# Počítačová bezpečnost pro seniory

## Časté hrozby

Kryštof Měkuta
Ondřej Soukup

# Představení

Kdo z vás pravidelně používá:

- počítač
- chytrý telefon
- e-mail
- internetový vyhledávač
- elektronické bankovnictví
- internetové obchody
- zpravodajské weby
- sociální sítě

# Digitální technologie jsou skvělý pomocník

- a my vás rozhodně nechceme od jejich užívání odrazovat
  - ostatně sami je hojně užíváme
- mohou ušetřit mnoho
  - času
  - energie
  - peněz
- poskytnout
  - užitečné informace
  - spojení s blízkými
- skýtají ovšem také různé hrozby
  - stejně jako běžný život mimo digitální svět
- a nejlepší obranou je ony hrozby znát

Setkali jste se sami s nějakou digitální hrozbou?

# Trocha statistiky

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) pravidelně vydává zprávy o stavu kybernetické bezpečnosti v ČR.

Mezi nejčastější evidovaná hrozby patří (asi 85% útoků na uživatele - nezahrnuje DDoS):

- ~40% škodlivý kód
- ~25% průnik
  - například kompromitování uživatelského účtu
- ~20% podvod
  - phishing (rybaření)
    - snaha obelstít uživatele podvodnou komunikací
    - s cílem vylákat citlivé údaje nebo peníze
  - krádež identity

Zdroj: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

# Co mají nejčastější typy kybernetických útoků společné?

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) pravidelně vydává zprávy o stavu kybernetické bezpečnosti v ČR.

Mezi nejčastější evidovaná hrozby patří (asi 85% útoků na uživatele - nezahrnuje DDoS):

- ~40% škodlivý kód - **uživatel stáhne a spustí neznámou aplikaci/přílohu emailu**
- ~25% průnik - **uživatel svůj účet nedostatečně zabezpečí (slabé heslo)**
  - například kompromitování uživatelského účtu
- ~20% podvod - **uživatel uvěří podvodníkům a poskytne informaci/provede akci**
  - phishing (rybaření)
    - snaha obelstít uživatele podvodnou komunikací
    - s cílem vylákat citlivé údaje nebo peníze
  - krádež identity

Zdroj: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

# Co mají nejčastější typy kybernetických útoků společné?

Významná část kybernetických útoků je umožněna neznalostí uživatele

Navíc útok často kombinuje několik hrozeb (podvodný email obsahuje škodlivý kód apod.), proto obrana vyžaduje uživatele s komplexní znalostí

# A co senioři?

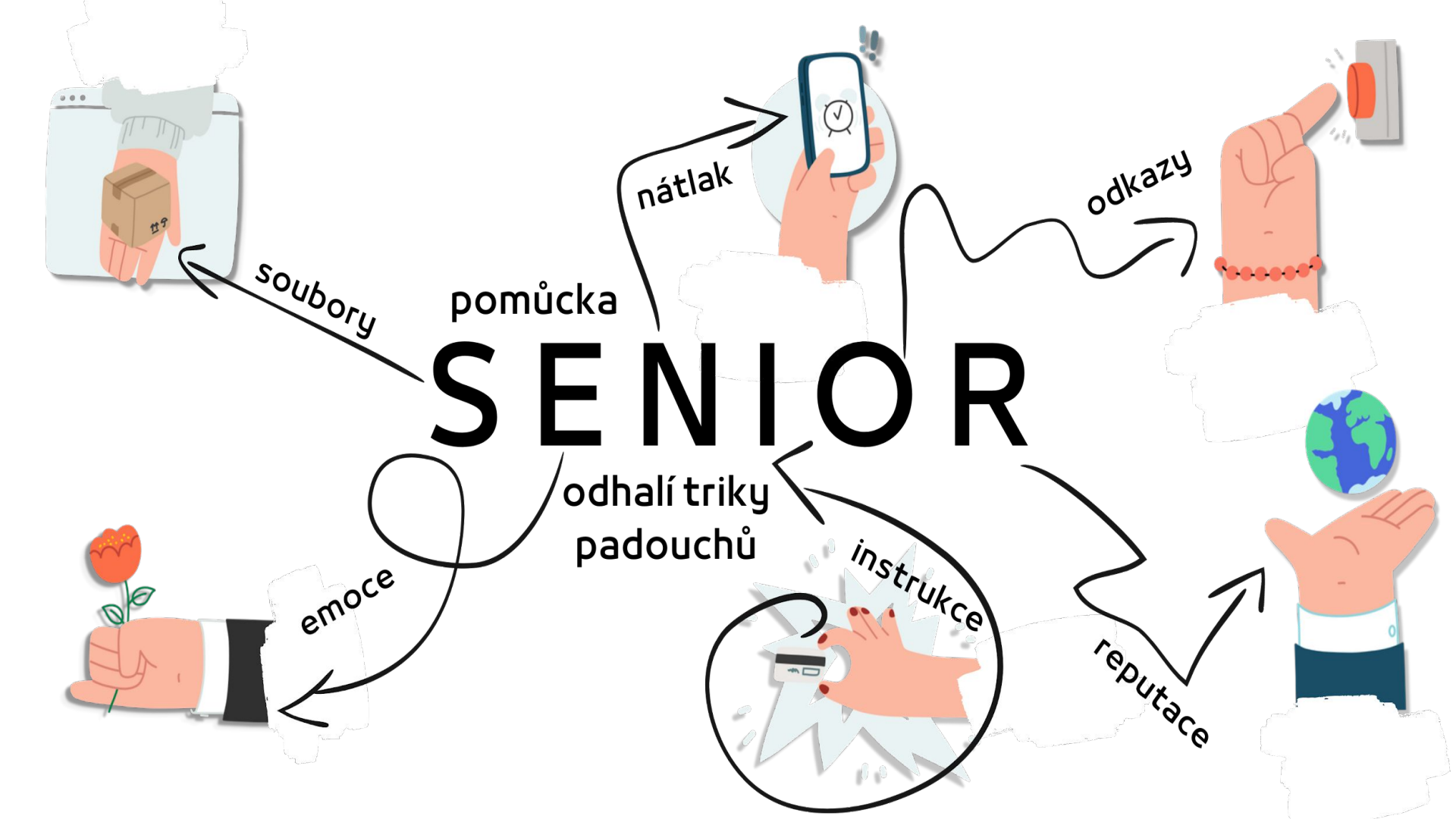
- **Národní strategie kybernetické bezpečnosti** v této souvislosti uvádí seniory jakožto významnou skupinu vystavenou negativním vlivům

Zdroj: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

- a proto NÚKIB vytvořil edukativní pomůcku SENIOR

Zdroj: https://osveta.nukib.cz/course/view.php?id=140

- na kterou bychom se chtěli společně s vámi podívat


pomůcka
SENIOR
odhalí triky padouchů
nátlak
odkazy
soubory
emoce
instrukce
reputace

# Soubory

- Dostali jste zprávu a k té je přiložený soubor?
  - **Zpozorněte!**
- Neznamená to samozřejmě, že je každý soubor škodlivý.
- Zkuste si položit následující otázky:
  - Vím, o jaký soubor se jedná?
  - Znám odesílatele? **Pozor: Na internetu je snadné předstírat, že jsem někdo jiný.**
  - Očekávám, že mi tento odesílatel bude takový soubor posílat?
  - Nemá soubor podezřelou příponu?
    - zejména spustitelné **.exe**, **.vbs**, **.docm**, **.xlsm** (pozor na složené **.pdf.exe** apod.)
    - ale také **.zip** a **.rar** - mohou skrýt obsah před antivirovým programem
- Pokud si s nějakou odpovědí nejste jistí, raději nic nestahujte a neotvírejte.

# Soubory

## Ilustrační příklady

*Vzhledem k nepříznivé situaci na trhu s energiemi jsme nuceni upravit ceník pro koncové spotřebitele. Nový ceník posíláme v příloze e-mailu. Otevřete soubor **cenik.exe** a postupujte podle pokynů.*

- Váš poskytovatel energie vám samozřejmě nový ceník poslat může.
- Určitě ale nebude mít příponu **.exe**.

# Soubory

## Ilustrační příklady

*Posíláme zvýhodněnou nabídku na léčiva. Nabídku najdete v souboru **nabidka.xlsm**, v případě zájmu nás kontaktujte. S přáním pevného zdraví Vaše **Chytrá biolékárna**.*

- Soubor s příponou **.xlsm** není bezpečné stahovat a spouštět, pokud mu absolutně nedůvěřujete.
- Skutečně očekáváte nabídku léčiva? Znáte danou lékárnu? Už jste u ní nakupovali?
- A co takhle si jejich nabídku raději najít a ověřit přímo na jejich stránkách?

# Soubory

## Ilustrační příklady

*Váš oblíbený supermarket slaví 25. výročí! Věrným zákazníkům nabízíme kupón v hodnotě 5000 Kč. Kupon najdete v souboru **kupon.docm**. Soubor stačí otevřít, vytisknout a předložit při platbě.*

- Soubor s příponou **.docm** je opět podezřelý a nemusí být bezpečný.
- Navíc vám text slibuje odměnu 5000 Kč. **Zpozorněte!**
- A rozhodně soubor nestahujte a neotvírejte.

# Soubory

## Shrnutí

- častou snahou útočníků je oběť přimět ke stažení a spuštění **škodlivého kódu**
- k tomu typicky využívají podvodné zprávy (nejen email)
- spuštění takového kódu může v zařízení napáchat škody všeho druhu
- proto je třeba **nestahovat** a **neotevírat** soubory které
    - neznám
    - neočekávám
    - vypadají podezřele

# Emoce

Ilustrační příklady

- „Chystá se snižování důchodů!! Vláda si neváží seniorů!! Přidejte se k petici za spravedlivé důchody. Klikněte zde a podepište se. Pro ověření vaší identity musíte zadat heslo do e-mailu.“
- „Agresivní školáci týrali nevinné zvíře. Získali jsme videozáznam jako důkaz. Klikněte sem a video si stáhněte. Nesmí jim to projít. Posílejte dále. Jen pro silné povahy!“
- „Dokázali jsme se zmocnit vašeho počítače a pořídili jsme videozáznam, jak navštěvujete erotické stránky. Máme vaše intimní materiály. Pokud nezaplatíte výkupné, zablokujeme váš počítač a pošleme videozáznam vašim kontaktům.“

# Emoce

- Přišla vám zpráva, která vás vyděsila, rozčílila, nebo vyvolala vaši zvědavost?
  - **Zpozorněte!**
- Pod vlivem emocí jednáme zbrkle, děláme chyby. Na to útočník spoléhá.
- Vyhrožuje ztrátou dat, zveřejněním choulostivých informací, odcizením peněz
- Může se snažit vyvolat i pocit soucitu nebo zvědavost
- Vždycky je lepší jednat s chladnou hlavou

# Nátlak

- Přijatá zpráva ve vás vzbuzuje pocit časové tísně či vyzývá k okamžité akci?
  - **Zpozorněte!**
- Časová tíseň bývá jedním z hlavních triků internetových podvodníků
- Vyhrožují nepříjemnými následky, pokud nebudeme obratem reagovat
  - Nebo naopak nabízejí zdánlivou výhodu, o kterou údajně při prodlení přijdeme
- Pod tlakem a v časovém presu všichni snáze chybujeme
  - a přesně to podvodníci chtějí
  - dostat nás do situace, kdy se zachováme tak, jak bychom se běžně nezachovali
- V takových případech dvojnásob platí lidová moudrost
  - ráno moudřejší večera | nic není tak horké, jak se vaří | dvakrát měř a jednou řež

# Nátlak

## Ilustrační příklady

*Na vašem účtu jsme zaznamenali neobvyklou transakci ve výši 10 000 směřující do Kuala Lumpur. Systém automatické kontroly transakci dočasně zablokoval. Chcete-li ji zablokovat trvale, je nutné **IHNED** vyplnit přiložený formulář a odeslat zpět.*

- Posílat 10 000 do Kuala Lumpur s největší pravděpodobností opravdu nechceme
  - Navíc to vypadá, že nám jde o čas … Co teď ?
- Nejlépe uděláme, když zachováme klid a vše si pořádně promyslíme
- A uvědomíme si, že zpráva, která **vyznívá naléhavě** a **obsahuje hrozbu**, je rozhodně podezřelá
  - Skutečně banka potřebuje vyplněný formulář, aby zablokovala podezřelou transakci?
  - Skutečně ho po nás bude vyžadovat e-mailem a ihned?
- Pokud si tím nejste jistí, zvedněte raději telefon a do banky zavolejte

# Nátlak

## Ilustrační příklady

*Blahopřejeme! Stáváte se vítězem mimořádného slosování o zájezd k moři zdarma. Stačí se stát členem klubu AI-travel. V případě, že se nestanete členem klubu !!!do 20 minut!!!, o výhru ihned přicházíte.*

- Zájezd k moři zdarma zní skvěle!
- Ale něco tady nehraje
  - zpráva vás opět nutí jednat urychleně
  - protože v opačném případě o údajnou výhru přijdete
    - a tedy vám vlastně hrozí
  - **Zpozorněte!**
- Ať už tedy stát se členem klubu vyžaduje jakoukoliv akci, bude bezpečnější na výhru zapomenout
- Nebo pokud se skutečně jedná o známou a důvěryhodnou firmu, kontaktujte ji jiným způsobem
  - můžete třeba kontakt vyhledat přímo na jejich stránkách

# Nátlak

Shrnutí

- Internetoví podvodníci se často snaží své oběti dostat pod tlak
  - vyvolat pocit ohrožení a časové tísně
- Protože spoléhají na to, že pak snáze udělají chybu
- Pokud máte tedy po přečtení zprávy pocit, že musíte okamžitě jednat
  - raději zachovejte klid
  - vše si ještě jednou přečtěte a promyslete
  - případně se nejdříve poraďte s někým dalším

# Instrukce

- Přišla vám návodná zpráva s konkrétnímy kroky, které máte vykonat?
  - **Zpozorněte!**
- Útočníci se snaží vylákat naše hesla, SMS kódy, údaje platebních karet
- Snaží se nás všemožně přesvědčit, že je splnění instrukcí v našem zájmu
- Případně vyhrožují následky, pokud instrukce nesplníme

# Instrukce

## Ilustrační příklady

*Evidujeme podezřelé převody peněz z vašeho účtu do zahraničí! Pro řešení bezodkladně kontaktujte naši odbornou podporu na telefonním čísle +322 8XX 8X8.*

- Opravdu potřebuje naše banka, abychom jí volali zpátky? Na zahraniční číslo?
- Opravdu mail posílá banka?
- Bude lepší si informaci ověřit na oficiální infolince nebo na pobočce

# Instrukce

## Ilustrační příklady

*Máte zájem o zvýšení bezpečnosti svého počítače? Odpovězte na tento e-mail a brzy vás bude kontaktovat náš specialista, který bude potřebovat vaši spolupráci. Připravte si své heslo a také telefon, na který vám chodí ověřovací SMS kódy.*

- To vypadá dobře! Lepší bezpečnost všichni chceme, proto jsme tady.
- Víme kdo nám mail poslal? Opravdu?
- (připojit k podpisu jméno známé IT firmy dokáže každý)
- Pokud firmu známe a považujeme za věrohodnou, bude lepší si vše ověřit přes oficální kontaktní údaje
- Pokud ne, je lepší preventivně nevěřit

# Instrukce

## Ilustrační příklady

*Důrazně doporučujeme, abyste si sílu svého hesla otestovali v našem novém nástroji.*

- Je v pořádku chtít mít silné heslo
- Ale heslo má být hlavně **tajné**
- Nástroje na kontrolu síly hesla opravdu existují a můžou fungovat.
  - Pokud chceme takový nástroj použít, najdeme si ho sami
  - a nikdy do něj nezadáváme heslo, které reálně používáme

# Odkazy

- Je ve zprávě odkaz, kterému máte věnovat pozornost?
  - **Zpozorněte!**
- Internetový podvodníci si s odkazy šikovně hrají
  - snadno vytvoří odkaz, který se tváří věrohodně a přitom nás vede jinam, než předpokládáme
  - navíc dokáží vytvořit podvodné internetové stránky, které jsou k nerozeznání od opravdových
    - pomocí nich se z nás snaží vylákat přihlašovací údaje
    - nebo nás třeba přimět stáhnout si škodlivý kód

# Odkazy

Ilustrační příklady

*Dobrý den, váš balík s dobírkou 0 Kč je připraven k výdeji. Podrobnosti k balíku najdete na adrese [www.ceskaposte.glhf.pl/912384](www.ceskaposte.glhf.pl/912384). Vaše Česká Pošta*

- To je skutečně podezřelá internetová adresa
- Takovou bychom v žádném případě otevírat neměli
- Tak jednoduché to ale většinou nebývá …

# Odkazy

Ilustrační příklady

*Vážený kliente, od teď máte svá vyúčtování vždy po ruce. Stačí se přihlásit do vašeho internetového bankovnictví na adrese ceska-banka.cn. Vaše Česká Banka*

- Mít vyúčtování vždy po ruce zní skvěle!
- Pokud jde ovšem o vaší banku, nepozornost se nevyplácí
  - Přihlašovací údaje k internetovému bankovnictví jsou častým cíle podvodníků
- A není ***ceska-banka.cz*** jako ***ceska-banka.cn***
- Všimnout si rozdílu není vždy jednoduché
  - ceska-barka.cz | ceska-hanka.cz | ceska.banka.cz …

# Odkazy

Ilustrační příklady

*Kapacita vaší e-mailové schránky byla překročena. Od této chvíle vám nebudou chodit všechny zprávy. Pro navýšení kapacity využijte tento odkaz.*

- Tentokrát na první pohled opravdu nepoznáme, kam odkaz vede
- Bylo by lepší si jej nejdříve zkontrolovat
  - **Ale jak?**
- Pokud na odkaz najedete myší, zobrazí se vám jeho cíl
  - (ale zatím neklikat)

# Odkazy

Ilustrační příklady

*Kapacita vaší e-mailové schránky byla překročena. Od této chvíle vám nebudou chodit všechny zprávy. Pro navýšení kapacity využijte tento odkaz.*

- A hned jsme trochu moudřejší!

# Odkazy

Ilustrační příklady

*Kapacita vaší e-mailové schránky byla překročena. Od této chvíle vám nebudou chodit všechny zprávy. Pro navýšení kapacity využijte tento odkaz.*

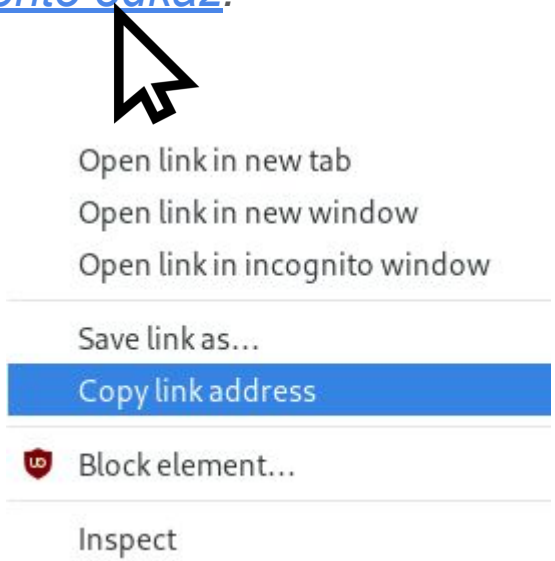

- A hned jsme trochu moudřejší!
- A někdy taky ne …
- Můžete ještě zkusit odkaz nejdříve zkopírovat jinam
  - třeba do textového soubor
  - stačí na odkaz kliknout **pravým** tlačítkem myši a vybrat z nabídky

# Odkazy

Ilustrační příklady

*Kapacita vaší e-mailové schránky byla překročena. Od této chvíle vám nebudou chodit všechny zprávy. Pro navýšení kapacity využijte tento odkaz.*

- Komplikací může být angličtina
  - pokud systém není v češtině



# Odkazy

Ilustrační příklady

*Kapacita vaší e-mailové schránky byla překročena. Od této chvíle vám nebudou chodit všechny zprávy. Pro navýšení kapacity využijte tento odkaz.*

- A pokud si stále nejste bezpečností odkazu jistí, raději jej neotvírejte
- Můžete místo toho na internetu vyhledat kontakt na svého poskytovatele e-mailové schránky a oslovit jej přes něj

# Odkazy

Shrnutí

- Pokud vám přišla zpráva s odkazem, buďte ostražití.
- Pokud vás navíc k otevření odkazu navádí, buďte dvakrát ostražití.
- Můžete odkaz nejdříve zkontrolovat
  - přejetím myší by se vám měla zobrazit skutečná cílová adresa
  - případně odkaz zkopírujte třeba do textového souboru
    - (pravým tlačítkem myši a výběrem z nabídky)
    - a ověřte, že adresa skutečně odpovídá deklarované
- A když si nejste jistí, **odkaz raději neotvírejte vůbec**
- Zadejte místo toho adresu do prohlížeče nebo vyhledávače ručně

# Reputace

Kontaktuje vás důvěryhodná instituce (úřad, policie) nebo firma (banka, mobilní operátor, jiná známá firma)?

- firmy a instituce mohou mít legitimní důvod nás kontaktovat a my jim zpravidla věříme
- ale útočník se za ně může vydávat
  - **Zpozorněte!**
- Pokud jde o mail, zkontrolujte adresu, ze které přišel.
- Pozorně si sdělení projděte a v případě pochybností

si vše radši ověřte pomocí oficiálních kontaktních údajů dané instituce/firmy.

# Reputace

## Ilustrační příklady

Z adresy info@mpsv-cz.cz vám přišla zpráva:

*MPSV vás tímto informuje, že máte nárok na příspěvek na bydlení. Žádost lze vyřídit i vzdáleně přes počítač. Pokračujte pomocí tohoto odkazu do našeho portálu. Přihlašovací údaje jsou stejné jako do vašeho e-mailu.*

- Na první pohled působí zpráva důvěryhodně
- Při **pozorném** přečtení si ale všimneme podezřelých prvků:
  - adresa odesílatele
  - odkaz

http://osklivy-scam.mpsv-cz.cz

# Reputace

## Ilustrační příklady

Z adresy info@mpsv-cz.cz vám přišla zpráva:

*MPSV vás tímto informuje, že máte nárok na příspěvek na bydlení. Žádost lze vyřídit i vzdáleně přes počítač. Pokračujte pomocí tohoto odkazu do našeho portálu. Přihlašovací údaje jsou stejné jako do vašeho e-mailu.*

- Na první pohled působí zpráva důvěryhodně
- Při **pozorném** přečtení si ale všimneme podezřelých prvků:
  - adresa odesílatele
  - odkaz
  - instrukce k zadání hesla do mailu

# Reputace

## Ilustrační příklady

Máte příchozí hovor z čísla +420 640 020 361:

*Dobrý den, tady XXX ze společnosti Microsoft. Váš počítač byl napaden hackerem a my máme povinnost vás o tom informovat a pomoci vám situaci vyřešit. Přepojím vás na kolegu a ten vám pomůže hackera zastavit…*

- Útočníci se snaží schovat za velkou firmu s dobrou reputací
- a vzbudit zdání, že opravdu jde o velkou firmu - přepojováním hovoru mezi operátory
- dále budou dávat velmi konkrétní **instrukce** (např. ke stažení a spuštění **souborů**), vyvíjet **nátlak,** útočit na **emoce**
- Pozor - číslo se dá podvrhnout (spoofing)
- Doporučení: hovor přerušit a ověřit si informace pomocí oficiálních kontaktních údajů firmy, která vám volá

# SENIOR

| | |
|---|---|
| S | Soubory |
| E | Emoce |
| N | Nátlak |
| I | Instrukce |
| O | Odkazy |
| R | Reputace |

- toto jsou nejčastější prostředky útoků internetových padouchů
- a my už víme
  - **jak je odhalit**
  - **jak jim odolat**
- ale ještě si ukážeme několik zásad užitečných před případným útokem

# Prevence - zabezpečení zařízení a účtů

- většinu uživatelských účtů a zařízení zabezpečujeme **heslem**
  - to by mělo být:
    - **tajné** - heslo nesdílím, nikam si ho nepíšu
    - **unikátní** - pro každou službu jiné heslo
    - **silné** - aspoň 12 znaků, velká a malá písmena, čísla, speciální znaky
      a neobsahuje jména, adresy, data narození, nejlépe ani žádná slova
  - pro nejdůležitější služby (datové schránky, internetové bankovnictví, mail?) používáme **dvoufázové ověření**
  - Jak si tolik hesel zapamatovat?
    - tvoříme hesla tak, aby byla snadno zapamatovat
      - Pojedeme na luka, až kukačka zakuká. -> Po1Na2Lu,Až4Ku5Za.
    - méně významná hesla můžeme uložit do správce hesel (případně uložit v prohlížeči)

# Prevence - zabezpečení zařízení a účtů

- Přístup do zařízení - telefonů, tabletů je také dobré zabezpečit
  - obzvlášť pokud zařízení používáme k dvoufázovému ověření
- Jaké jsou možnosti?
  - Heslo
  - PIN
  - Biometrie - obličej, otisk
  - Gesto - nejméně bezpečné

# Prevence - veřejné počítače a sítě

I ten, kdo nemá počítač, se může pohybovat na internetu (např. v knihovně, internetové kavárně, u známého). Je ale potřeba:

- dávat pozor na ukládání hesel, formulářů a historie v prohlížeči
- ideálně použít anonymní režim

A ten, kdo nemá mobilní internet se může dostat na internet prostřednictvím veřejných sítí.Ty nemusí být nebezpečné, ale jsou zneužitelné. Radši na nich:

- nepracujeme s citlivými službami (např. s internetovým bankovnictvím)
- nenavštěvujeme stránky, které nejsou zabezpečené certifikátem

# To by byla teorie

A nesmí chybět zdroje:

- https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/
- https://www.nukib.cz/download/vzdelavani/rozcestniky/Rozcestnik_pro_seniory.pdf
- https://osveta.nukib.cz/course/view.php?id=140#section-0

# A teď trochu praxe

https://www.kybertest.cz/

(projekt České bankovní asociace ve spolupráci s PČR a NÚKIB)

Děkujeme za pozornost