

JAK NA SILNÉ HESLO?

1 BUĎTE ORIGINÁLNÍ

Hackeri vlastní statistiky hesel a znají nejčastější postupy při jejich tvorbě. Proto nad vytvářením hesel přemýšlejte a nespěchejte. Přidáním speciálního znaku např. ? nebo : to hackerům dost znepříjemníte.

2 ZAPOMEŇTE NA OBLÍBENÉ LIDI A VĚCI

Spoustu osobních informací lze snadno dohledat na internetu. Zapomeňte proto na hesla jako jsou: vaše jméno, jména dětí, datum narození nebo jméno vašeho zvířete.

3 DÉLKA SE POČÍTÁ

Čím delší a složitější heslo zvolíte, tím déle potrvá jeho rozluštění. Ideální je min. 12 znaků. Může jít např. o frázi, pozměněnou hlášku z filmu apod. Prostě to, co si dobře zapamatujete.

4 VYUŽÍVEJTE SPECIÁLNÍ ZNAKY

Zde platí obdobné pravidlo jako s délkou - heslo pouze z písmen útočník prolomí rychleji než kombinaci různých znaků. Využijte češtinu: ř, š, ů, ě, přidejte čísla a speciální znaky, třeba ? !)

5 POUŽÍVEJTE GENERÁTOR HESEL

Pokud budete neustále vymýšlet nová hesla, nejspíš si budou v něčem podobná. Nechte to na náhodě a nechte si vygenerovat nesouvisející směs znaků. Využijte správce hesel. např. vimheslo.cz

6 ZAMĚŇTE PÍSMENA ZA ČÍSLICE

Ve svém hesle zaměňte některá písmena za číslice. Např. místo písmeno A uděláme číslici 3. Naše heslo je sedmikraska a vznikne sedmikr3sk3. To už vypadá bezpečněji, nemyslíte?

7 PRO KAŽDOU SLUŽBU JINÉ HESLO

To znamená: nepoužívám univerzální heslo! Kamkoliv se přihlašuji, vždy používám jiné heslo, ať už by šlo o obměnu např. zkratkou služby, do které se přihlašuji. =email3 =banka3

8 VYUŽÍVEJTE SPRÁVCE HESEL

Děsí vás délka a množství hesel, které po vás chceme? Nezoufejte. Hravě vám s tím pomůže správce hesel, kde budete mít všechny přístupy na jednom místě. Využijte např. vimheslo.cz

9 OVĚŘUJTE DVOUFÁZOVĚ

Jakmile můžete bezpečnost posílit dalším ověřením vaší identity, udělejte to. Jde např. o SMS s kódem, kliknutí na odkaz v e-mailu nebo o opsání kódu z aplikace.

10 NEPODCEŇUJTE BEZPEČNOSTNÍ OTÁZKY

Podobně jako u bodu č. 2 - nedají se o vás tyto údaje dohledat? Pokud můžete, zvolte netradiční otázky nebo raději úplně jiný způsob ověření vaší identity. Např. alternativní e-mailovou adresu.

