

ABECEDA BEZPEČNOSTNÉHO POVEDOMIA



A

AKTUALIZUJTE A PLÁTAJTE

Váš počítač, smartfón, wifi router a všetky IT zariadenia musia mať vždy nainštalované posledné verzie aktualizácií a záplat operačného systému. Týka sa to aj internetového prehliadača a všetkých aplikácií. Hackeri ako prvé hľadajú známe zraniteľnosti v neaktualizovaných systémoch, čiže bezpečnostné diery, a tie treba plátať.



C

COOKIES PATRIA DO KOŠA

Pravidelne vymazávajte cookies a vymažte históriu internetového prehliadača. Aj keď je technológia „cookies“ regulovaná európskym právom, mnohí prevádzkovatelia svoje povinnosti nedodržiavajú.



E

E-MAIL NIE JE BEZPEČNÝ

Správa elektronickej pošty je ako korešpondenčný lístok. Nikdy nemáte istotu, že odosielateľom je ten, za koho sa vydáva. Obsah správy môže prečítať množstvo neznámych ľudí. Pokiaľ nepoužívate šifrovaný e-mail, vážte informácie, ktoré odosielate.



G

GROOMING

Chráňte sa pred groomingom. Výraz „groom“ znamená „pripraviť na špecifickú pozíciu alebo účel“ či „pripraviť na budúcu rolu alebo funkciu“. Groomingom si útočník „pripravuje“ dieťa, rodinu, komunitu tak, aby mohol neskôr realizovať sexuálne zneužívanie. Iným slovami je to pestovanie si vzťahu a budovanie dôvery medzi sexuálnym predátorom a jeho obeť.



GH

CHRÁŇTE SÚKROMIE

Sociálne siete navádzajú k tomu, aby ste prezradili o sebe čo najviac. Výsledkom bývajú vykradnuté domácnosti počas dovolenky, odcudzené peniaze z bankových účtov, ale aj sexuálne vydieranie či ujma na duševnom zdraví dieťaťa, napríklad prostredníctvom kyberšikany. Rešpektujte zároveň právo na súkromie iných ľudí.



J

JE TO PRAVDA?

Hoax je podvodná správa, zámerne konštruovaná tak, aby pôsobila ako dôveryhodná a objektívna pravda. Táto technika využíva manipuláciu na zneužitie vlastností ľudského rozhodovania.



B

BUĎTE OSTRÁŽITÍ

Pred kliknutím na akýkoľvek odkaz v správe elektronickej pošty si overte, kam tento odkaz naozaj smeruje.



D

DODRŽUJTE PRAVIDLÁ

Bezpečnostné politiky vašej organizácie a odporúčania informatikov a „bezpečákov“ nie sú samoúčelné. Obchádzanie pravidiel vám možno zvýši používateľský komfort, avšak pravidlá vám zaručia súkromie a bezpečnosť vašich cenných údajov.



F

FILTRUJTE SPAM

Nástroje na „odchytávanie“ nevyžiadaných a škodlivých správ elektronickej pošty znižujú riziko infiltrácie a ohrozenia vášho systému.



H

HESLÁ A HESLOVÉ VETY

Silné heslá sú tie, ktoré nikto neuhádne a zároveň si ich pamätáte. Vytvorte heslá, ktoré majú aspoň 15 znakov a obsahujú kombináciu veľkých a malých písmen, čísl a symbolov, ak to aplikácia umožňuje. Heslovou vetou môže byť napríklad citát, alebo text skladby, kde nahradíte aspoň jedno písmeno špeciálnym znakom a pridáte číslice.



I

INŠTALUJTE SI ANTIVÍRUS

Voči útoku škodlivým kódom vás obránia najmä antivírusové aplikácie. Nainštalujte si niektorú z nich a nastavte ju tak, aby automaticky kontrolovala prístupy na webové stránky, sťahované súbory, prílohy e-mailov a pamäťové médiá.



K

KONTROLUJTE ADRESY

Pred otvorením webovej stránky vždy najprv skontrolujte adresu. Nespúšťajte neznáme odkazy. Podhodenie adresy a presmerovanie na nebezpečnú webstránku je typickým spôsobom prípravy útoku. Neotvárajte neznáme prílohy a linky v správach, väčšinou je ich obsahom škodlivý kód.

