

JAK NA BEZPEČNÉ HESLO

Své důležité účty, mezi které určitě patří účet v bance nebo např. e-mailová schránka či účet na sociální sítích, si zabezpečte tzv. silným heslem. Tedy heslem, které je:

- neodhadnutelné (NE vaše jméno, jméno někoho blízkého nebo mazlíčka),
- nezjistitelné roboty (hesla á la „password“ či „12345“ a slova ze slovníku).
- dostatečně dlouhé (doporučuje se minimálně 12 znaků, mělo by obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků).

Nastavte si heslo, kterým se budete přihlašovat. Heslo musí mít minimálně 8 znaků a zároveň by mělo splňovat minimálně 2 z následujících podmínek:

- jedno VELKÉ písmeno
- jedno malé písmeno
- jednu číslici
- jeden speciální znak

Heslo pro vaše důležité účty (jako např. internetové bankovníctví, sociální sítě, e-mail) by mělo být navíc UNIKÁTNÍ - tzn. pro každou službu jiné, a samozřejmě silné heslo. Rozhodně nedoporučujeme, abyste měli jedno jediné heslo pro bankovní účet a sociální sítě či e-mail.

JAK VYTVOŘIT SILNÉ HESLO?

Jedna z metod, s níž lze vytvořit silné heslo, je pomoci si nějakým textem, který si pamatujete. Třeba vaší oblíbenou písničkou, příslovím, citátem apod.

Písnička „Čtyři páry bílých koní, podkovy jim pěkně zvoní.“ může posloužit jako dobrý příklad.

Vezměme první slovo zapsané jako číslici, čárku mezi dvěma verši jako speciální znak a z ostatních slov třeba první písmena – a máme poměrně silné heslo: 4pbk,pjpz.

To můžeme vylepšit tak, že každé druhé písmeno změníme na velké: 4pBk, PjPz.

Vytváření silného hesla může být nakonec vlastně i docela zábavné. Chcete-li například ještě posílit, znovu zopakujte všechny znaky, ale posuňte se o znak dále (např. za písmenem p je v abecedě písmeno q, po písmenu z opět první písmeno abecedy a) a oddělte pomlčkou. V našem případě by výsledné heslo bylo 4pBk, PjPz.-5qCl,QkQa.

JAK SI HESLO UCHOVÁVAT?

Nejbezpečnější je vaše hlava, svá hesla si prostě zapamatujte, opravdu to za tu „práci“ stojí, vždyť v případě některých účtů jde o vaše peníze. Pokud máte potřebu si heslo zapsat, pak jej ukládejte na bezpečné místo, nenechávejte papírek s heslem v blízkosti či přímo na zařízení, které jím lze otevřít. V případě platebních karet

není bezpečným místem pro uložení PINu ani vaše peněženka, ani váš mobil. Důležitá hesla neukládejte do počítače, respektive do webového prohlížeče, který používáte.

Pokud máte hodně hesel, můžete využít i speciální aplikace „správce hesel“, ale pozor, i do nich se budete muset přihlásit bezpečným a silným heslem.

MĚNIT HESLO ČI NEMĚNIT?

V případě, že používáte výše popsaná silná, tedy bezpečná hesla, není v podstatě třeba je v nějakém pravidelném intervalu měnit. Samozřejmě je ale nesmíte s nikým sdílet a musíte mít jistotu, že nebyla třeba uložena v nějaké databázi hesel, která unikla na veřejnost. Máte-li podezření, že vaše heslo bylo prozrazeno, například slyšeli-li jste o nějakém velkém úniku ze sociální sítě, kterou používáte, případně chcete-li mít jednoduše jistotu, heslo změňte. Nezapomeňte ale, že nové heslo musí být opět silné!

JAK TO UDĚLAT JEŠTĚ BEZPEČNĚJŠÍ?

Ještě bezpečnějším způsobem, jak ověřit, že ten, kdo se chce přihlásit do nějaké aplikace, je skutečně tím, za koho se vydává, je tzv. dvoufaktorové ověřování. Tento způsob je třeba využíván bankami v rámci nástrojů internetového bankovníctví (po zadání hesla vám např. na mobilní telefon přijde SMS zpráva s kódem, který slouží jako další faktor ověření). Ještě bezpečnější je pak tyto kódy přijímat ve speciální aplikaci. Vaše banka vám jistě poradí, jak na to.