adresa v nějakém úniku dat již objevila. Pokud ano, doporučujeme si v dané službě změnit heslo – a pokud stejné heslo používáte i jinde, bude třeba ho změnit na unikátní i tam. Podobnou službu nabízí i [Firefox Monitor](https://monitor.firefox.com/). |

**Více o heslech, jejich ochraně nebo vícefaktorovém ověření** se dozvíte v modulu č. 2.

# Tomáš, magisterský student fyzioterapie

Tomáš chodí na pravidelné pivo s kamarádem, kde probírají novinky, radosti i strasti svých životů. Dnes probírají jednu aktuální nepříjemnost: minulý týden Tomovi na telefonu začala vyskakovat upozornění o podezřelých přihlášeních na jeho sociální sítě z druhé strany světa. Všechna přihlášení zamítnul, ale každý den se objevují další. Tomášův kamarád je v kyberbezpečnosti zběhlý, a tak Tomovi odhalil, jak jednoduché a rychlé může být tzv. prolamování hesel. Společně si na speciální webové stránce zkusili zadat heslo podobné těm, které používá Tomáš: bylo prolomeno do tří minut. Zděšený Tomáš ihned po příchodu domů svá hesla změnil na silnější. S novými hesly už byl obezřetnější. Nastudoval si všechny potřebné aspekty, jako třeba že délka je důležitější než složitost a veškeré své poklady svěřil správci hesel, aby si nová a unikátní hesla nemusel pamatovat.

Heslo nemusí jen uniknout (jako v případě Petrova příběhu). Když používáme heslo příliš jednoduché, může se nám přihodit to, co se stalo Tomášovi: heslo prostě někdo takzvaně prolomí. Dnes už se samozřejmě „neláme“ ručně. Slovníkové útoky nebo útoky hrubou silou jsou zpravidla prováděny pomocí speciálních crackovacích programů, které zkouší jako možné heslo všechna slova ve slovníku nebo kombinace různých znaků. Jedná se o metodu poměrně rychlou a efektivní: program zkouší různé kombinace tak dlouho, až tu správnou prostě najde.

Rychlost lámání záleží mimo jiné i na tom, zda uživatel používá jednoduchá nebo silná hesla. **Více o správných heslech, jejich ochraně nebo vícefaktorovém ověření** se dozvíte v modulu č. 2.

# Bětka, studentka sociologie

Na přednášky jezdí Bětka tramvají přes celé město – po chvíli se většinou začne nudit, z kapsy vytáhne mobil, rychlým gestem na displeji ho odemkne a sleduje, co nového se událo na Instagramu. Dnes díky tomu ztratila přehled o čase a skoro zapomněla vystoupit u fakulty: na poslední chvíli vystřelila ze sedadla a ze dveří. Až na přednášce zjistila, že mobil nemá. Uf, naštěstí byl zamčený... Bětka na přednášce dlouho nevydrží, musí pořád myslet na svůj telefon: vyplíží se pryč z posluchárny a spěchá zpátky domů, aby mohla na Facebook nasdílet výzvu, zda někdo její telefon na tramvajové lince 4 nenašel. Na počítači ale zjišťuje, že někdo mezi tím změnil její hesla do většiny služeb: od Facebooku přes Instagram až po její soukromý e-mail. Nikam se teď nedostane a nad svým kyberprostorem dočasně úplně ztratila kontrolu.

Mnohdy pečlivě chráníme své notebooky či stolní počítače a na chytré souputníky zapomínáme. Přitom jsou v podstatě branami do našich digitálních životů: v mobilním telefonu má většina z nás přihlášeny všechny základní a důležité služby, sociální sítě a e-mail nevyjímaje. Náhodný útočník využil Bětčinu nepozornost a jednoduchou praktiku, zvanou *shouldersurfing*: prostě stál vedle Bětky a zahlédl, jakým gestem telefon otevírá. Zamykání telefonu vzorem je jedním z nejslabších a zároveň nejjednodušeji zapamatovatelných způsobů: až 64 % lidí je schopno si odemykací vzor zapamatovat, i když ho vidí jen jednou a letmo – třeba právě u spolucestujícího v tramvaji.

Kdyby se Bětka po cestě na přednášku navíc rozhodla i zkontrolovat rozvrh ve školním systému, viděl by útočník i jak zadává přihlašovací údaje. Těch by mohl později zneužít i bez toho, aby telefon fyzicky odcizil. Tak pozor, kdo se dívá...

# Tereza, studijní referentka na právnické fakultě

Jako studijní referentka má Tereza většinou práce až nad hlavu: řeší potíže studentů i akademiků, nastavuje rozvrhy nebo třeba pomáhá vyučujícím zadávat známky ze závěrečných testů do systému. Část týdne může pracovat z domu – a to si Tereza užívá. Když je hezky, jde si sednout do parku, připojí se na otevřenou Wi-Fi z nedaleké kavárny a všechny zapeklité administrativní záležitosti se najednou řeší mnohem příjemněji. Dnes si ale Tereza všimla, že její kalendář a poznámky nejsou takové, jak je posledně zanechala. Zítra ve 3 měla mít přece schůzku – a ta v kalendáři najednou není! A z té konzultace se studijním oddělením určitě udělala pro kolegy poznámky – a přitom jsou v souboru na interním úložišti jen nějaké nesmyslné odkazy. Co se to děje? Tereza si po chvíli přemýšlení vzpomněla, že v některých dokumentech lze dohledat historii změn. A samozřejmě! Někdo prováděl změny v době, kdy zcela určitě spala. Nemohla to tedy být ona. Kdo to ale byl? Kdo prováděl tuto záškodnickou činnost?

Dostat se na internet zdarma venku v kavárně nebo parku je fajn, ale dostat se tam bezpečně – to už je oříšek. U veřejných sítí si nemůžeme být jistí, že jsou dobře nastaveny a zabezpečeny, a ačkoliv je situace lepší než před lety, stále bychom se měli venku "v divočině" chovat jinak, něž když jsme připojení na univerzitní síť. Na veřejných WiFi je lepší se nepřihlašovat do citlivých systémů, jako je třeba naše elektronické bankovnictví nebo univerzitní systém.

|  |
| --- |
| **Víte že...** Mezi časté praktiky navíc patří i falešné sítě, které se pouze jmenují podle podniků v okolí: ve skutečnosti se ale jedná o takzvané *honeypoty*, které ovládá útočník – na jeden takový se nejspíš nachytala i Tereza v parku. |

Vždy je třeba počítat se situací, že nás útočník na veřejné síti odposlouchává: může sledovat kudy brouzdáme, kam se přihlašujeme, někdy dokonce může vidět i heslo, které zadáváme. Díky většímu rozšíření zabezpečených protokolů (HTTPS) už dnes není tak jednoduché odposlouchávat samotný obsah našeho brouzdání, někdy jsou však pro útočníka velmi zajímavá i takzvaná *metadata*: na jaké weby chodíme, v jakém pořadí nebo třeba kolik na nich trávíme času. Dobrou praxí je proto využívat virtuální privátní síť (VPN <odkázat na school-specific návod>), která nás před tímto typem sledování dostatečně ochrání.

|  |
| --- |
| **Vyzkoušejte si,** že někdy stačí jen málo a naše kyberbezpečnost dramaticky vzroste. Třeba takový obyčejný doplněk do prohlížeče [HTTPS Everywhere](https://www.eff.org/https-everywhere), který zajistí, že vždy když vstupujeme na webovou stránku, vstoupíme na ní zabezpečenou cestou pomocí bezpečnějšího protokolu (*pokud to daná stránka umožňuje*). Stačí ho nainstalovat, a pak na něj můžeme zapomenout. |

# Radek, student ekonomiky

Radek studuje jeden z magisterských programů ekonomické fakulty. Protože je šikovný, občas si pomáhá k penězům navíc jako konzultant pro známé, kteří chtějí začít investovat. To zahrnuje práci se spoustou citlivých dat a někdy i svěřených fondů svých klientů. Do e-mailu dnes ráno Radkovi přišla zpráva, která odkazuje na přihlašovací okno investičního účtu, kde spravuje většinu produktů. Odkaz byl doplněný zprávou, že pokud se Radek přihlásí přes zaslaný odkaz ještě daný den, dostane ke každému produktu 5 % měsíčně investované částky.

Obsah zprávy zněl velmi lákavě a pokud by Radek své údaje vyplnil a odeslal, putovaly by přímo do rukou útočníka. V tomto případě se totiž jedná o ukázkový phishing, kdy útočník rozesílá hromadné množství podvodných e-mailů a snaží se tak sbírat přihlašovací údaje. Ty pak může libovolně zneužít. Následky by pro Radka mohly být nedozírné: od finanční škody až po škraloup na pověsti ve vysněném zaměstnání. Naštěstí je však na podobné typy zpráv již poměrně zvyklý a ví, že je vždy důležité myslet na několik bodů:

**1. Kriticky přemýšlet** – proč by mu někdo cizí na internetu dával jen tak něco zdarma? Ne každý e-mail musí být skutečně od toho odesílatele, od jakého se zdá, že je.

**2. Prohlédnout si gramatiku a pravopis zprávy** – divné formulace a chyby ve zprávě by Radka i nás měly zalarmovat, stejně tak jako například urgence a deadline *(“Pokud to neodešleš ještě dnes, přijdeš o bonus.”)*.

**3. Nespěchat, pořádně si prohlédnout URL odkaz** (někdy může jít jen o prohozená písmenka v adresním řádku a phishing je na světě!), ale i celkovou grafickou podobu stránky. I drobné nuance mohou být předzvěstí nekalosti. Navíc platí, že heslo nikdy nezadáme přes odkaz, který nám někdo zašle. Heslo je prostě jako zubní kartáček, nikdy ho nepůjčujeme a nikdo důvěryhodný se nás nikdy na naše heslo mailem nebo telefonicky ptát nebude.

|  |
| --- |
| **Vyzkoušejte si,** jaké to může být v podobných situacích, jakou zažil Radek. Poznáte phishing a další zákeřné metody? Odhalíte je dostatečně brzy? Otestovat se můžete v češtině [na webu KYBERTEST](https://kybertest.cz/), v angličtině v [testu od společnosti Google](https://phishingquiz.withgoogle.com/) nebo ve slovenské verzi podobného testu [na webu CSIRT.SK](https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html). |

# Lenka, ekonomka Právnické fakulty

Množství emailů, které každý den přistanou Lence ve schránce, je skoro nekonečné. Lenka je zvyklá pracovat velmi rychle a efektivně: jeden mail za druhým řeší palčivé problémy akademiků a výzkumníků s jejich projekty a rozpočty. Dnes dopoledne dostala stručný e-mail od vedoucího jedné z kateder:

Předmět: Platba (naléhavá)  
Od: Profesor Syrový, syrovy@law.universita.cz  
Komu: Sekretářka Prudká, prudka@ekon.univerzita.cz

Dobrý den, Lenka,  
Jaký je zůstatek na našem bankovním účtu?  
Můžeme dnes zaplatit 28.780,00 EUR?

Je třeba ihned proplatit faktura v příloze.  
S pozdravem, Profesor Syrový

*Odesláno z mého iPhonu.*

Lenka zpět odpověděla s informací o velikosti zůstatku a doptala se pana profesora, zda jde o platbu v rámci jeho projektu a zda bude dokládat průzkum trhu. Zpět však opět přišla jen zpráva o tom, že je třeba fakturu co nejdříve proplatit. Ale takové zvláštní slohové formulace... A taky nesedí to oslovení v prvním pádu! Že by to pan profesor psal ve spěchu? Je pravda, že podle patičky e-mail píše ze svého mobilního telefonu... Možná mu Lenka raději ještě zkusí zavolat, než platbu provede.

Příběh Lenky je podobný zkušenosti Radka. Jen tady nebyl žádný odkaz, kam se měla Lenka prokliknout a přihlásit. Tento e-mailový podvod využívá metod sociálního inženýrství – útočník například předpokládá, že Lenka se příkazu od profesora zalekne a ihned uposlechne (*případně často také že otevře nakaženou přílohu*). Útočníci v podobných případech velmi často využívají časovou tíseň: „*do druhého dne*“, „*máte po splatnosti faktury*“ atp. Takovéto nečekané prosby a žádosti vždy kontrolujeme i jinou komunikační cestou, pokud to situace umožňuje: tak například pan profesor Syrový píše e-mail, že máme proplatit fakturu? Tak to mu raději zavoláme na jeho pracovní mobil a vše ověříme.

**Více o bezpečné komunikaci** (nejen) e-mailem nebo o šifrování a podepisování e-mailů najdete v kapitole 3, **více o sociálním inženýrství** a jeho metodách pak v modulu 4.

# Aneta, bakalářská studentka filmových studií

Aneta studuje druhým rokem svůj vysněný obor Filmová studia. Škola ji velmi baví, ráda by se v budoucnu věnovala filmovým kritikám, a tak se také ve volném čase snaží psát a sdílet své kritiky na webu. Aneta ráda trénuje na starších filmech, může totiž potom porovnávat své úvahy s výroky slavných kritiků. Méně známé a starší filmy však někdy není jednoduché sehnat, proto filmy občas stahuje skrze poskytovatele v takzvané šedé zóně. Včera Aneta stahovala film z dvacátých let pomocí tzv. torrentů, který ovšem kromě filmového zážitku přinesl Anetě do počítače také malware. Počítač je teď podezřele pomalý...

Aneta ani neví, jak rizikové je stahování ze zmíněných zdrojů (často v křížku se zákonem), a kolikrát unikla velkému problému jen díky svému antivirovému a plně aktualizovanému programu. Antivirový software funguje jako síto toho nejhoršího, na co můžete (nejen) na internetu narazit. Identifikuje podezřele se chovající soubory, software a malware.

|  |
| --- |
| **Víte že...** malware může mít různé cíle? Některé škodlivé programy sledují naše chování na počítači a pátrají po osobních datech, některé na naše zařízení pašují reklamu, některé nás chtějí vydírat a jiné třeba v pozadí těží kryptoměny (tzv. *cryptojacking*) a tím náš počítač výrazně zpomalují – zrovna takový malware si spolu s filmem stáhla Aneta. |

Ať jste zvolili placený antivirový program nebo bezplatnou verzi, nikdy neotálejte s aktualizacemi. To však platí u všech programů, které máte v zařízení instalované. A pozor – mezi zařízení nepatří jen váš počítač, ale i tablet, notebook nebo chytrý telefon, kde lze také instalaci antivirového programu doporučit – a především zde doporučujeme důsledně systémy těchto zařízení aktualizovat. A na závěr, v případě serverů ve křížku se zákonem nemusí pomoci ani antivir...

# Josef, výzkumník a sociolog

Josef je sice výzkumník, ale taky trochu chaotik. Většina souborů, se kterými pracuje, leží u něj na ploše: data z výzkumů, tabulky, rozepsané články i prezentace na konference. Jednou za čas se rozhodne plochu vyčistit, ale většinou to skončí vytvořením složky s názvem 'Stará plocha', do které všechny soubory přesune. V praxi to znamená, že Josef své soubory uchovává lokálně na svém počítači. Něco jako zálohování nikdy neřešil, protože na to jednoduše neměl čas. Dnes ráno Josef z úložiště stáhl program, který nutně potřeboval k analýze dat: jenže po jeho rozbalení a spuštění počítač zamrzl. Josef zařízení zrestartoval a teď na zářivě červené obrazovce svítí agresivní zpráva: "Vaše soubory byly zašifrovány! Pokud k nim chcete znovu získat přístup, pošlete alespoň 400 dolarů v digitální měně Bitcoin na níže uvedený účet."

Způsoby, jakými se na naše zařízení může dostat malware, je mnoho: otevřeme přílohu zákeřného e-mailu, klikneme na podvržený zkrácený odkaz, stahujeme ZIP archiv s filmy z nelegálního úložiště jako Aneta nebo si třeba stáhneme nelicencovaný software – a malware s ním přijede jako černý pasažér. Josef se stal obětí zákeřného typu malware: *ransomware* útoku. Není to nic vzácného: poslední roky počet těchto případů dramaticky roste i u nás v Česku.

Pokud selže naše antivirová ochrana (nebo ji dostatečně neaktualizujeme), výsledek je vždy velmi podobný: naše data jsou zašifrována, zařízení zablokováno a na obrazovce výzva, abychom za své soubory zaplatili výkupné. V takový moment už většinou není příliš jak pomoci.

Nejlepší cestou je prevence: dnes svá data zálohujeme a naše budoucí já nám za to poděkuje. Když pak ransomware zašifruje data, nebolí to tolik, protože je máme v dostupné kopii i jinde: na externím disku nebo třeba na úložišti v cloudu (*OneDrive atp.*). I takové zálohy samozřejmě musíme dostatečně chránit, v případě cloudových služeb například silným heslem a dvoufázovým ověřováním. Zálohování nechrání jen před ransomware útoky, pomůže stejně i při ztrátě či odcizení zařízení nebo když počítač nebo mobil jednoho dne prostě už odejde stářím – a to se jednou stane určitě, dříve nebo později.

|  |
| --- |
| **Na co nezapomenout z prvního modulu?** Kyberbezpečnostní incidenty se dějí každý den.  Technologií se nemáme bát, ostražitost a obezřetnost jsou ale na místě.  Způsobů, jak může být naše kyberbezpečí narušeno, je celá řada. Důležité je například dbát na silné a unikátní heslo a vyžívat vícefaktorové ověření (2FA). Sociální inženýrství je reálná hrozba: ne každý je tím, za koho se vydává. Zálohování dat nám může ušetřit mnoho práce nejen v případě ransomware útoku. |

|  |
| --- |
| **Pozor!** **Co dělat, když se něco pokazí?** V případě, že došlo k bezpečnostnímu incidentu nebo máte podezření, že mohlo být narušeno vaše kyberbezpečí, obracejte se na <school-specific: doplňte kontaktní osobu nebo popište proces řešení kyberbezpečnostních incidentů>. |