# Bezpečná komunikace

V elektronickém prostředí komunikujeme neustále: každý den pošleme a přijmeme desítky (někteří z nás i stovky a tisíce) e-mailů a zpráv přes chat a messengerové aplikace. Komunikace v on-line prostředí však skrývá mnohé kyberbezpečnostní nástrahy: jak si například můžeme být jisti, že zprávu skutečně poslal člověk, který je uveden jako odesílatel? Nebo kdo a jak se může snažit zneužít známá slabá místa elektronické komunikace, aby z nás vytáhl osobní data nebo dokonce peníze? A kdo všechno třeba může číst naši komunikaci v kyberprostoru?

Ve třetím modulu se společně nejprve zaměříme na e-mailovou komunikaci – neodmyslitelnou součást našich studijních i pracovních životů. I když se zdá, že ji pomalu a jistě vytlačují chatovací aplikace, na světě se každý den stále rozešlou miliardy e-mailů. To není vůbec zanedbatelné číslo. Ruku v ruce s tímto množstvím rostou i možnosti a šance útočníků, jak využít naší nepozornosti a způsobit nám značné škody v pracovním i soukromém životě. Co tedy útočníci dělají pro to, aby získali citlivá data a napáchali co nejvíce škod? Pojďme se nejdříve podívat na jejich základní techniky.

# Píše mi děkan... nebo ne?

Stalo se vám už také, že vám přišel e-mail, u kterého se na první zběžný pohled zdálo, že je adresa odesílatele v pořádku, ale po bližším zkoumání něco nesedělo? Pravděpodobně jste se setkali s metodou známou jako ***podvržení odesílatele***. Podvrhnout odesílatele u e-mailu je skoro stejně snadné, jako u klasických dopisů: prakticky kdokoliv může napsat do políčka odesílatele co chce. Zjevným cílem takto podvrženě zaslaných e-mailů je působit na příjemce tak, že samotná e-mailová adresa vypadá jako regulérní a důvěryhodná. Ve skutečnosti za zasláním zprávy stojí útočník. S touto metodou se bohužel v posledních letech setkáváme stále častěji.

|  |
| --- |
| **Vyzkoušejte si,** jak jednoduché je zfalšovat odesílatele e-mailu. Využít k tomu můžete některý z volně dostupných *fakemailerů* <odkaz na slovník>: třeba [Emkei’s](https://emkei.cz/). Falešné e-maily třeba od Billa Gatese ale posílejte pouze sobě, nezneužívejte tyto služby! Také si takto zfalšovaný e-mail neposílejte na oficiální pracovní e-mail, ale třeba na starší e-mailovou adresu.  Skuteční útočníci samozřejmě používají pokročilejší metody. Důležité je si ale uvědomit, že odesílatel jakéhokoliv e-mailu **nemusí být skutečně ten, kdo je v hlavičce zprávy uvedený**... |

<school-specific: podle pohledu na etiku takového praktického cvičení; legislativně bylo konzultováno a není problematické takovou službu ukazovat/využívat pro vzdělávání uživatelů.>  
  
Abychom byli schopni podvržený e-mail odhalit, musíme vědět, co vlastně hledat a kam se dívat. Proto se na podezřelé znaky společně podíváme.

## Jak poznám podvržený e-mail?

Prvním krokem je samozřejmě bedlivě sledovat kontext: mohu takovou zprávu od tohoto odesílatele skutečně očekávat? Není třeba podezřelé, že mě zrovna tato osoba takto žádá např. o proplacení faktury, nebo že mi posílá v příloze dokument, o kterém jsme nikdy předtím nemluvili?

Druhý krok je techničtější: součástí každého e-mailu je vedle těla (*obsahu zprávy*) i tzv. hlavička. V těchto hlavičkách jsou obsaženy základní informace o daném e-mailu, které zpravidla obsahují odesílatele, příjemce, adresu pro zaslání odpovědi, kopii či předmět e-mailu, dále pak podrobnější informace o cestě e-mailu kyberprostorem či zda je digitálně podepsán apod.

|  |
| --- |
| **Víte že...** hlavička e-mailu se v e-mailovém programu nebo službě zobrazuje pouze ve zkrácené podobě? Její plné znění si však většinou můžeme zobrazit – a je to vhodné, pokud si nejsme autenticitou emailu jistí a chceme si ověřit některé další informace (viz dále). V každém e-mailovém klientovi však musíme hledat trochu jinde. [Kde to najdete zrovna v tom svém?](https://security.muni.cz/clanky/e-mailove-hlavicky) |

Útočník může využít několik triků a cest, jak nás zmást. Nejčastěji bývá útočníky zneužito pole „*Od*“ (*From*), které obsahuje informaci o odesílateli. Právě tam se totiž nachází ona Achillova pata, tedy zfalšovaná adresa, která slouží útočníkovi k nekalým účelům. Jak ale tuto podvrženou adresu identifikovat? Co nám může pomoci odhalit podvržený e-mail, je pole ***Reply-To*** (Return-Path), kde se nachází adresa, na kterou by měla být zaslána odpověď, tedy e-mailová adresa skutečně využívaná útočníkem. Další metody zahrnují například **využití trochu jiné domény** (např. dekan@universita.cz místo skutečného dekan@univerzita.cz) nebo může útočník **napadnout přímo účet odesílatele** a pak nemusí nic podvrhovat – v tu chvíli nám píše ze skutečné adresy odesílatele. I s takovou možností je proto třeba počítat.

|  |
| --- |
| **Víte že...** útočníci navíc často zneužívají tzv. *homoglyfy*? Jde o znaky, které vypadají podobně, ale ve skutečnosti pochází z jiných abeced. Typickým příkladem mohou být některá písmena z cyrilice či azbuky, která na první pohled připomínají latinku. Zdá se vám, že *dekan@univerzita.cz* a *dekan@univеrzita.cz* jsou stejné adresy? Počítač si to nemyslí: v druhém případě je ve slově univerzita místo písmena ”e” z latinky použito malé “ie” z cyrilce, které vypadá skoro stejně. Pro počítač jsou to dvě odlišné adresy, jako příjemci si toho ale nemusíme všimnout. Nebo si **zkuste rozkliknout** tyto dva odkazy: <https://www.аррӏе.com> a <https://www.apple.com>. Zdají se být stejné... Tušíte, proč každý z odkazů vede na jiný web? Šikovný trik, že? |

Proč by vlastně někdo vůbec měl zájem na tom falšovat odesílatele? Samozřejmě to může být jen nevinný vtípek: někdo si může chtít vystřelit z kamaráda, že mu píše třeba slavná herečka, aby ji vzal na rande. To je sice morálně diskutabilní fórek, příliš mnoho škody to ale nenadělá. Mnohem zásadnější jsou útoky typu BEC neboli *business email compromise.*

Jde o podvodné jednání, které má za cíl **vylákat informace citlivé povahy**: osobní a přihlašovací údaje, privátní klíče, obchodní tajemství apod. Tyto údaje se snaží získat nejčastěji od osob, které se v rámci hierarchického žebříčku organizace zabývají činnostmi souvisejícími například s finančními operacemi. Poslední dobou roste počet útoků, kdy se útočníci vydávají za významné představitele univerzit rozesílají zaměstnancům například falešné **příkazy k proplacení faktur**. To už je ale jedna z metod *phishingového útoku* a **sociálního inženýrství**, o kterých se více dozvíte v modulu č. 4.

## Co dělat, když mám podezření na podvržený e-mail?

**1.** To nejdůležitější je nikdy neklikat na žádný odkaz ani přílohu, který v e-mailu přijde. Stejně tak se nepodvolit ani nátlaku, který z e-mailu může plynout (*např. končící splatnost faktury atp.*) a vše řešit v klidu a s rozmyslem.

**2.** Pokud nás e-mail vybízí k nějaké aktivitě (zaplaťte fakturu, přihlaste se a obnovte si heslo atp.), je žádoucí si vše ověřit jinými kanály. Doporučuje se kontaktovat odesílatele např. telefonicky nebo přes jinou komunikační aplikaci. Vždy však využívejme prostředky, které jsme získali důvěryhodnými způsoby: nikdy např. nevolejme na čísla, která jsou použita přímo v podezřelém e-mailu!

**3.** Na e-mail nikdy neodpovídáme! Tím, že na e-mail reagujeme, dáváme útočníkovi najevo, že je naše adresa funkční a aktivní. Výsledkem pak bude jen mnohem více podobných útoků nebo spamu <slovník>. Prostě je třeba zatnout zuby a z celého srdce zprávu ignorovat...

**4.** Pokud máme podezření (nebo jistotu), že je e-mail podvržený, je nejlepší jej **přeposlat kyberbezpečnostnímu týmu**! Nejrychlejší způsob, jak e-mail předat, je přeposlat samotný e-mail (tělo), nejlépe však i s hlavičkami a přílohami či odkazy, pokud se v e-mailu vyskytují. <school-specific: doplnit, co od uživatele očekáváme a kam to mají posílat – podle nastaveného procesu.>

# (Ne)vinný spam

O spamu, tedy nevyžádaných zprávách, pravděpodobně v dnešním online světě slyšel každý z nás. Spam je dnes všudypřítomný a můžeme jej kromě e-mailu naleznout také na stránkách blogů, sociálních sítích, v různých komunikačních programech a v posledních letech i ve formě SMS zpráv apod. Když zůstaneme u e-mailu, představuje až neuvěřitelných 45 % všech odesílaných zpráv (některé zdroje uvádějí dokonce až 98 %!).

## Co je to spam?

Pokud bychom se na spam podívali podrobněji, zjistili bychom, že se jedná o nevyžádané sdělení, které je rozesíláno obrovskému množství uživatelů. Nejčastěji se asi setkáme s reklamním spamem. Otravné nabídky s nepřeberným množstvím výhodných slev a skvělých produktů dostáváme čas od času do e-mailové schránky asi všichni.

|  |
| --- |
| **Víte že...** na každých 12 500 000 odeslaných e-mailových spamů obdrží útočníci minimálně jednu odpověď? Nezdá se to jako mnoho, ale je nutné si uvědomit, že každý den je zasláno přibližně 14,5 miliardy nevyžádaných e-mailů. |

Hranice mezi spamem a nebezpečnějším phishingem je dnes už velmi tenká: s postupem času se pole působení spamu přesouvá od hloupých reklamních sdělení k nebezpečnějším cílům: rozšiřování hoaxů či rozposílání malwaru. Cílem spammerů (těch, kdo spam rozesílají) je třeba získat osobní data od příjemců nebo se podílet na rozeslání dezinformace či jiných polopravd a podvodů. V neposlední řadě spam značně přetěžuje e-mailovou infrastrukturu organizace. Spam prostě nelze brát na lehkou váhu.

## Proč mi spam vlastně přišel? Kde vzal útočník mou adresu?

Každý z nás si pravděpodobně při čištění složky SPAM někdy položil otázky jako „*Kde vzali moji e-mailovou adresu?”* nebo *„Proč mi ty spamy pořád chodí, když jsem nikde e-mail nezadával?*“. Nejvíce e-mailových adres získají spammeři prostřednictvím robotů, kteří procházejí internetové stránky a hledají odkazy na e-mailové kontakty. Mnohdy dochází i k tomu, že si spammer zakoupí databázi adres, ať už legálně nebo na černém trhu s takovými databázemi. Existuje mnoho způsobů, jak získat náš e-mail, aniž bychom museli spammerovi sami poskytnout sebemenší vodítko.

## Co dělat, když mi spam přijde?

Není doporučeno spam otevírat, jakkoliv na e-mail reagovat, a už vůbec není dobrý nápad klikat na odkazy či otvírat případné soubory v příloze. V některých případech můžeme už jen samotným otevřením spamového e-mailu potvrdit, že e-mail někdo přečetl a schránka je tedy používána. Díky tomu se pak můžeme dočkat další záplavy spamů. Spam je prostě nejlepší pohřbít hluboko do koše a ani ho neotvírat.

## Jak spamu předcházet?

Pokud vás věčné nabídky výhodných reklamních příležitostí a „miliony“ spamů otravují, je cestou pravidelně v e-mailové schránce označovat nevyžádané zprávy jako SPAM. Minimalizovat množství spamu v pracovním e-mailu můžeme také tak, že naši univerzitní adresu nevyužíváme například k nakupování na internetu. Pro soukromé účely používáme soukromou e-mailovou adresu. Vedle naší soukromé e-mailové adresy můžeme mít navíc ještě sekundární, kterou budeme využívat výhradně pro online nákupy, k odběru novinek apod.

|  |
| --- |
| **Vyzkoušejte si** *tempmail*: službu, která umožňuje přijímat e-mail na dočasnou adresu. Ta se pak po určité době sama zničí. Mnoho webových stránek nebo blogů po nás často požaduje, abychom se zaregistrovali dříve, než nás pustí k obsahu. V takových případech můžeme využít právě dočasnou e-mailovou adresu, a ne tu naši skutečnou, která by pak mohla skončit na nějakém seznamu pro spammery. Jen pozor: pokud do takové služby pak zapomeneme heslo, pomocí e-mailu ho už neobnovíme... Zkusit si můžeme třeba [TempMail](https://temp-mail.org/cs/) nebo [Mail.tm](https://mail.tm/en/). |

## Podezřelé přílohy

Spam dnes už není jen o reklamě a výhodných nabídkách: často bývá nosičem příloh, které mohou nepěkně zamávat s naším zařízením. Stačí pár kliků a chvilka nepozornosti k tomu, abyste si do svého zařízení stáhli nebezpečný malware. Ano, řeč je o podezřelých přílohách, které jsou neopomenutelnou součástí mnoha typů kyberbezpečnostních útoků.

Jak poznat podezřelou přílohu? Nejlehčí je to v případě, kdy obdržíme e-mail s přílohou z adresy, kterou vůbec neznáme a která nepůsobí důvěryhodně, případně i samotná e-mailová zpráva je podivná. V takovém případě rovnou považujeme přílohu za nebezpečnou. Bohužel se i zde stává, že je k šíření nebezpečné přílohy využita metoda podvržení odesílatele: škodlivá příloha přijde ze zdroje, který je nám známý a důvěřujeme mu, došlo však k manipulacím s hlavičkou e-mailové zprávy, případně je účet odesílatele napaden útočníkem. V takovém případě musíme zapojit veškeré kritické myšlení, které je nám vlastní. Pomoci nám může identifikace typu souboru v příloze nebo šikovný nástroj pro kontrolu podezřelých souborů [VirusTotal](https://www.virustotal.com/).

|  |
| --- |
| **Pozor!** Některé přílohy na nás působí svými ikonami nebo názvy důvěryhodně. Vyvolávají v nás dojem, že se jedná o legitimní dokumenty či mediální soubory. Jedná se třeba o ikony typu PDF, Word, MP3 nebo JPEG. Tady však pozor! Samotný název podvržené přílohy má totiž odlišnou příponu! Nesetkáváme se tedy s klasickou formou „.DOC“ nebo „.DOCX“, ale úplně jinými písmeny, které se vůbec neshodují s ikonkou. Někdy je dokonce [skutečná přípona souboru skrytá](https://support.zcu.cz/index.php/Skr%C3%BDv%C3%A1n%C3%AD_p%C5%99%C3%ADpon_v_syst%C3%A9mech_Windows)! Podezřelejší také bývají komprimované přílohy (RAR, ZIP atp.). Platí zde, že pro tyto situace je k nezaplacení mít nainstalovaný a aktualizovaný kvalitní antivirový program, případně využít nástroj pro kontrolu podezřelých souborů [VirusTotal](https://www.virustotal.com/). |

Mezi nejproblematičtější soubory patří ty, které lze nazvat jako *spustitelné* aplikace, typicky například soubory s koncovkou .EXE, .JS, .VBS a další typy souborů, se kterými se jako běžní uživatelé většinou nesetkáváme. Vždy je také dobré posuzovat celý e-mail jako celek: dívat se na hlavičku, na tělo e-mailu a jeho gramatiku – a v závěru i na zmiňované přílohy.

# Kdo může číst moji komunikaci?

Taky ještě občas z dovolené posíláte tradiční papírové pohlednice? Na takovou pohlednici bychom nejspíš žádné tajnosti a osobní věci nenapsali: je nám jasné, že v celém procesu poslání pohlednice je její obsah viditelný pro kohokoliv – od pošťáků přes třídiče pošty v poštovní centrále až po naši zvědavou sousedku.

Takový běžný e-mail je bohužel tak trochu jako pohlednice: po své cestě ho akorát místo pošťáků vidí mnoho e-mailových serverů, jejichž správce obvykle neznáme. A s valnou většinou ostatní naší on-line komunikace je to úplně stejné. V běžném každodenním shonu mnohdy využíváme ty komunikační kanály, které máme nejjednodušeji po ruce. To ovšem nemusí být vždy ty nejbezpečnější.

Magda posílá kolegům z katedry i svým doktorským studentům zprávy přes Facebook. Často je pro ni rychlejší vyřešit přes Messenger i administrativní náležitosti: posílá interní pracovní dokumenty, své pracovní výkazy, smlouvy – prostě to, co je zrovna třeba rychle řešit. Nedávno své kolegyni přes Messenger dokonce poslala heslo pro přihlášení do systému mezinárodní mobility Erasmus – bylo to prostě nejrychlejší řešení: rovnou na dotaz kolegyně, která napsala na Messenger, odpovědět stejnou cestou.

Je to úplně totéž, jako by Magda heslo napsala na pohlednici a odeslala ji poštou. Některé komunikační nástroje stéle mohou posílat zprávy v takzvaném *plaintextu* (obyčejný čitelný text, který se přenáší v takové podobě, v jaké ho vidíme a čteme). Všechno tak může být za určitých podmínek po cestě odchyceno a přečteno – a to se zde nebavíme o rovině ochrany našeho soukromí.

# Co s tím? Šifrování!

V případě zmiňované pohlednice z dovolené můžeme naše tajemství ochránit třeba tak, že text zašifrujete a příjemci svěříme tajemství klíče, pomocí kterého nesrozumitelnou změť znaků převede znovu zpátky do srozumitelného textu. Trochu jako na skautském táboře. V elektronické komunikaci to funguje velmi podobně, jen místo táborových šifer se využívají pokročilejší matematické procesy. Takové komunikaci se říká **šifrovaná komunikace**.

Jedním z typů šifrované komunikace je tzv. **end-to-end šifrování** (E2E). Dejme tomu, že se potřebuji kolegyně nebo spolužačky zeptat na něco důležitého a nerad bych, aby zprávu po cestě někdo četl:

Využít proto můžu komunikační aplikaci, která E2E šifrování nabízí. Zpráva se zašifruje na mém zařízení a do internetu odejde v šifrované, tedy nečitelné podobě. Pro kohokoliv, kdo by ji cestou chtěl přečíst, bude vypadat nějak takhle:

oR9MzsC3FTobl3Ph9T/aQng5HZ+hhS3udDwzYix83oE=

Do čitelné podoby se opět rozšifruje až na zařízení mojí kolegyně, která využívá stejnou aplikaci. Ani samotný provozovatel nástroje, přes který s kolegyní řešíme dnešní oběd, díky E2E šifrování nevidí, o čem si píšeme.

|  |
| --- |
| **Pozor!** Některé nástroje se prezentují jako šifrované, ve skutečnosti ale šifrují zprávu jen částečně – na cestě od nás na server provozovatele, tam se rozšifruje do čitelné podoby a znovu zašifruje na cestu k adresátovi. To ale není to pravé ořechové end-to-end šifrování... Při výběru nástroje tak hledáme ten, který přímo uvádí, že nabízí E2E, tedy **koncové šifrování**. |

|  |
| --- |
| **Víte že...** mnoho poskytovatelů komunikačních aplikací *(včetně e-mailových schránek)* využívá faktu, že konverzace není šifrována a čmuchají v našich osobních konverzacích? Hledají tam zajímavé informace, aby na nás pak mohli lépe cílit reklamu. Tím, že upřednostníme aplikaci s E2E šifrováním, se vyhneme i tomuto modernímu nešvaru. |

## Které nástroje tedy šifrují E2E?

Mezi nejrozšířenější E2E šifrované komunikační aplikace, které by dle všech informací v současnosti měly využívat tento typ šifrování, patří **WhatsApp** a **Signal**. Druhý jmenovaný je pak dnes obecně vnímán jako bezpečnější varianta. Zprávy na Instagramu, Google Hangouts nebo Snapchat a většina dalších komunikačních platforem E2E šifrování nevyužívají – neměli bychom je tedy používat při komunikaci citlivějších témat. Některé nástroje pak nabízejí E2E šifrování pouze v případě, že ho sami cíleně zapneme (např. Facebook Messenger, Telegram).

|  |
| --- |
| **Vyzkoušejte si:** používáte Facebook Messenger? Víte, že umožňuje komunikovat v režimu end-to-end šifrování? Musí se ovšem zapnout speciální funkce Tajná konverzace. Facebook sám ji příliš nepropaguje, nemá komerční zájem na tom, aby jeho uživatelé komunikovali šifrovaně. Přitom je vyšší míra bezpečí vzdálená jen na jedno kliknutí! |

# Může být šifrovaný i e-mail?

Ano, i e-mail po sítí běhá čitelný jako pohlednice a lze ho zašifrovat. Když odesíláme e-mail chceme příjemce ujistit, že je skutečně od nás, tzn. chceme e-mail digitálně podepsat, a pak také zašifrovat, aby ho mohl přečíst skutečně jen adresát. Budeme k tomu potřebovat osobní certifikát, který následně nastavíme ve svém e-mailovém programu: <school-specific: přepsat a doplnit podle vlastního řešení, např. <https://it.muni.cz/sluzby/osobni-certifikaty>>.

Využít je možné služeb infrastruktury veřejných klíčů CESNET na adrese [https://pki.cesnet.cz/](https://pki.cesnet.cz/cs/ch-intro.html) a generování osobního certifikátu na webu <https://tcs.cesnet.cz/>. Certifikát poté musíme [importovat](https://it.muni.cz/sluzby/microsoft-outlook/navody/importu-certifikatu-do-outlooku) do poštovního klienta a následně je možné e-maily [podepisovat](https://it.muni.cz/sluzby/microsoft-outlook/navody/podepisovani-e-mailu-v-outlooku-pro-android) i [šifrovat](https://it.muni.cz/sluzby/microsoft-outlook/navody/sifrovani-a-podepisovani-posty-v-outlooku).

|  |
| --- |
| **Pozor!** Jakékoliv šifrování komunikace nám nemusí být nic platné, pokud si dostatečně nezabezpečíme koncové zařízení: po cestě zprávy sice čitelné nejsou, u nás v zařízení a v zařízení adresáta však leží v čitelné podobě. Pokud si tak např. telefon dostatečně nezabezpečíme a necháme ho někde volně ležet, útočník si může zprávy číst, šifrování nešifrování. Stejně tak to bude i v případě, že se nám do telefonu nastěhuje malware. Všechno jde tedy ruku v ruce a vyplatí se věnovat pozornost i zabezpečení zařízení (více v modulu 5). |

# Ještě jedno důležité pravidlo na závěr...

Využívejme přednostně ta řešení, která **nabízí naše univerzita**.

Petr si školní e-mail přeposílá do své soukromé schránky na Gmailu. Dělá to proto, že se mu nechce přihlašovat do více e-mailů a je pro něj jednodušší vše řešit z jednoho prostředí. Heslo k přihlášení do Gmailu je navíc jednodušší a už si ho za ty roky pamatuje – však ho také využívá i jinde. Jeho údaje teď ale byly součástí úniku dat. Útočník se do Petrova účtu přihlásil a změnil mu heslo; teď si nerušeně čte nejen Petrovu osobní i pracovní poštu, ale také se za Petra může jednoduše vydávat. Petr napsal na podporu firmy Google, nikdo ale nereaguje – Petr navíc nemá Googlu, jak dokázat, že je skutečně Petrem. Obrátil se tedy na kyberbezpečnostní podporu své univerzity, ale ani tam mu příliš pomoci nemohou: servery firmy Google nespravují a nemají k nim přístup. Kdyby Petr využíval služby oficiálně podporované univerzitou, měl by teď kyberbezpečnostní tým mnohem širší možnosti, jak Petrovi ve svízelné situaci pomoci.

Není vhodné pro pracovní záležitosti používat vlastní e-mailové schránky, tj. například si přeposílat pracovní poštu do svého soukromého e-mailu (jako je třeba Gmail, Seznam Mail a podobné). V případě bezpečnostního incidentu leží interní pracovní informace na serveru třetí strany, například Seznamu nebo Googlu, a mohou tam být ohroženy. Vždy využívejte ten nástroj a e-mailový klient, který poskytuje nebo doporučuje vaše univerzita. <school-specific: přepsat a doplnit podle vlastního řešení> Kdykoliv dojde k bezpečnostnímu problému, vždy bude pro povolané odborníky z univerzity jednodušší řešit ho v prostředí, které přímo spravují nebo k němu mají lepší přístup.

To se týká i messengerů a rychlé komunikace: se spolužáky a kolegy pro pracovní a studijní náležitosti přednostně využívejme ty nástroje, které poskytuje univerzita. Může jít například o Yammer, Microsoft Teams pro rychlé zprávy i skupiny (např. místo nešifrovaných Facebook Skupin) a podobně. <school-specific: přepsat a doplnit podle vlastního řešení>

|  |
| --- |
| **Na co nezapomenout z třetího modulu?** Podvrhnout odesílatele e-mailu lze několika způsoby a není to vůbec složité. Vždy bychom měli být ostražití a ptát se, zda e-mail skutečně odeslal uvedený odesílatel. Pokud máme podezření na podvržený e-mail, neotvíráme přílohy a neklikáme na odkazy. Spam ani neotvíráme, protože tím můžeme dát signál, že je naše schránka aktivní.  Naše komunikace on-line může být čitelná úplně stejně jako pohlednice. Přes komunikační nástroje bez E2E šifrování bychom neměli řešit citlivé záležitosti. Určitou úroveň bezpečné komunikace poskytují nástroje s E2E šifrováním (např. Signal). **Pro pracovní a studijní účely bychom měli vždy využívat ta řešení, které nabízí naše univerzita.** |

|  |
| --- |
| **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>. |