


Nástěnka: IT bezpečnost

Humbuku, který nastal okolo pandemie, se radostně chytli útočníci na internetu. Začali využívat strach, nejistotu, pochybnosti a nepozornost, které současnou situaci provází. Nenechte se, prosím, nachytat!

Úvodní rychlokurz: Nenechte se nachytat!

- Udržujte své počítače i mobily aktuální.
- Používejte silné heslo! Co to je? Mrkněte na  video (https://www.youtube.com/watch?v=sUpGHM_Adxo) (a pak se prosím z YouTube nezapomeňte vrátit zpět k dalším bodům níže :-)).
- Při zadávání hesla si zkontrolujte, že jste na správné stránce.
- Před otevřením odkazu z mailu ukažte na odkaz myši a zkontrolujte adresu, kam vede. Útočníci jsou protřelí. Nachytali byste se například na konkrétní příklady z Univerzity Karlovy (https://csirt.cuni.cz/cs/dangerous_email/)?
- Před otevřením přílohy mailu si uvědomte, zdali přílohu očekáváte a zdali není celá zpráva nějaká podezřelá.

To je stručně a nyní mrkněte na konkrétní tipy a triky.

Zbystřete u každé e-mailové zprávy!

Anglicky psané e-mailové zprávy týkající se koronaviru.

Spousta e-mailových zpráv o koronaviru obsahuje nebezpečné odkazy a nebezpečné přílohy. Ukázky takových e-mailů poskytl již během února bezpečnostní tým GovCERT na svém Twitteru (https://twitter.com/GOVCERT_CZ/status/1230097149729419264). Určitě se na ně podívejte (nemusíte mít twitterový účet)!

Česky psané e-mailové zprávy týkající se koronaviru.

Podobné e-mailové zprávy se závadnými odkazy či přílohami lze očekávat i v českém jazyce. Vždy zpozorněte a řiďte se radami uvedenými níže.

Nenechejte se ukolébat tím, že e-mail přišel od známého kontaktu nebo organizace.

Zfalšovat e-mailovou adresu odesílatele je stejně snadné, jako napsat cizí adresu odesílatele na korespondenční lístek. Fakt! Známa e-mailová adresa nezaručuje, že vám to poslal kolega, známý, příbuzný nebo organizace WHO!

Pokud chcete kliknout na jakýkoli odkaz v e-mailu, nejprve na něj ukažte myši.

Ve stavovém řádku prohlížeče vlevo dole nebo v „bublině“ u myši se vám ukáže, na jakou adresu odkaz směřuje. Ukázka např. opět na Twitteru (https://twitter.com/GOVCERT_CZ/status/1230097149729419264/photo/2), určitě se na ni podívejte.

Neotevírejte přílohy e-mailu, které neočekáváte.

Pokud si nejste jistí, kontaktujte odesílatele jiným kanálem (osobně, telefonicky) a zeptejte se, zdali vám přílohu opravdu poslal. Pozor si dejte zejména na zazipované archivy (soubor.zip), soubory s dvojitou příponou (soubor.exe.zip) i dokumenty Office (Word, Excel, PowerPoint).

Nezadávejte své přihlašovací údaje na žádnou stránku, kterou jste předtím rozklikli z e-mailové zprávy.

Raději zadávejte webovou adresu ručně (typicky webmail, přihlášení na firemní/nemocniční stránky apod.). V adrese může být drobný „překlep“, který jste přehlédli, a ve skutečnosti zadáte přihlašovací údaje nějakému útočníkovi.

Zpozorněte, pokud se e-mail nebo web týká koronaviru.

Spousta závadných e-mailů chodí pod falešnou hlavičkou WHO (s návodem, jak postupovat, statistikou apod.), pod hlavičkou různých falešných charitativních organizací (příspěvek na výzkum, léčbu apod.). Zpozorněte také u webů okolo koronaviru. Například společnost ESET varuje před falešnými e-shopy (<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-detekoval-falesne-e-shopy-v-cestine-s-nabidkou-hygienickych-rousek-cilem-jsou-osobni-data-zaka/>) nabízejícími roušky, jejichž cílem není prodat produkt, ale získat osobní údaje nachytaných návštěvníků.

Co se stane, když otevřu závadnou přílohu?

- Může dojít k napadení celé počítačové sítě virem (malware).
- Může dojít ke smazání dat či zašifrování všech počítačů v síti.

Pokud si svou chybu včas uvědomíte, je ještě čas zasáhnout.

1. **Kontaktujte ihned své nejbližší (fakultní, nemocniční) IT oddělení, případně bezpečnostní tým:**
 - Univerzita Karlova: <https://csirt.cuni.cz/>
 - Masarykova univerzita: <https://csirt.muni.cz/>
 - Univerzita Palackého: <https://cvt.upol.cz/> případně <https://helpdesk.upol.cz/> (dle

https://wiki.upol.cz/upwiki/Kyberneticka_bezpecnost)

- Ostravská univerzita: <https://www.osu.cz/csirt/>
- apod.

2. **Škodám se dá zabránit, pokud se o omylu ví včas.** Nebojte se ozvat, protože rychlý zásah je mnohem snadnější než řešit následky dokončeného útoku. Pokud se zmeškají první chvíle po otevření přílohy, virus se rozšíří a již není pomoci. Pak se musí vypnout všechny počítače v síti a obnova dat a provozu pak zabere několik dní, příp. týdnů a finanční škody mohou dosáhnout i desítek milionů korun.

Co se stane, když zadám přihlašovací údaje na podvodnou stránku?

- Váš účet může být využit útočníky k napadení počítačů a sítě. Pokud se jedná o přihlašovací údaje do e-mailové schránky, útočníci mohou využít vaši adresu k dalšímu rozesílání nebezpečných zpráv či příloh.

Pokud si uvědomíte, že jste zadali přihlašovací údaje na podvodnou stránku, není ještě vše ztraceno:

1. **Okamžitě si změňte heslo.** Pokud nepoužíváte *správce hesel*, vymyslete si třeba dlouhou větu (*Moje babička chová slepice a pěstuje ředkev.*) To pro začátek stačí.
2. **Kontaktujte ihned své nejbližší (fakultní, nemocniční) IT oddělení**, případně bezpečnostní tým:
 - Univerzita Karlova: <https://csirt.cuni.cz/>
 - Masarykova univerzita: <https://csirt.muni.cz/>
 - Univerzita Palackého: <https://cvt.upol.cz/> případně <https://helpdesk.upol.cz/> (dle https://wiki.upol.cz/upwiki/Kyberneticka_bezpecnost)
 - Ostravská univerzita: <https://www.osu.cz/csirt/>
 - apod.
3. **Škodám se dá zabránit, pokud se o omylu ví včas.** Nebojte se ozvat, protože rychlý zásah je snadnější než řešení následků dokončeného útoku.

Obecné rady

- Udržujte svůj počítač i mobilní telefon aktuální.
- Odinstalujte aplikace, které nepoužíváte.
- Používejte na každou službu jedinečné a silné heslo. Může to být klidně věta týkající se vašeho života. Ideální je ovšem mít nějakého správce hesel, který vám silné heslo vygeneruje (KeePass (<https://keepass.info/>), LastPass (<https://www.lastpass.com/>), 1Password (<https://1password.com/>) apod.).
- Pokud to služba umožňuje, používejte dvoufaktorovou autentizaci (např. Google, sociální sítě). To je např. kód, který vám přijde v SMS nebo v aplikaci na mobilu, abyste se mohli přihlásit do svého účtu.
- Zkontrolujte si, že se vaše heslo nepovaluje volně někde na internetu. Jak na to? Zadejte svou e-mailovou adresu (pracovní i osobní) na kontrolní web Have I Been Pwned? (<https://haveibeenpwned.com/>) a uvidíte, které služby neuhlídaly vaše přihlašovací údaje. Na těch si určitě změňte svá hesla.
- Při brouzdání na webu dávejte pozor, na jaké odkazy klikáte a kam zadáváte své přihlašovací údaje. Nekontrolujte jen vzhled, ale také přesnou webovou adresu a ikonu záměčku vedle adresy ve webovém prohlížeči (HTTPS).
 - Ikona záměčku vedle adresy v prohlížeči neznamená, že jde o důveryhodnou stránku, nýbrž to, že je vaše spojení s webem alespoň zašifrováno, byť ten web může být klidně podvodný.

Bonus navíc: videonávody

O heslech

O heslech Počítačová bezpečnost v kostce... tentokrát o heslech.

Petr Kajzar

Ústav biofyziky a informatiky, 1. lékařská fakulta Univerzity Karlovy

O e-mailech

O e-mailech Počítačová bezpečnost v kostce... tentokrát o (podvodných) e-mailech.

Petr Kajzar

Ústav biofyziky a informatiky, 1. lékařská fakulta Univerzity Karlovy

O WiFi a Bluetooth

O Wi-Fi a Bluetooth Počítačová bezpečnost v kostce... tentokrát o bezdrátových rozhraních.

Petr Kajzar

Ústav biofyziky a informatiky, 1. lékařská fakulta Univerzity Karlovy

S počítačem na cestách

S počítačem na cestách Počítačová bezpečnost v kostce... tentokrát o cestování s počítačem.

Petr Kajzar

Ústav biofyziky a informatiky, 1. lékařská fakulta Univerzity Karlovy

Školení počítačové bezpečnosti (komplet záznam)

O počítačové bezpečnosti za časů (nejen počítačových) virů Školení počítačové bezpečnosti pro zaměstnance 1. LF UK. Natočeno v Adobe Connect dne 22.04.2020.

Petr Kajzar

Oddělení výpočetní techniky, 1. lékařská fakulta Univerzity Karlovy

Ukázky a screenshoty

- Tým GovCERT.cz na Twitteru (https://twitter.com/GOVCERT_CZ/status/1230097149729419264)
- Secret Service Warning: Exploiting the Coronavirus for Fraud and Profit (<https://blog.knowbe4.com/piling-on-exploiting-the-coronavirus-for-fraud-and-profit>)
- Exploiting the Coronavirus: The Spammers, the Scammers, and the Bad Guys (<https://blog.knowbe4.com/exploiting-the-coronavirus-the-spammers-the-scammers-and-the-bad-guys>)
- Coronavirus and Phishing (<https://www.youtube.com/watch?v=tEFFZ7uZoFM>) – video na YouTube
- ESET detekoval falešné e-shopy v češtině s nabídkou hygienických roušek, cílem jsou osobní data zákazníků (<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-detekoval-falesne-e-shopy-v-cestine-s-nabidkou-hygienickych-rousek-cilem-jsou-osobni-data-zaka/>)
- Falešné e-shopy vás připraví o osobní údaje (<https://www.dvojklik.cz/falesne-e-shopy-vas-pripravi-o-osobni-udaje/>)
- Podpůrné materiály k zabezpečení videokonferencí (NÚKIB) (<https://nukib.cz/cs/infoservis/aktuality/1645-podpurne-materialy-k-zabezpeceni-videokonferenci/>)