

# Hesla

Heslo .....	1
Co je to nebezpečné heslo? .....	1
Co je to bezpečné heslo? .....	2
Prolamování hesel .....	2
Tvorba hesel .....	3
Doporučení .....	3
Software .....	3
Generátory .....	3
Správce hesel .....	4
Závěr .....	4

## Heslo

Heslo je souvislá sekvence znaků, které se používají k tomu, aby se počítačový uživatel prokázal, že skutečně je oprávněným uživatelem<sup>1</sup>.

Takové definici odpovídá de facto jakákoli kombinace kláves, ovšem každý uživatel by si měl uvědomit, že heslo musí být primárně bezpečné. Slouží k zamezení přístupu neoprávněným osobám a tím pádem by i jeho kvalita měla být adekvátní.

Hesla lze laicky rozdělit na bezpečná a nebezpečná.

## Co je to nebezpečné heslo?

Nebezpečné heslo je takové, které lze velmi jednoduše odhalit. Toho lze dosáhnout buď prostým testováním často používaných hesel, nebo při lepší znalosti dané osoby lze použít i sofistikovanější metody jako jsou například rodná čísla, jména členů rodiny nebo domácích mazlíčků a jiné více či méně úsměvné kombinace.

V počátcích fungování webu bylo nejpoblárnějším heslem „12345“. Dnes je tato číselná kombinace o jednu číslici delší, tedy „123456“. Každý pátý uživatel používá snadno odhadnutelná hesla jako například „abc123“, „iloveyou“ nebo „password“.

Důkazem o lehkovážnosti při stanovování hesel jsou odcizená hesla 32 milionů uživatelů amerického serveru RockYou. Téměř 1 % z nich mělo nastaveno heslo „123456“, druhé nejčastěji používané bylo „12345“. Do nejlepší dvacítky se probojovala i hesla jako „abc123“, „qwerty“ a „princess“. Celkem 20 % uživatelů, což představuje přibližně 6,4 milionu lidí, volilo svá hesla z portfolia 5.000 hesel. Proč si však lidé vybírají taková hesla? Dle Jeffa Mosse, zakladatele populární hackerské konference, je tento fakt dán tím, že v dnešní době jsme zahrnuti informacemi a musíme si pamatovat i 10 \* více hesel, než tomu bylo před 10 lety<sup>2</sup>.

Jiným nebezpečím, které je stále častější a ve kterém již nehraje síla hesla svou úlohu, jsou phishingové útoky. Dnes a denně je možné se setkat s internetovými stránkami, které mají nám známý obsah, ovšem s prazvláštní internetovou adresou. Vložit své heslo do připravených formulářů je díky důmyslnému sociálnímu inženýrství jen otázkou inteligence či nepozornosti

<sup>1</sup>Zdroj: [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci213800,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213800,00.html)

<sup>2</sup>Zdroj: <http://www.nytimes.com/2010/01/21/technology/21password.html>

jedince, který potvrzením formuláře odevzdává svůj účet do rukou hackerů.

Naprostě legitimním nebezpečím je u některých účtů možnost získání přístupu k účtu pomocí bezpečnostní otázky. I kdyby totiž bylo heslo sebevíc bezpečné, odpověď na bezpečnostní otázku může být natolik jednoduchá, že heslo již nemá význam.

## Co je to bezpečné heslo?

I když není vždy možné předejít hrozbě phishingu, snadno lze ovlivnit sílu zabezpečení hesla, které jedinec používá. Jak by se nejspíše dalo očekávat, používání jednoho stejného hesla není tou nejlepší metodou k ochraně dat.

Bezpečné heslo je tedy unikátní, dlouhé a mělo by obsahovat více než málo znaků. Tato vágní formulace dává najevo, že neexistuje nejkratší délka hesla, která by představovala hranici mezi bezpečnými a nebezpečnými hesly, ovšem s větší délkou narůstá geometrickou řadu doba nezbytná k jeho prolomení.

Bezpečné heslo není ani slovo, které je běžně k nalezení v nějakém slovníku, protože právě slovníkové útoky jsou často oblíbenou metodou k testování hesel.

Je taktéž nevhodné heslo vystavovat veřejně na internetu, a to ani tím způsobem, že by jej někdo posílal svým známým pomocí elektronické pošty, komunikátorů nebo jinými způsoby. Podobně nevhodné řešení je ukládání do TXT nebo XLS souborů s názvem „hesla“. Úplně nejhorším řešením je nalepit si papírek se svým bezpečným heslem na monitor.

K lepší bezpečnosti hesla přispěje i jeho pravidelná obměna.

## Prolamování hesel

Jak je snadné či neskadné heslo prolomit? Níže uvedená tabulka předkládá dobu potřebnou na nalezení hesla v závislosti na jeho délce a použitých znacích. Rychlost vyhledávání hesel je 100.000 za vteřinu.

Počet znaků	a-z (26 možností)	a-z, 0-9 (36 možností)	a-z,A-Z (52 možností)	Všechny tisknutelné znaky (96 možností)
4	0	0	1 minuta	13 minut
5	0	10 minut	1 hodina	22 hodin
6	50 minut	6 hodin	2,2 dnů	3 měsíce
7	22 hodin	9 dní	4 měsíce	23 let
8	24 dní	10,5 měsíců	17 let	2 287 let
9	21 měsíců	32,6 let	881 let	219 000 let
10	45 let	1 159 let	45 838 let	21 000 000 let

Zdroj: <http://lastbit.com/psw.asp>

S rychlejšími stroji by se však tyto odhady výrazně měnily. Naopak šance uživatelů na bezpečnější heslo by rostla s využíváním lokalizovaných znaků, kterých má třeba i čeština hned několik. Ne vždy to však musí nést kýžený efekt, pokud se náhodou uživatel ocitne na druhé straně zeměkoule a chce přistoupit přes japonský počítač do své e-mailové schránky. V tomto případě bývá i použití anglické klávesnice oříšek.

### Doporučení

Existují některá doporučení, kterými je možné se při výběru hesel řídit:

1. **Délka:** minimálně 8 znaků (případně 14-15 znaků)  
Obecně platí, že čím je heslo delší, tím je lepší, ale pokud si ho není uživatel schopen zapamatovat, nemá takové heslo velký smysl.
2. **Kombinace znaků:** velká i malá písmena, čísla a symboly  
Je nutné dávat si pozor na změnu umístění kláves „z“ a „y“ a ideálně se zcela vyhnout některým speciálním znakům nebo lokalizovaným písmenům.
3. **Časté měnění:** alespoň 1x za 90 dní
4. Nové heslo je výrazně jiné než předchozí.
5. Nepoužívat stejné heslo pro více účtů.
6. Heslo nesdílet s jinými osobami.
7. Neukládat hesla do internetových prohlížečů a ani na stránky služeb třetích stran.
8. Nezadávat heslo na počítačích, nad kterými nemá uživatel kontrolu (použit kopírování jednotlivých písmen nebo virtuální klávesnici).
9. Při opuštění počítače se odhlásit.
10. Heslo si spíše pamatovat než zapisovat.

Pro pohodlnější práci s hesly je vhodné použít některý z programů pro správu hesel.

### Software

Pro tvorbu nebo uchování hesel je možné využít některý z on-line generátorů nebo správců hesel. V tomto případě nejsou brány v potaz tabulkové programy nebo poznámkové bloky jako alternativy.

### Generátory

Generátory hesel mohou ulehčit uživatelům jejich vymýšlení, ale ne vždy se musí jednat o bezpečný způsob. Riziko hrozí u on-line generátorů takových hesel. Pokud by se totiž administrátor serveru rozhodl vygenerovaná hesla zneužít, postačí mu k tomu uchování seznamu IP adres a příslušných vytvořených hesel. Lepší variantou je samozřejmě použití speciálních programů, které se dají spustit přímo na počítači v off-line režimu.

### On-line generátory

- <http://www.hsgi.cz/generator-hesel/>
- <http://www.onlinepasswordgenerator.com/>
- <http://www.converter.cz/passgen/pswdgen.php>
- <http://www.generate-password.com/?language=cz>
- <http://www.pctools.com/guides/password/>

### Off-line generátory

- passGEN – <http://www.converter.cz/passgen/>
- Password Generator – <http://www.pctools.com/guides/password/>
- RoboForm – <http://www.roboform.com/cz/>
- Hesluj – <http://jsperl.sweb.cz/freeware.htm>

## Správce hesel

Správce hesel umí mnohem více než jednoduchý seznam hesel v Excelu nebo poznámkovém bloku. Příkladem takové aplikace je KeePass. Existuje v instalovatelné verzi ale stejně tak i ve verzi přenosné, kterou je možné umístit na přenosný USB Flash disk.

Některé funkce programu

- nutnost pamatovat si pouze přístupové heslo do šifrovaného databázového souboru
- velmi bezpečná databáze (šifrovaná pomocí AES a Twofish algoritmů)
- generátor hesel
- kategorizace hesel do skupin
- nastavení expirace hesla
- možnost importu/exportu hesel z/do jiných formátů souborů
- podpora řady jiných platforem (PocketPC, iPhone, BlackBerry,...)

Odkazy

- Stránky programu – <http://keepass.info/>
- Stažení programu – <http://keepass.info/download.html>

Pro milovníky linuxových operačních systémů existuje řada jiných správců hesel. Mezi ty oblíbené lze zařadit:

- KWallet (prostředí KDE)
- PwManager (prostředí KDE)
- Revelation (prostředí GNOME)
- KeySAfe (prostředí GNOME)
- GPass (prostředí GNOME)
- KeePassX – linuxová varianta programu KeePass

## Závěr

Závěrem lze říci, že je možné najít bezpočet tipů a návrhů, jak si vytvořit správné heslo. Mnoho programů či on-line formulářů pomůže bezpečná hesla vytvořit. Je nutné si však uvědomit, že opravdu bezpečná hesla jsou pouze u uživatelů, kteří s nimi umí adekvátním způsobem zacházet.