



Školenie o GDPR a bezpečnosti v
elektronickom prostredí

Peter Bíro (CEO)



3: Základy bezpečnosti v elektronickom prostredí



Základy bezpečnosti v e-prostredí

- Súčasnosť – najcennejšia „komodita“ nie sú financie, ale informácie => informačná/vedomostná spoločnosť – sú najmä v e-prostredí!
- Zisky vďaka PC únikom/útokom prevýšili zisky z drôg
- Útok na novopripojené zariadenie do internetu [min]
- **Nič nie je 100% bezpečné**
- Bezpečnosť je len tak dôležitá, aby sa ju útočníkovi neoplatilo narušiť => **nastavenie primeranej bezpečnosti**



Bezpečnostné desatoro (1/10)

1. Bud'te obozretní!

- Neverte nikomu a to doslova. **Škodlivé odkazy** môžu prísť **od vašich priateľov**, kolegov či kamarátov na sociálnych sieťach, ktorých účty boli kompromitované.
- Ľudia, ktorých stretnete online, nemusia byť vždy tými, za koho sa vydávajú. **Falošné profily** na sociálnych sieťach sú populárnym nástrojom kyberzločincov.
- Bud'te tak obozretní a vnímaví vo virtuálnom svete, ako ste aj v tom reálnom. Ak sa vám niečo nezdá, radšej to neurobte.



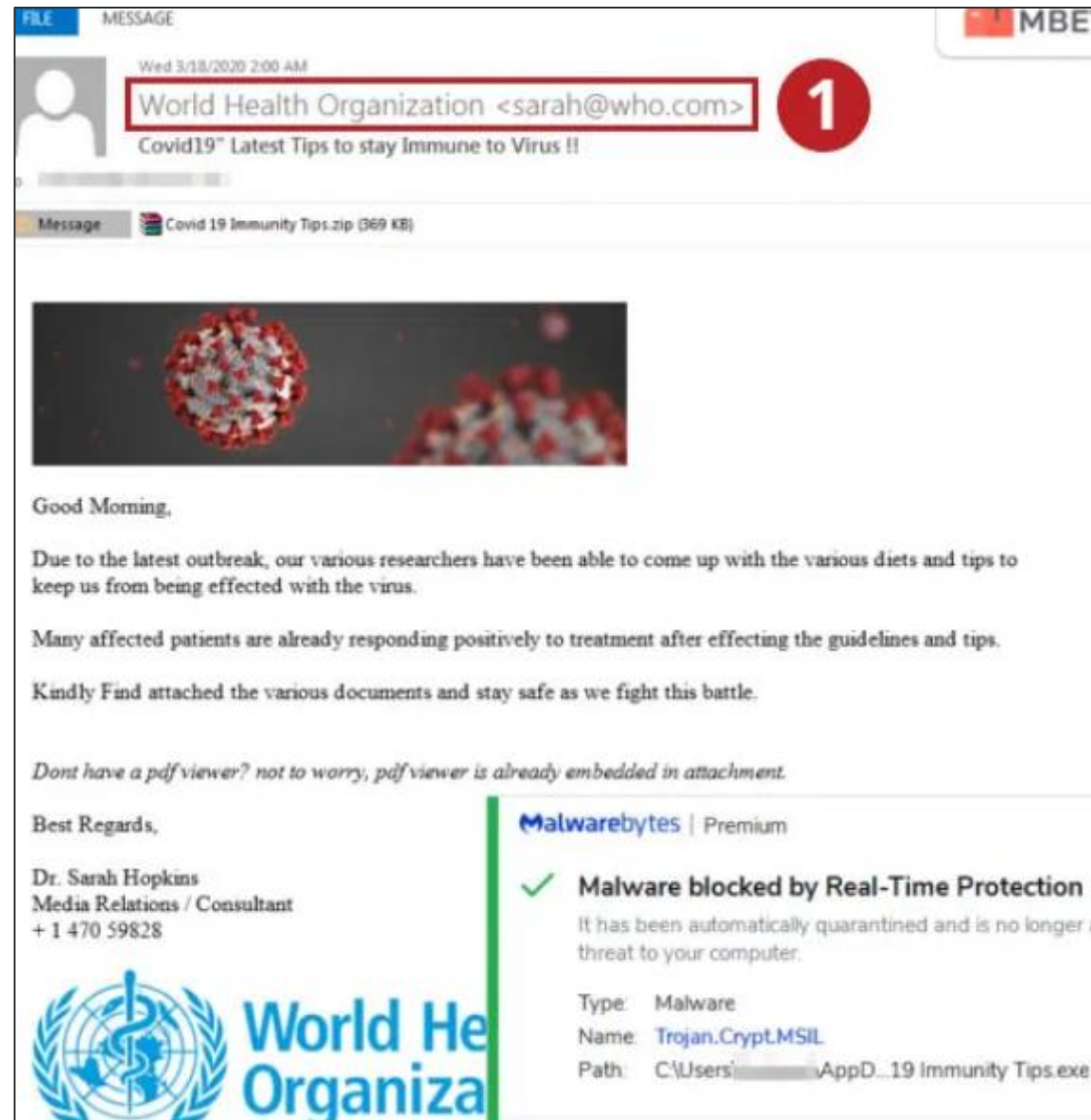
Bezpečnostné desatoro (2/10)



2. Nepodľahnite spamu a phishingu

- Kyberzločinci často rozposielajú falošné e-mailové správy, ktoré napodobňujú e-mailové upozornenia, napríklad z online obchodu alebo banky.
 - Cieľom je oklamať používateľa, ktorý pri nevedomom kliku na infikovaný odkaz rozšíri malvér.
- Nikdy neotvárajte súbory, ktoré poslal neznámy odosielateľ.
- Nikdy neklikajte na odkazy v tele SPAM e-mailu, pretože vás takýto odkaz môže zaviest' na podvrhnutý web, ktorý váš počítač infikuje škodlivým softvérom.

Bezpečnostné desatoro (2/10)



Bezpečnostné desatoro (3/10)

3. Dávajte pozor kam dávate svoje údaje

- Neposielajte osobné či citlivé (kreditná karta) údaje voľne e-mailom – e-mail = pohľadnica => aspoň zaheslovaný súbor
- Nedávajte osobné údaje kade-tade, vždy len nutné minimum – príklad:
 - ak sa chcete jednorazovo prihlásiť na nejaký neznámy diskusný portál, nikto vám nekáže dávať pravdivé údaje
- Nepíšte na sociálne siete, že niekam idete
- Ak sa na sociálnych sieťach k niečomu (politike, udalosti...) vyjadrite, je to verejné ak tam dáte fotografie, môžete ich nájsť kdekoľvek inde

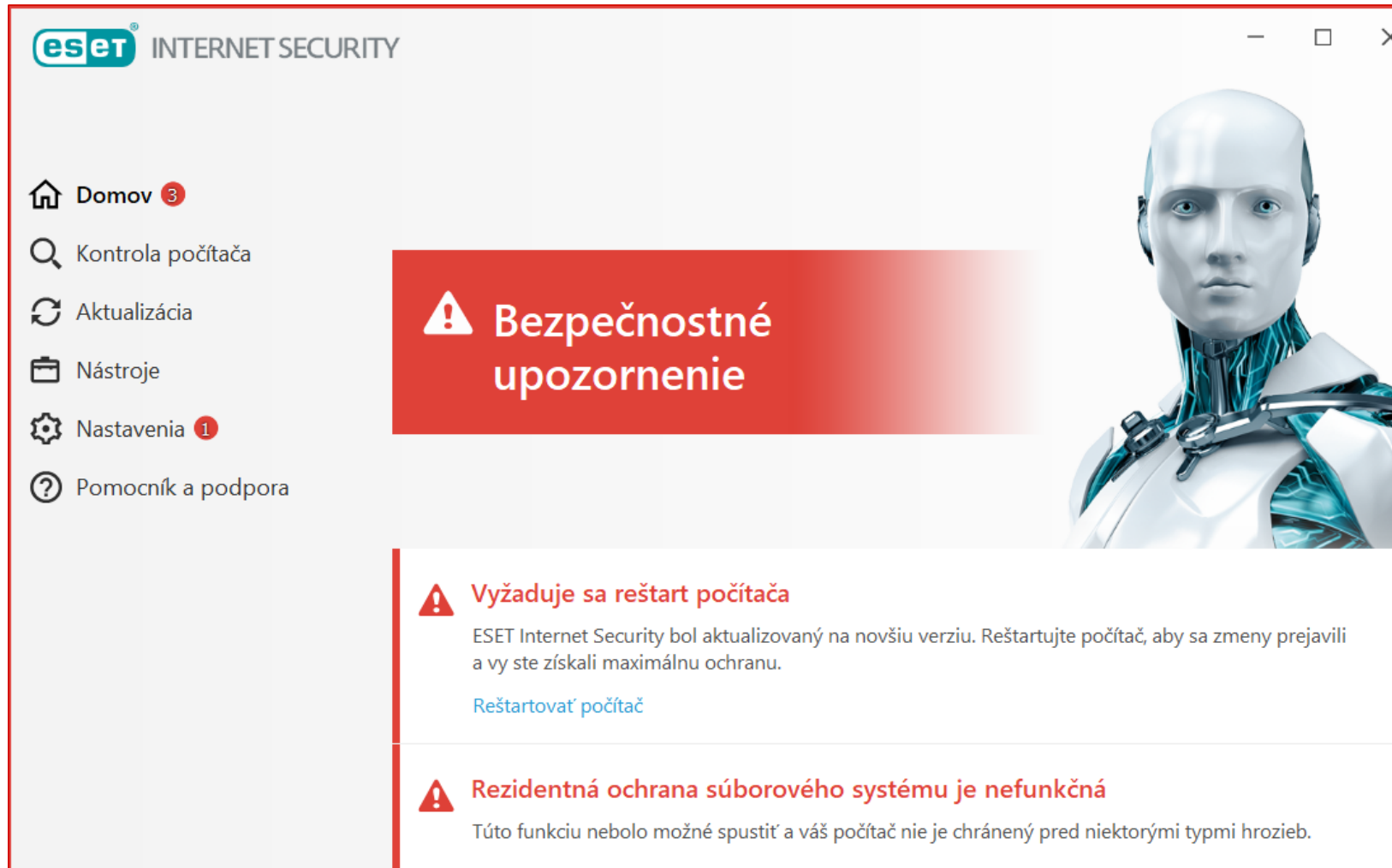


Bezpečnostné desatoro (4/10)

4. Používajte aktualizovanú ochranu pred škodlivým softvérom

- **Antivírus** – hľadá malvér - okrem zariadenia skenujte aj USB kľúče
- **Firewall** – chráni pred nechceným prenosom údajov (tam aj späť)
 - Overte si, že je Váš firewall zapnutý (napr. na OS Windows - vyhľadávacie okienko - zadajte “firewall” -> kliknúť na výsledok)
- **Webová ochrana v prehliadačoch** (blokovanie vyskakovacích okien ako prednastavené...)
-

Bezpečnostné desatoro (4/10)



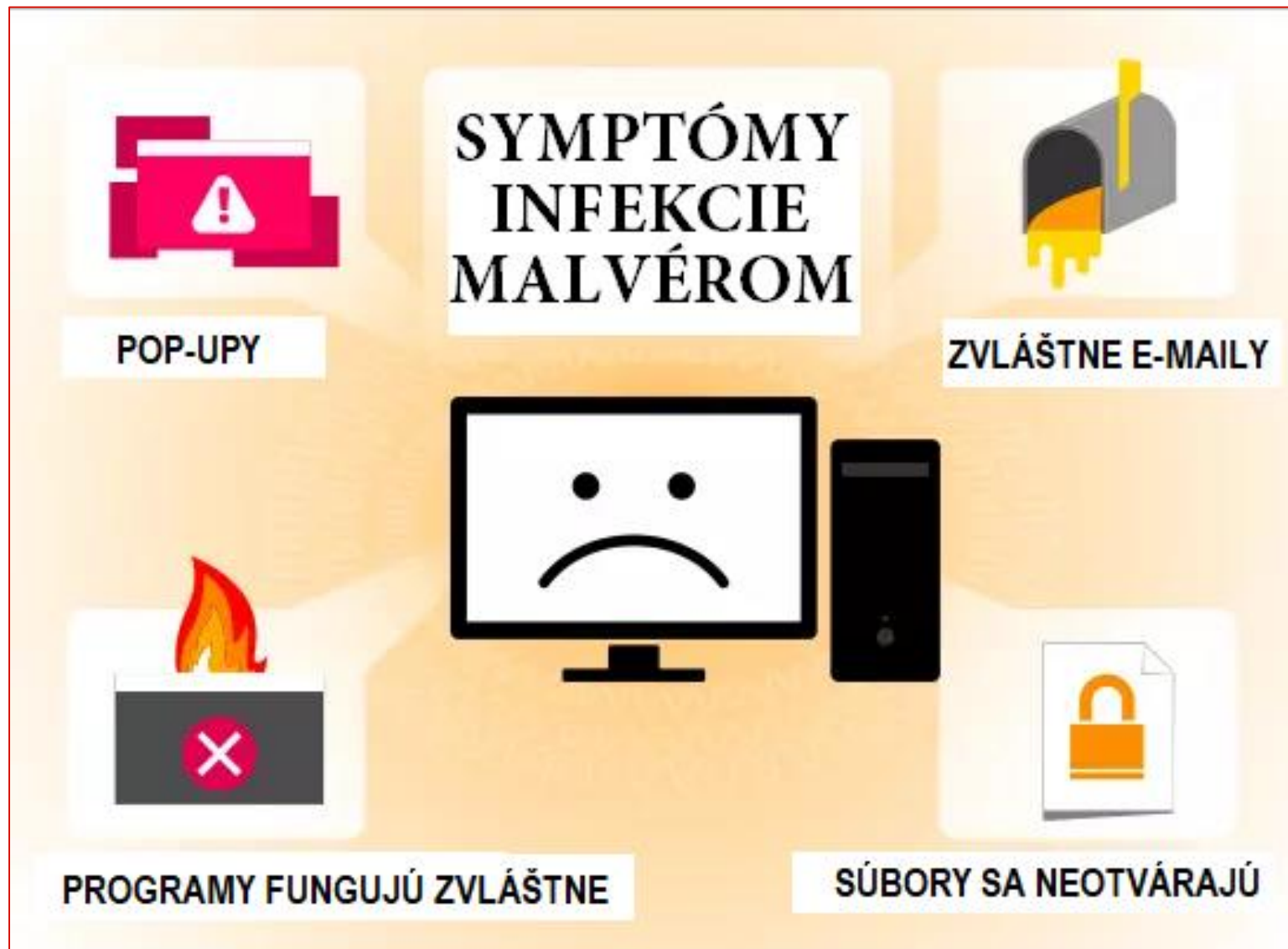
Bezpečnostné desatoro (5/10)

5. Pozor na sťahované súbory

- Jednou z TOP priorít kyberzločincov je **nevedomé stiahnutie malvéru do zariadenia**. Maskujú ho do programov a aplikácií a následne sa po jeho stiahnutí snažia napr. odcudziť údaje – typicky odchyťovanie zadaných hesiel. Horší je tzv. „ransomvér“.
- **Pozor!** Malvér môže byť prezlečený za akúkoľvek aplikáciu, od populárnych hier, až po sledovanie dopravy alebo počasia.
- Nestahujte súbory a aplikácie z nedôveryhodných zdrojov (napr. warez fóra, torrenty, porno stránky alebo pirátske filesharingové stránky)



Bezpečnostné desatoro (5/10)



Bezpečnostné desatoro (5/10)



Bezpečnostné desatoro (6/10)

6. Používajte silné a unikátne heslo

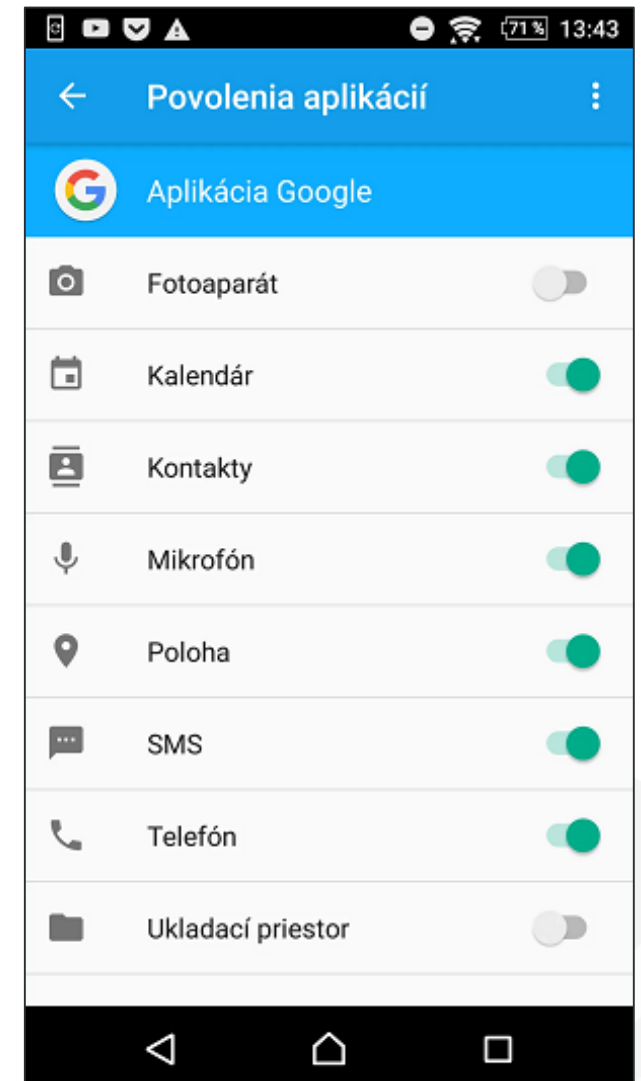
- Štandard – **aspoň 8 znakov**, aspoň 1 malé a veľké písmeno, 1 číslica a 1 iný znak (#-=+)
 - Ideálne veta predelená inými znakmi
- Prístup do banky nech je iný ako na Facebook
- Prístup do práce nech je iný ako ten doma
- Veľa hesiel = náročné na evidenciu => existujú aj nástroje na správu hesiel

~~123456~~ ~~heslo1~~ **Ked27pojdem@na10BED**

Bezpečnostné desatoro (7/10)

7. Majte povolenia pre mobilné zariadenia pod kontrolou

- Mobilné aplikácie bežne žiadajú o **súhlas pristupovať** ku kontaktom, súborom, kamere, mikrofónu, polohe... – niektoré z týchto aplikácií sú bez takéhoto súhlasu priam nepoužiteľné.
- Majte pod kontrolou povolenia, ktoré aplikáciám dávate!
- Kľudne oprávnenia **zase odoberte** alebo povoľujte prístup iba keď danú aplikáciu používate



Bezpečnostné desatoro (8/10)

8. Dbajte na bezpečné online nákupy

- Keď nakupujete online, zväčša poskytujete citlivé informácie
 - zadávajte tieto informácie iba na weboch chránených SSL (šifrovaná komunikácia) = https
 - keď sa otvorí platobná brána, skontrolujte si SSL aj tam
 - skontrolujte si aj doménu (adresu), rovnako pri presmerovaní na internet banking
- Zvážte, či sa potrebujete zaregistrovať
- Zvážte, či chcete v e-shope uložiť svoju kreditnú kartu



Bezpečnostné desatoro (9/10)

9. Vyvarujte sa cudzích zariadení

- Siete a prístupy v hoteloch – viete kto ich sleduje?
- Cudzie nabíjačky, USB kľúče... – viete, či nemajú malvér?
- Zadávate niekam PIN? Skryte si ho pred ostatnými aj prípadnou kamerou



Bezpečnostné desatoro (10/10)

10. Zálohujte... zálohujte... Zálohujte

➤ Strata

- ...3 hodiny rozpracovaného dokumentu
 - ...nainštalovaného softvéru
 - ...všetkých e-mailov
 - ...zbierky digitálnych motýľov... resp. rodinných fotografií
 - ...
-
- Dôležité súbory zálohujte viac krát a pre istotu aj na offline externý disk (výpadok el, ransom...)
 - Zálohy čas od času overte (životnosť médií...)





OTÁZKY ?

Peter Bíro (CEO)

Ďakujem za pozornosť!

Peter Bíro

SK-NIC, a.s. (správca domény .sk)

<https://sk-nic.sk>

Prednáška je autorským dielom a je chránená v zmysle autorského zákona č. 618/2003 Z. z. v znení neskorších predpisov. Akékoľvek použitie je možné výlučne s predchádzajúcim súhlasom a za podmienok určených autorom.

