



KYBERNETICKÁ BEZPEČNOST, KYBERŠIKANA

Ing. Anna Dolníková

utorok, 14. júna 2022

KYBERNETICKÁ BEZPEČNOST

CHARAKTERISTIKA

- je oblasť vedy o počítačoch, ktorá sa zaoberá:
 - odhaľovaním a eliminovaním rizík spojených s používaním informačno-komunikačných technológií

Cieľom počítačovej bezpečnosti je zabezpečiť:

- ochranu pred neoprávnenou manipuláciou:
 - so zariadeniami
 - s dátami
- ochranu pred nelegálnou tvorbou kópií dát
- bezpečnú komunikáciu a prenos dát
- bezpečné uloženie dát

KYBERNETICKÁ BEZPEČNOST

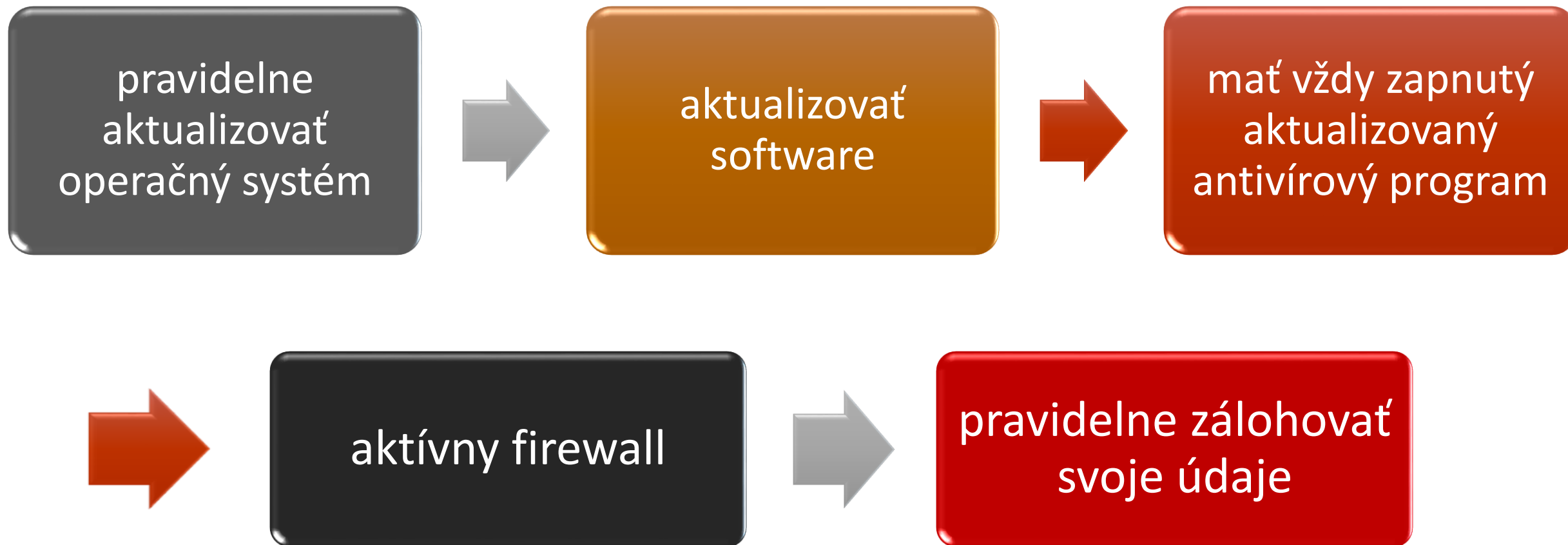
1. Zabezpečenie zariadení (počítača, notebooku, mobilného zariadenia...)

2. Zabezpečenie pripojenia k internetu

3. Heslo

1. Zabezpečenie zariadení

- počítača, notebooku, mobilného zariadenia





OPERAČNÝ SYSTÉM



- je to základný program, ktorý umožňuje užívateľovi zariadenie ovládať
- medzi najznámejšie OS patrí: Windows, Mac OS, Linux, Android, iOS...
- útočníci často využívajú chyby v OS, preto

je nutné ho pravidelne aktualizovať

- práve prostredníctvom týchto chýb v OS útočník je schopný:
 - ovládať časť alebo celý systém
 - sledovať užívateľa
 - ukradnúť alebo inak manipulovať s jeho údajmi
- je vhodné s novým zariadením kupovať aj originálny OS a nestahovať si tzv. cracknuté – čiže nelegálne stiahnuté OS*



SOFTWARE – PROGRAMY



Každý z nás používa mnoho rôznorodých programov:

- ❖ internetové prehliadače na prezeranie webových stránok
- ❖ kancelárske balíky – MS OFFICE
- ❖ rôzne ďalšie programy

Z hľadiska bezpečnosti je nutné rovnako ako OS **pravidelne aktualizovať** aj prehliadače a ostatné programy.*



ANTIVÍROVÝ PROGRAM



- je software, ktorý slúži na ochranu zariadení pred malwarom (vírusy, škodlivý software...) a to:
 - ich detekciou - odhaľovaním
 - elimináciou – vylúčením ich činností
 - a úplným odstránením zo zariadenia
- z toho je viac než jasné, že používanie neaktualizovaného antivírusového programu je celkom bezpredmetné.
- medzi najznámejšie antivírusové programy patrí: ESET, Avast, AVG, NOD32, Kaspersky atď.*



Orientačné ceny ESETu na trhu

Zlatá stredná cesta



ESET NOD32 Antivirus pre 1 počítač na 24 mesiacov SK (elektronická licencia)

Antivirus ESET NOD32 Antivirus pre 1 zariadenie, kompatibilný s operačným systémom Windows, dĺžka predplatného: 24 mesiacov, spôsob licencovania: predplatné, jazyková verzia: SK, vhodné pre domácnosti, pre firmy, pre školy a pre štátnu správu, určený pre PC, lic. kľúč nájdete v časti „Moja knižnica“ – „Licencie“

59,90 €
bez DPH 49,92 €



Ihneď na stiahnutie



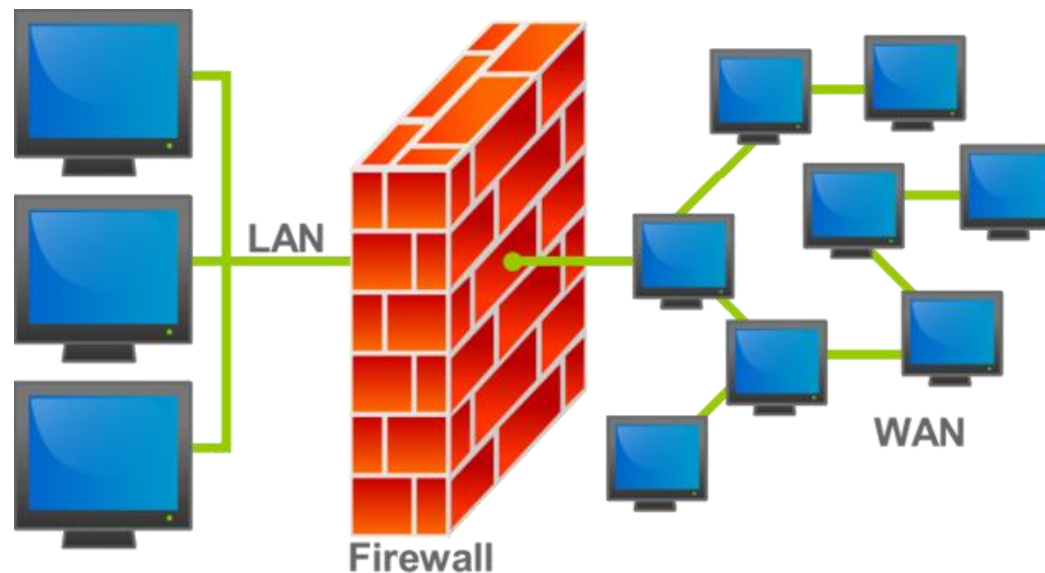
ESET Mobile Security pre Android na 12 mesiacov SK (elektronická licencia)

Internet Security, chráni smartfóny a tablety so systémom Android. Elektronická licencia je určená pre 1 zariadenie. Okrem ochrany pred škodlivým kódom poskytuje aj prémiové zabezpečenie vašich aplikácií a pomáha v prípade straty alebo krádeže vášho mobilného zariadenia. Jazyková verzia: SK; spôsob inštalácie: na stiahnutie (elektronicky); kľúč nájdete v časti „Moja knižnica“ – „Licencie“.

10 €
bez DPH 8,33 €



FIREWALL



- je program, ktorý „dohliada“ na dátový tok medzi zariadením a vonkajšou počítačovou sieťou
- je to akýsi ochranný štít pred nebezpečnými údajmi, ktoré by zariadenie mohli ohroziť
- v tomto prípade sa brána Firewall uzavrie a zabráni vstupu podozrivých informácii do PC
- bránu firewall nikdy nevypínajte!!!*



ZÁLOHOVANIE ÚDAJOV



- je jednou z najspoľahlivejších metód ochrany dôležitých údajov pred ich stratou

Na zálohovanie využívame rôzne média:

- *optické média (CD, DVD, Blu-ray)*
- *USB, externé pevné disky*
 - pozor na stratu – existujú dnes USB, ktoré je možné zaheslovať, ale je možné zaheslovať aj jednotlivé súbory
 - [USB SafeGuard](#) – program na uzamknutie USB kľúča

Tento spôsob zálohovania sa dnes používa vo veľkej miere, je potrebné ale pamätať, že aj tieto média sa môžu poškodiť, stratiť...

Inteligentné dátové úložiska

- centrálny domáci (firemný, školský) disk
 - VÝHODY: veľká kapacita
 - je možné nastaviť:
 - zálohu v pravidelných intervaloch
 - dostupnosť dát pro ďalšie zariadenia zapojené do počítačovej siete – smart TV, tablety, mobilné telefóny
 - pozor na zabezpečenie



Externé cloudové úložiská



iCloud

- jedná sa o dátový priestor na serveri prevádzkovateľa **CLOUDU** (niekde na internete), ktorý je dostupný prakticky odkiaľkoľvek a z ktoréhokoľvek zariadenia (PC, tablet, mobilný telefón)

Výhody:

- okamžitá synchronizácia dát medzi všetkými pripojenými zariadeniami
- možnosť zdieľať dáta s ďalšími užívateľmi

Nevýhody:

- závislosť na rýchlosti pripojenia
- pri väčších objemoch sú spoplatnené
- skutočnosť, že užívateľ svoje dáta zveruje „cudzej“ spoločnosti
- najznámejšie cloudové úložiská sú: Dropbox, OneDrive, I Cloud, Google Drive atď..



2. Zabezpečenie pripojenia k internetu



- pripojenie sa uskutočňuje sa prostredníctvom **ROUTRA**
- **ROUTER** je vlastne krabička s anténkou, ktorá dokáže pripojiť Wi-Fi sieť, routuje (smeruje) dátový tok medzi 2 sieťami
- práve nezabezpečený router môže byť prostriedkom k neoprávnenému prieniku do počítačovej siete
- akonáhle útočník cez náš router do našej domácej počítačovej siete prenikne, môže napr. sledovať prostredníctvom IP kamery náš súkromný život, krahnúť a zneužívať naše dáta, alebo z nášho internetového pripojenia môže ďalej páchať trestnú činnosť

Ako router zabezpečiť?

Zmeniť prístupové údaje do administrácie!!!

- do nastavenia sa užívateľ dostane tak, že v internetovom prehliadači zadá prístupovú IP adresu (najčastejšie 192.168.1.1 alebo – nájdeme na štítku nalepenom na routri) a je vyzvaný na zadanie užívateľského mena a hesla, ako by sa prihlasoval do svojho emailového účtu*
- väčšina hlavne starších routrov má tieto údaje z výroby nastavené rovnako – užívateľské meno: **admin** a heslo: **admin**.
- po prihlásení do administrácie routera je to prvá vec, ktorú je potrebné zmeniť

3. Heslo



- je reťazec znakov, ktorý sa používa ako identifikačný a overovací prvok
- spolu s užívateľským menom často tvorí základnú užívateľovu ochranu používaných zariadení (telefón, počítač apod.) alebo k rôznym aplikáciám, webovým službám, prístupu k počítačovým systémom, sieťam apod.

Dĺžka hesla

Čo je nutné dodržať:

- dĺžka hesla minimálne 8 znakov (odporúčenie 12 – 14 znakov)
- kombinácia číslíc, malých a veľkých písmen a špeciálnych znakov (!, #, \$, & apod.)

Určite nepoužívať ľahko uhádnuteľné heslá:

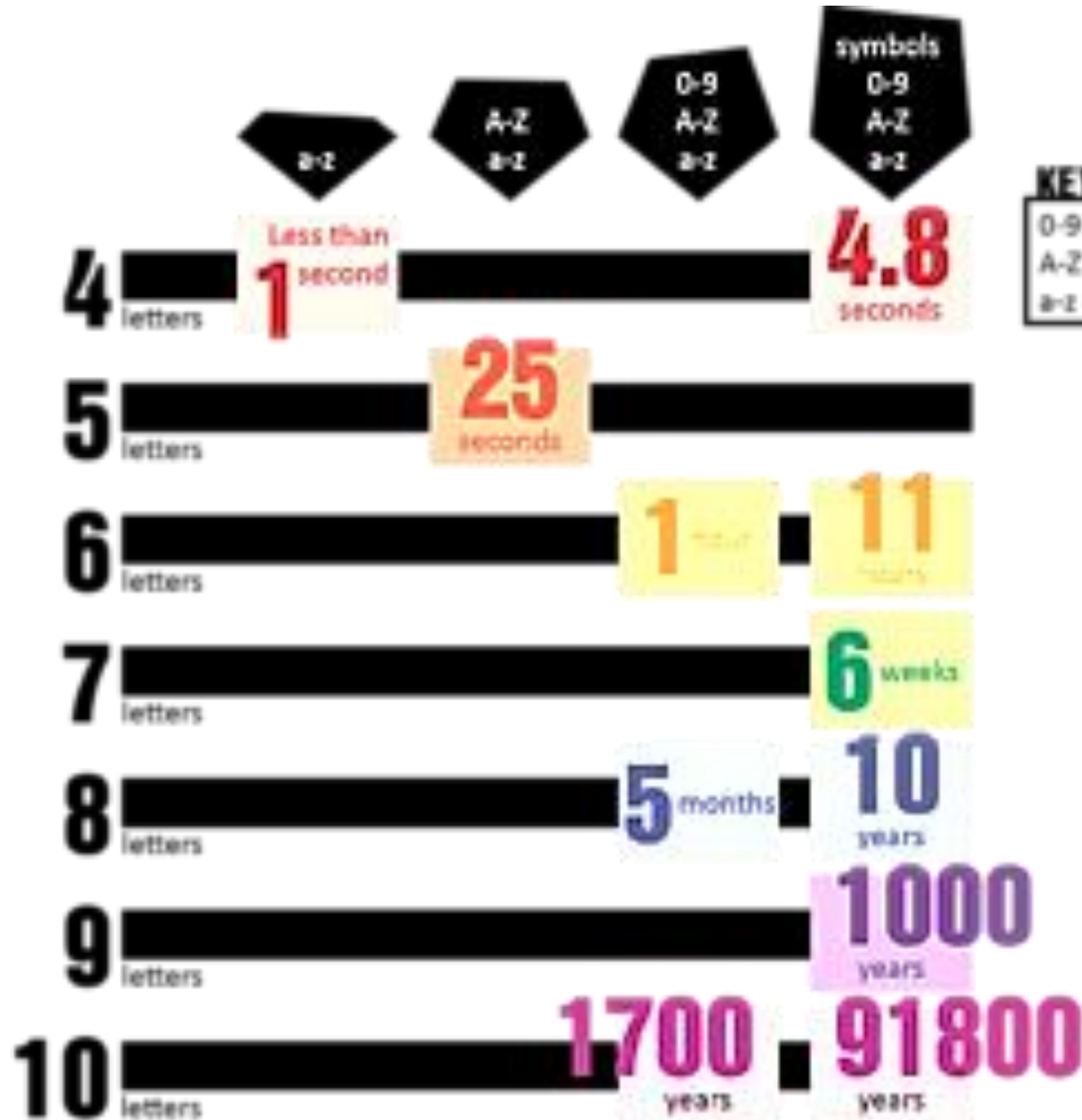
- bežné slová samostatne
- mená blízkych osôb
- dátumy narodenia
- bežnú postupnosť čísel (123456, 11111111 apod.)

Sila hesla

- určuje ako dlho bude trvať počítaču so špeciálnym programom takéto heslo prelomiť

Slovníkový útok má veľmi vysokú úspešnosť!

Metóda brute-force – teda metóda hrubou silou, využíva všetky možné kombinácie znakov a je teda značne závislá na výkone počítača



VYTVORENIE SILNÉHO HESLA

- Heslo má byť SILNÉ a ĽAHKO ZAPAMATATEĽNÉ

POSTUP TVORBY:

1. Vytvorím si ľahko zapamätateľnú frázu:

1. „môj pes má 4 nohy“

2. Vynechám samohlásky – **mjpsm4nh**

3. niektoré písmená vo fráze zmením na veľké (napr. rovnaké písmena:
MjpsM4nh)

4. pre rôzne služby, kontá si k danému heslu pridám skratku danej služby:

5. napr: e-mail a facebook

1. MjpsM4n_em

2. MjpsM4n_fb...

2. fráza:

- „mám rada pizzu“
- mmrdpzz
- mmrdpZZ
- mmrd1pZZ
- mmrd1pZZ_fb
- mmrd1pZZ_em...

Ochrana hesla

- svoje vytvorené heslo je potrebné stále ochraňovať:
 - nebudeme ho písať na papierik vedľa klávesnice
 - do poznámok v telefóne
 - a samozrejme ho nebudeme nikomu hovoriť
- **Pozor na funkciu zapamätania hesla v prehliadačoch!!!**

Dôsledkom slabého hesla môže byť:

KRÁDEŽ IDENTITY



KRÁDEŽ IDENTITY

O krádeži identity hovoríme vtedy, ak sa na internete niekto vydáva za niekoho iného

Krádež identity sa môže udiť dvoma spôsobmi:

- 1. pri registrácii, napr. na sociálnej sieti, zadaním falošných údajov,
- 2. neoprávneným získaním prihlasovacích údajov a vstup do vášho konta alebo viacerých kont

KRÁDEŽ IDENTITY - DÔSLEDKY

Napríklad:

- Ak niekto sa dostane k prihlasovacím údajom do vašej elektronickej pošty, môže:
 - posilať správy vo vašom mene, alebo z nej získať ďalšie osobné údaje
 - vytvárať objednávky na rôznych e-shopoch
 - čerpať menšie spotrebné úvery vo vašom mene
- veľmi častá býva
 - krádež identity **na sociálnych sieťach**, kde si útočník vytvorí účet inej, väčšinou verejne známej osoby (herec, spevák, politik a pod.), a začne komunikovať a prezentovať v jej mene svoje názory, robiť falošné charitatívne zbierky a pod.

AKO CHRÁNIŤ SVOJE MOBILNÉ ZARIADENIA PRED POTENCIÁLNYMI HACKERMI

AKTUALIZUJTE SVOJE ZARIADENIA

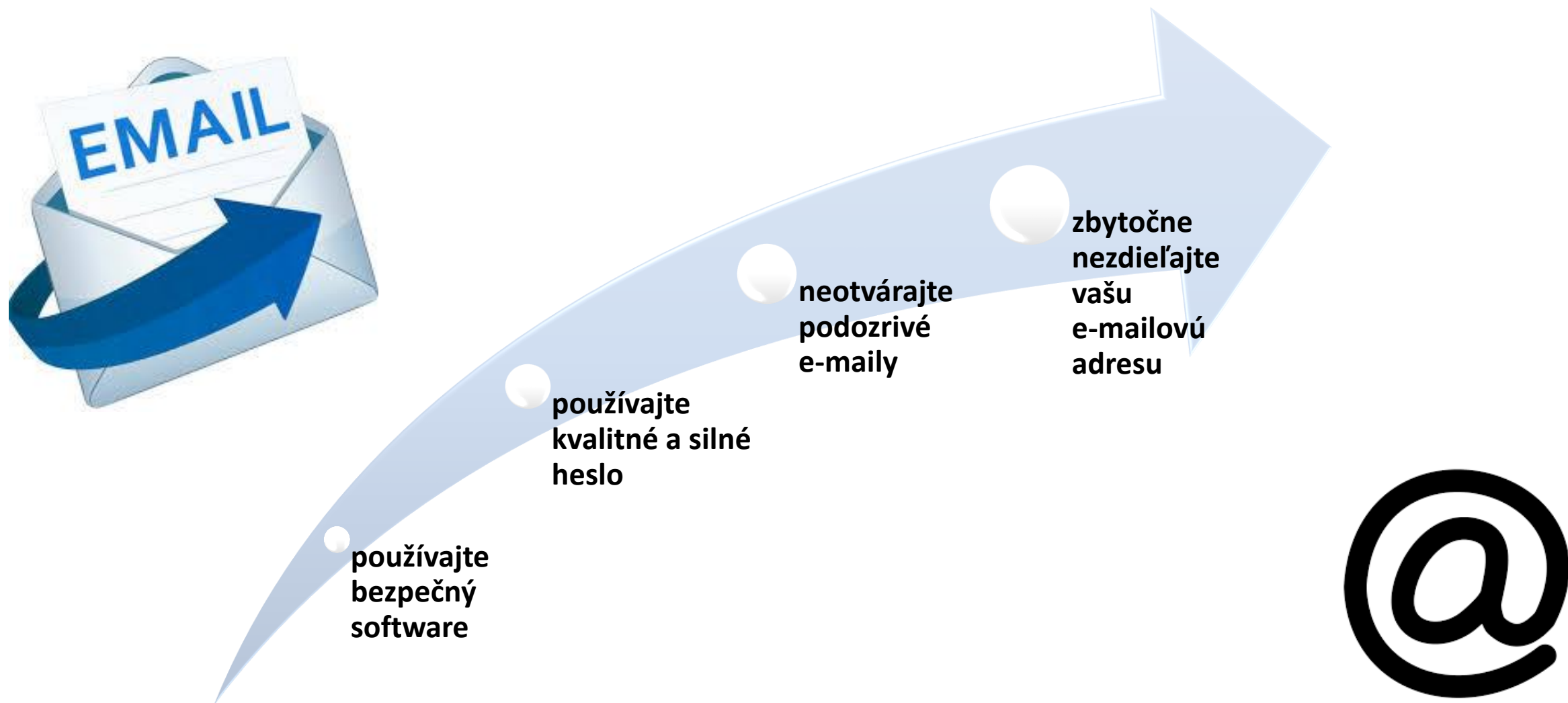
POUŽÍVAJTE BIOMETRICKÉ HESLÁ

WI-FI A BLUETOOTH ZAKÁŽTE TAK ČASTO, AKO JE TO MOŽNÉ

PRISPÔSOBTE NASTAVENIA ŠIFROVANIA



Ako účinne zabezpečiť e-mailovú schránku



Pokračujeme KYBERŠIKANOU 😊