Scenár 12

Téma:

Ako na bezpečné heslo?

Autor:

Rajmund Modriansky

Ako na bezpečné heslo?

Scéna 1

Interiér. Škola. Trieda informatiky. Žiak sedí na stoličke pred monitorom počítača a hovorí:

„Ak používate stále rovnaké heslo typu „milacik" pre všetky internetové služby od Facebooku až po email, je to podobné, ako keby ste si nechali spraviť jeden kľúč od dverí do domu, schránky, kancelárie, domu rodičov a potom ho schovali pred dvere pod rohožku, aby sa nestratil.

Mať silné heslo pre služby je dnes dôležitejšie ako kedykoľvek predtým. Stačí, ak si uvedomíte, ako veľmi sa za posledných päť rokov zmenil spôsob, akým sa hýbete na internete.

V komunikácii sa ľudia čoraz viac spoliehajú na email a sociálne siete, ktoré chráni len kombinácia emailovej adresy a hesla. Ak používate stále rovnaké heslo, jeho únik spôsobí, že sa v nebezpečenstve ocitne všetko, čo na webe robíte. Pri rastúcom množstve rôznych webových služieb je únik dát otázkou času.

A preto sme tu teraz my, aby sme všetkým pripomenuli, že „**Bezpečnosť zanedbávame"**

Informácie vo veku neobmedzených veľkostí emailových schránok ostávajú v archívoch. Ak sa dakto dostane do schránky, môže nájsť aj pred rokmi poslané rodné číslo či číslo kreditky, alebo prihlasovacie údaje do inej služby.

Úplne samostatnou kapitolou sú škody, ktoré môže napáchať niekto, kto sa vám vláme do facebookového účtu a spraví z vás rasistu, zdroj spamu a milovníka či v horšom prípade aj šíriteľa nevhodného obsahu.

Podľa prieskumu agentúry Accenture z roku 2008 približne polovica ľudí používa len jedno heslo na všetky internetové služby, a to napriek tomu, že väčšina si uvedomuje, že je

to nebezpečné. Prieskum spoločnosti Tufin Technologies zasa ukázal, že polovici z amerických vysokoškolákov sa niekto dostal do emailu alebo facebookového účtu.“

Strih

Text na obrazovke: „Na čo dať pozor“

Scéna 2

Interiér. Škola. Trieda. Žiak stojí pred bielou stenou.

„Základným pravidlom je, že treba mať dobré a rozdielne heslá pre dôležité služby. Obzvlášť pre email a sociálne siete. Tam sa vyskytuje najviac informácií a môže tam dôjsť k najväčším škodám. Jedinečné heslo pre každú službu zaručí, že ak niekto nepovolaný získa prístup napríklad k účtu na Facebooku, nebude ho vedieť využiť na to, aby sa dostal do iných služieb.

Dobré heslo nesmie byť uhádnuteľné a nemalo by sa ani nachádzať v bežnom jazyku, aby ho nemohli uhádnuť automatické „hádače hesiel“, ktoré skúšajú do účtu preniknúť pomocou často používaných slov. Malo by obsahovať najmenej osem znakov, číslo a špeciálny znak.

Čiastočným riešením je aj vytvoriť si jednoduché odpadkové heslo pre služby, ktorých strata nespôsobí väčšiu škodu, a používať silné heslá pre kľúčové služby.“

Strih

Text na obrazovke: „A ako si vytvoriť bezpečné heslo?“

Ďalší text na obrazovke: (k tomu zvukový komentár)

V ideálnom prípade by ste mali vytvoriť špeciálne heslo pre každú z dôležitých stránok. Výhodou je, že namiesto spelti znakov si môžete do pamäti uložiť len frázu, číslo a špeciálny znak. Pre neuhádnuteľné 15-znakové heslo si stačí zapamätať tri veci.

Všeobecné pravidlo pre bezpečné heslá:

- Nesmie byť čitateľné", teda nemalo by mať v jazyku žiadny skutočný význam
- Má obsahovať kombináciu písmen, čísel a špeciálnych znakov
- Nepoužívajte rovnaké heslo pre viacero dôležitých služieb

Zvukový komentár k zobrazenému textu 1:
„Vyberte si ľahko zapamätateľné slovné spojenie, napríklad – mám rád čokoládu. Vynechajte všetky medzery a samohlásky. Na ľubovoľné miesto pridajte číslo a špeciálny znak – napríklad zavináč, mriežku, percento alebo hviezdičku. A máte bezpečné heslo."

Zvukový záznam k zobrazenému textu 2:
Prečítať to isté, čo bude na obrazovke o pravidlách bezpečného hesla.

Záver:

Scéna 3
Interiér. Škola. Trieda. Žiak stojí pred bielou stenou.

„Ďakujem za pozornosť a dúfam, že ste sa z môjho videa poučili.“

KONIEC