**10 tipů na bezpečné zacházení s hesly**

1. **Dejte si tu práci s vytvořením originálního hesla pro každý účet.** Především pro ty klíčové, jako je e-mail, Facebook nebo internetové bankovnictví.
2. **Hlídejte si, jestli přihlašovací údaje opravdu zadáváte pouze tam, kam máte.** [Phishing](http://www.chytraskola.visualio.cz/clanek/9/phishing-viry-a-socialni-inzenyrstvi/1986) (česky rybaření) je metoda [sociálního inženýrství](http://www.chytraskola.visualio.cz/clanek/9/phishing-viry-a-socialni-inzenyrstvi/1989), která vás může zmást k zadání přihlašovacích údajů na úplně jiném webu, než kam patří. Phishingové útoky například běžně vytvoří kopii přihlašovacích stránek internetového bankovnictví.
3. **Své přihlašovací údaje nikdy nedávejte nikomu cizímu.** Pamatujte si, že provozovatel webu, aplikace či softwaru vaše heslo nejenom nepotřebuje, ale také vám ho nemůže říct – nemá a nesmí ho mít uložené v databázi. K přihlašování se ve skutečnosti používá jenom matematický „otisk“ vašeho hesla – z toho původní heslo zjistit ani nejde.
4. **Pokud jste s nějakou službou, programem či aplikací přestali pracovat, tak se odhlaste.** Platí to zejména tam, kde počítač nebo zařízení mohou použít další lidé. Ve škole, v práci, v kavárně. Výjimkou může být váš domácí počítač, ale i tam možná budete chtít být opatrní, pokud k němu mají přístup děti.
5. **Nenechte internetový prohlížeč pamatovat si hesla, pokud není počítač přímo a jenom váš.** Ani ten by si ale neměl pamatovat zásadní hesla, jako je heslo k vašemu e-mailu či do internetového bankovnictví.
6. **Hesla se neposílají e-mailem ani chatem.** Bezpečné příliš není ani poslání přes SMS. Vždy se může najít někdo, kdo takhle k heslu získá přístup.
7. **Hesla si nepište nikam, kde je možné si je volně přečíst.** Nepatří na lepicí lísteček na váš monitor, není vhodné je ukládat v souboru v počítači. S výjimkou toho, že použijete šifrování, a soubor s hesly je tak zabezpečený proti neoprávněnému přístupu.
8. Pravidelná změna hesla je nebezpečný mýtus, za který se jeho tvůrce již celému světu omluvil. **Heslo si měňte pouze tehdy, pokud je k tomu důvod** – zejména pokud došlo k jeho prozrazení.
9. **Chraňte si počítač, notebook i telefon antivirovým softwarem.** Heslo vám může ukrást i virus v počítači, pro který se používá označení [keylogger](http://www.chytraskola.visualio.cz/clanek/9/phishing-viry-a-socialni-inzenyrstvi/1987) (zaznamenává stisky klávesnice).  Bezpečnostní otázky jsou velmi častý důvod hacknutí účtů, nikdy na ně nedávejte reálné odpovědi. Něco si vymyslete nebo dejte jako odpověď další unikátní heslo.
10. **Snažte se používat správce hesel,** které vytvoří unikátní a složité heslo a zapamatují si ho za vás. Můžete v nich mít stovky hesel, aniž by bylo potřeba si je skutečně pamatovat. Některé umí i varovat, pokud se vaše hesla objevila v seznamu uniků.