

Mezi bezpečnostní prvky proti možnosti odcizení údajů k e-mailu či hesel nepatří:

- To, že nikomu nesdělují svá hesla, ani na vyžádání.
- To, že si nastavím kontrolní otázku k e-mailu.
- **To, že si zadám jednoduché heslo (např. jméno nebo datum narození).**

Jak se mám zachovat, když dostávám hodně nevyžádané pošty:

- Nic, nevyžádané pošty se nelze nijak zbavit.
- Odpovědět na každý nevyžádaný e-mail a do předmětu zprávy vepsat NE/ANO.
- **Aktivovat funkci filtrování nevyžádané pošty.**

Za spam se nepovažuje e-mail:

- Nabízející nabídku pracovního místa, spamy nabízejí pouze zboží.
- **Od firmy, které jsem někdy v minulosti poskytl souhlas se zasíláním reklamních a informačních sdělení na mou adresu.**
- Odesílaný ze zahraničí, tedy z adresy nekončící doménou „.cz“

Co mám udělat, pokud dostanu z neznámé adresy e-mail, který mi nabízí peníze:

- Na e-mail normálně odpovím.
- Na e-mail odpovím, pouze pokud je odeslán z adresy s doménou „.cz“
- **Na e-mail neodpovídám a ihned jej smažu.**

Je odesílatelem e-mailové zprávy vždy člověk, který je zobrazen jako odesílatel:

- **Nemusí to tak být, pravého odesílatele lze snadno skrýt.**
- Nemusí to tak být, ale pouze u e-mailů odesílaných z veřejných (free-mailových) adres.
- Ano, ovšem jen pokud se vedle jeho adresy objeví i celé jméno.

On-line komunikace je:

- Marketingová komunikace určená uživatelům internetu.
- **Komunikace prostřednictvím internetu v reálném čase.**
- Komunikace probíhající v kuse, po dobu 24 hodin.

Co patří mezi nástroje rychlé komunikace na internetu:

- Kvalitní počítač a rychlé připojení na internet.
- Web relations, media, event management apod.
- **E-mail, instant messaging, chat, internetové volání apod.**

Který program umožňuje provozovat telefonování po internetu:

- QIP
- **Skype**
- Jabber

Je bezpečné se připojovat ke své e-mailové schránce z veřejně přístupného místa, například z internetové kavárny:

- **Ano, pokud nikomu neřeknete své heslo a vypnete v internetovém prohlížeči jeho automatické uložení.**
- Ano, veřejně přístupné počítače jsou ze zákona nejlépe zabezpečené.
- Ne, protože veřejně používaný počítač automaticky odesílá informace o přihlášení do veřejné databáze.

Jaké údaje zásadně nesdělují prostřednictvím e-mailu:

- Jména rodinných příslušníků.
- **Veškeré citlivé osobní údaje (rodné číslo, přihlašovací hesla, adresu atd.).**
- Své telefonní číslo do zaměstnání nebo do školy.

Pokud dostanu od neznámého uživatele e-mail s podezřelou přílohou:

- Neotevírám přílohu a ujistím se u odesílatele, že jde o přílohu neškodnou.
- Přílohu neotevírám přímo z e-mailu, ale uložím ji předtím na pevný disk.
- **Přílohu neotevírám a e-mail ihned smažu.**

Mezi nejnebezpečnější e-mailové přílohy hrozící šířením virů patří soubory:

- **Soubory s příponou .exe.**
- Soubory s příponou .txt.
- Soubory s příponou .jpg.

Službu *ignore* využiji v případě:

- Když mě někdo svými vulgárními e-maily či nabídkami obtěžuje.
- Když mi administrátor pošle nové informace o zabezpečení mé schránky.
- Když mi přítel pošle pozvání na sportovní zápas a já o něj nemám zájem.

Údaje včetně fotografií, které o sobě na sociální síti či internetu zveřejním:

- Nemohou být zneužity.
- Jednoduše vymažu, kdykoli budu chtít.
- **Sdílím se všemi uživateli a většinou je nejde vzít zpět.**

Pokud mi přijde e-mail s žádostí, abych pro zvýšení zabezpečení potvrdil jakékoli své přihlašovací heslo:

- Na e-mail odpovím a zvýším si tak svou internetovou bezpečnost.
- Na mail odpovím, ale heslo sdělím až poté, co mi odesílatel v dalším e-mailu potvrdí, k čemu přesně mé heslo potřebuje.
- **Na e-mail v žádném případě neodpovídám.**

Jak se pozná silné, tedy maximálně bezpečné heslo pro internetovou komunikaci?

- **Kombinuje všechny povolené znaky, tedy velká a malá písmena, číslice a speciální znaky, jako jsou uvozovky, závorky a další.**
- Skládá se z co možná nejdelší řady číslic.
- Skládá se z co možná nejdelší řady písmen s háčky a čárkami, které nemají nic společného se jménem uživatele.

Pokud mě někdo na chatu požádá o sdělení adresy a telefonu:

- Pošlu mu je teprve, až on mi pošle svoje.
- Pošlu mu je, ale požádám o odpovídající protislužbu (peníze, lístky do kina, kredit na mobilní telefon...).
- **Nepošlu je, jde o citlivé údaje.**

Tzv. kyberšikana hrozí nejčastěji:

- Na serverech s nevhodným obsahem.
- **Na chatech.**
- Prostřednictvím stránek na sdílení obrázků.

Co vás ochrání proti nevyžádané poště?

- Antirootkit.
- **Antispam.**
- Antivir.