# Bezpečné heslo

Heslem prokazujeme svoji identitu v on-line prostředí. Je tedy jedním z nejdůležitějších prvků naší kyberbezpečnosti. Proto je potřeba vytvářet unikátní bezpečná hesla, nepřijít o ně a chovat se k nim způsobem, aby zůstala doopravdy v bezpečí. Jakmile naše hesla získá kdokoliv další, otevírá se mu přístup do našich nejniternějších zákoutí – stává se námi. V tomto modulu se dozvíme, jak funguje základní princip bezpečnosti hesel, jak se hesla prolamují a jak si správné a silné heslo vyrobit.

## Hesla: kde se vzala a kam jdou?

Známý příběh popisuje důležitost hesel: je jím pohádka Ali Baba a čtyřicet loupežníků. Příběh sleduje dobrodružství chudého dřevorubce Ali Baby, který odhalí tajemství nebezpečných a bohatých loupežníků. Jakmile před jeskyní čtyřiceti zlodějů vysloví zjištěnou kouzelnou frázi *„Sezame, otevři se"*, může vstoupit dovnitř a objevit tam velké a dlouho střežené poklady. V dnešní době jsou poklady digitální povahy chráněny téměř stejným způsobem. Místo drahých drahokamů a orientálních olejů chrání hesla naše citlivá data, jako jsou čísla kreditních karet, obchodní dokumenty nebo osobní údaje. A žádného Ali Babu ve svých digitálních jeskyních rozhodně nechceme.

### Novodobá historie hesel

Internet byl v čase jeho budování (a ještě i dlouho potom) místem bez větších omezení nebo bezpečnostních mechanismů. To ovlivnilo také zavedení používaní hesel. Když byla hesla implementována, pojem hackování neexistoval. V té době nikdo netušil, že velká část naší komunikace, práce, nakupování, osobního života či spravování financí bude probíhat online.

|  |
| --- |
| **Víte že...** hesla byla prvotně používaná pouze při dělení výpočetního času na velkých sdílených sálových počítačích? Retrospektivně může být až úsměvné, že první krádež hesla provedl vědec, který chtěl jen strávit více času na sdíleném počítači. Dosáhl toho tak, že vytiskl soubor, který obsahoval všechna uživatelská jména a hesla. Poté se mohl přihlásit pomocí získaných přihlašovacích údajů za své kolegy, aby získal čas navíc na dokončení své práce. |

Jak se internet rozrůstal a zvyšovala se potřeba soukromí, zvyšovaly se také nároky na hesla a jejich bezpečnost. Metody zpracovávání a uchovávání hesel se rychle zlepšovaly, stávaly se kryptograficky silnějšími a mnohé tehdy ustanovené principy se používají dodnes. Na druhé straně také útoky na hesla byly časem stále sofistikovanější a techničtější.

Oficiálně první masový útok na hesla byl proveden v roce 1988 prostřednictvím viru s názvem *Morris Worm*. Útok byl veden spíše jako experiment, který měl simulovat, co by se přinejhorším mohlo stát, kdyby podobný vir unikl. Výsledek byl velice znepokojivý: během prvních 24 hodin se infikoval každý desátý počítač. V stejném období se objevily také první pokusy o vícefaktorové ověřování, většinou pro použití ruku v ruce se vznikající VPN technologií.

### Hesla budoucnosti

V dnešní době stále více platí, že zabezpečení jenom kombinací uživatelského jména a hesla, hlavně pro účty s vysokou důležitostí, **nemusí stačit** a vystavujeme se tak bezpečnostnímu riziku. Odborníci varují před slabinami hesel vycházející z jejich podstaty: mohou být uživateli špatně volena, tedy například krátká, lehko uhodnutelná nebo opakovaně používaná pro různé aplikace. Následně jsou hesla zranitelná vůči útokům například pomocí hrubé síly (příkladem je slovníkový útok, kdy útočník zkouší otestovat všechna známá slova a kombinace slov v konkrétním jazyce a heslo uhodnout), nebo sociálního inženýrství. Z toho důvodu trendy v zabezpečování účtů směrují k používaní **vícefaktorového ověřování**: tedy že k tradičnímu přihlašovaní jménem a heslem přidáváme ještě další faktor ověření – to vše si dnes ukážeme.

Vědci se shodují, že v jistém bodě už budou běžná hesla zastaralá. Zároveň odhadují, že metody ověřovaní směřují k technologickému vývoji v oblasti **biometrie**. Očekává se, že snímače otisků prstů budou součástí jakéhokoliv chytrého telefonu, stejně tak pokročilejší technologie odemykání zařízení obličejem, skenování duhovky či sítnice a velké naděje se vkládají i do neinvazivního ověřování ucha. Je taktéž možno předpokládat, že budou vznikat i zcela nové metody ověřování. **Než se tak ale stane, musíme stále svoje tradiční hesla správně tvořit a opečovávat!**

## Jak vytvořit dobré heslo?

Umění tvořit bezpečná (silná) hesla nespočívá ve využití desítek speciálních znaků a symbolů, ze kterých se nám motá hlava i jazyk. Revolucí v tvorbě hesel jsou takzvaná **frázová hesla**. O co se jedná? Frázová hesla se skládají z kombinace pro nás zapamatovatelných slov. Například “BotaTancujePolku” nebo “SprávnéŽábyNecvičí” a prolomit je by trvalo až několik milionů let.

Frázové heslo se může skládat z části básně, scenerie cestou do práce, vzpomínky z dětství. Cokoli, co se nám bude dobře pamatovat, bude dostatečně dlouhé, ale nikdo si to s naší osobou nespojí. Tři až čtyři slova postačí, celkově bychom ale měli použít frázové heslo **delší než 12 znaků**. Pokud chcete heslo dovést k dokonalosti, přidejte na náhodná místa zástupné znaky (mezera, čísla, interpunkce, symboly) například “trhat.fialky.B00M.dynamitem”.

|  |
| --- |
| Warning on Apple iOS 14.6**Pozor!** Při přechodu na nové frázové heslo mají lidé tendenci si jej vytvořit velmi kreativně a komplikovaně – a pak jej zapomenout za pár dní. Nové frázové heslo si raději ze začátku často opakujme, než se spolu sžijeme. Nebo můžeme využít správce hesel, o kterých si přečtete za chvíli. |

V čem tento nejnovější trend v tvorbě hesel spočívá?

Je to vlastně poměrně jednoduché. Můžeme si to ukázat na příkladu.

*GK2/6@*   *JezevecZpíváNerad100Let*

Které z těchto hesel si za hodinu budete pamatovat líp?

### Zastaralá heslová doporučení: co už neplatí, ale všichni to děláme?

Víme, že o tvorbě správného hesla nejspíše neslyšíte poprvé. I tady se ale trendy mění, tak se pojďme ještě podívat na zastaralá doporučení, která se časem ukázala jako neefektivní, ba někdy i kontraproduktivní – mnohdy se jimi ale stále nevědomky řídíme. Tohle jsou nejznámější a nejčastěji zaužívané heslové retro pravdy, která už nemusí úplně platit:

* **Častá změna hesla.** Pravidelná změna hesla se může jevit jako rozumný způsob, jak se vyhnout potenciálnímu riziku ohrožení našeho účtu. Jisté období tento přístup prosazovali i mnohé popřední IT organizace, ale čas ukázal a výzkum potvrdil, že tento přístup přináší více škody než užitku. Stručně řečeno: častá změna hesla způsobuje primárně to, že si vytváříme slabší hesla. Uživatelé pokaždé udělají ve svých heslech jenom drobné, předvídatelné změny (často přidání nebo změnění posledního znaku), které útočník snadno odhalí. Na druhé straně ovšem platí, že když jsme si vědomi, že došlo k úniku našeho hesla například prostřednictvím phishingu, je nutno heslo skutečně co nejrychleji změnit!
* **Nezapisovaní si hesel a pamatováni si hesel nazpaměť.** Stále platí, že zapsat si heslo od počítače na papírek a přelepit jej na monitor je jeden z největších heslových přešlapů. Není však v našich silách zapamatovat si hesla ke všem účtům (obzvlášť, když se držíme zásady, že pro každý účet máme jiné jedinečné heslo). Je tak vhodné využívat správce hesel, o kterých si ještě povíme.
* **Zaměňovaní některých písmen za podobné číslice či speciální znaky**. Mnohdy jsme při tvorbě nového hesla nuceni splnit složité požadavky na kompozici a použit malá a velká písmena, aspoň jednu číslici či speciální znak. Problémem je, že taková pravidla jen zřídka nabádají uživatele k nastavování silnějších hesel a vedou spíše k heslům, která jsou slabá a těžko zapamatovatelná. Často ve snaze splnit požadavky nahrazujeme písmena podobnými čísly nebo speciálním znaky, například velké písmeno E je často nahrazováno číslem 3, nebo namísto písmena „a“ použijeme @ atp. Ale tohle útočníci velmi dobře vědí! Držme se proto při tvorbě hesel zásad **dlouhých frázových hesel**, protože jsou pro nás lehko zapamatovatelná a jak mnohé výzkumy potvrdili, také bezpečná.

## Prolomitelnost hesla

Myslíte si, že vy nebo někdo koho znáte je tak dobrý, že jeho heslo je neprolomitelné? Uděláme vám jasno. Neprolomitelná hesla neexistují. A to zcela vážně. Na planetě Zemi nenajdete osobu, která by takové heslo dokázala vytvořit. Jste překvapení? Zajímá vás na jakém principu hesla fungují? Pojďme na to!

Na hesla se totiž nikdy nekoukáme způsobem JESTLI naše heslo někdo může prolomit, **ale ZA JAK DLOUHO**. A to platí u všech různých hesel, které si dokážete představit.

Zjednodušeně můžeme říct, že existují dva hlavní způsoby, jak prolomit heslo. Sociálním inženýrstvím, tudíž kdy útočníkovi nějakým způsobem prozradíme své heslo sami, nebo útok takzvaně hrubou silou. Níže si rozebereme jednotlivé způsoby, jakou roli při nich hraje složitost hesla a jak se proti nim bránit.

|  |
| --- |
| **Víte že...** jednou z metod, jak prolomit něčí heslo, může být kombinace sociálního inženýrství a využití speciálních zařízení? Útočník se může na pracoviště dostat např. metodou zvanou *tailgating (více v modulu 4)*, nenápadně se dostat k našemu zařízení a mezi počítač a klávesnici napojit takzvaný *keylogger*, malou nenápadnou krabičku, která se skryje za počítač a dokáže zaznamenávat všechny znaky, které píšeme na klávesnici – hesla nevyjímaje. |

### Prolamování sociálním inženýrstvím

Sociálnímu inženýrství se budeme podrobně věnovat v modulu 4, nyní nám bude stačit vědět, že se jedná o určitý druh manipulace, kterého se na nás útočník dopouští. Často používanou technikou sociálního inženýrství je odeslání falešného e-mailu s odkazem na podvodnou přihlašovací stránku. Pokud podvod zavčas neodhalíme a formulář na heslo vyplníme, naše heslo je v útočníkových rukou. V případě prolamování hesla sociálním inženýrstvím **nehraje roli síla našeho hesla**. Heslo může mít třeba bilion znaků nebo být učebnicovým frázovým heslem, pokud ho ale vyplníme sami a dobrovolně, je nám to k ničemu. Na závěr je nutno dodat, že tento způsob prolomení hesla může trvat jen pár minut a záleží jen na naší schopnosti útočníkovy podvodné techniky rozpoznat.

|  |
| --- |
| **Pozor!** Co si z informací o tomto typu prolamování hesel odnést?  Útočník nemusí disponovat nijak velkou technickou znalostí. Složitost našeho hesla nehraje roli, protože jej útočníkovi sdělíme sami. Jedinou účinnou obranou je rozpoznávání technik sociálního inženýrství a **zdravá nedůvěra**. Věnujte proto zvýšenou pozornost tomuto tématu v modulu *Sociální inženýrství*. |

### Útoky hrubou silou

Útoky hrubou silou (*brute-force*) nejsou o manipulování s uživatelem. Pokud někdo bude chtít zkusit hrubou silou prolomit vaše heslo, nepotřebuje ani vědět kdo přesně jste. Hezký názorný příklad je, když se někomu například nechce platit za internet a zkouší prolomit naše heslo na Wi-Fi.

Jak samotný útok probíhá? Existuje hned několik variant. Pro nás je však důležité, že prakticky všechny fungují na principu do jisté míry náhodného generování znaků na různé pozice. Pro tento účel existují takzvaní boti, kteří jsou schopni vyzkoušet několik tisíc hesel za pár vteřin.

Představme si tento útok na konkrétním případu. Uživatel Bořivoj má na svém mobilním zařízení nastavený PIN kód pro odemknutí mobilu. Ten je 2233. Pomocí útoku hrubou silou lze k jeho telefonu připojit malé šikovné zařízení, které velmi dobře dělá svoji práci. Začne logicky vyplňovat pozice na PIN kódu dle instrukcí svého stvořitele. Začne 1111, pokračuje 2222, za nějakou dobu už je na pozici 1122. Za jak dlouho se dostane k PIN kódu Bořka? Jediné, co tento útok hrubou silou zpomalí je fakt, že telefony po několika neúspěšných přihlášení na chvíli odstaví tuto možnost (například na 90 vteřin). Hrubou silou by se tedy útočník do telefonu mohl dostat i v řádech hodin. Takže příště, až telefon někde zapomeneme nebo ztratíme, měli bychom myslet na fakt, že hesla nejsou všespásná a útoky hrubou silou jsou při některých případech poměrně nepříjemné.

Dobrou zprávou je, že na většinu našich online účtů by takovýto útok nefungoval, a to například díky vícefaktorové autentizaci, o které se ještě dočtete. Zjednodušeně: pro náš případ by scénář fungoval tak, že i kdyby útočníci uhodli naše heslo, než by se mohli do účtu připojit, nám by přišel požadavek na ověření na mobilní zařízení a věděli bychom, že je něco špatně. V tomto případě je nutné tento přístup zamítnout a neprodleně změnit heslo. Ideálně takové, co by programu útočníka trvalo prolomit pár milionů let!

|  |
| --- |
| **Pozor!** Co si z informací o tomto typu prolamování hesel odnést?  Útoky hrubou silou mohou probíhat absolutně bez našeho vědomí nebo kontaktu s útočníkem. Jejich úspěšnost záleží zcela na složitosti našeho hesla. Proti útokům hrubou silou se lze velmi efektivně bránit vícefaktorovým ověřováním |

**VŽDY PREFERUJTE DÉLKU PŘED SLOŽITOSTÍ!**

|  |
| --- |
| Memo on Skype Emoticons 1.2**Vyzkoušejte si...** jak dlouho by trvalo prolomit vaše heslo. Využít můžete nástroj [Kaspersky Password Check](https://password.kaspersky.com/). Ač se jedná o bezpečný nástroj, nikdy nedoporučujeme v podobných on-line nástrojích zkoušet svá pravá hesla. Můžete zkusit podobné o stejné délce a typu znaků. Poté můžete zvážit, zda není na místě heslo vyměnit za silnější, třeba frázové. |

## Vícefaktorové ověřování

Útočníci neustále přicházejí s novými a sofistikovanějšími metodami, jak se dostat k našim přihlašovacím údajům a jak se nabourat do našich účtů. Používat pouze hesla ne vždy stačí. Proto pro ochranu účtů s vysokým stupněm důležitosti musíme být ještě o krok napřed. K tomu nám dokáže pomoct právě **vícefaktorové ověřovaní** nebo autentizace, která přidává další krok do procesu přihlašování se k účtu. Takových kroků při přihlašování může být více, ale většinou se využívá jeden navíc – tedy dohromady dva a mluvíme tak o **dvoufaktorovém ověřování** (2FA).

Proč se nám tato práce navíc při každém přihlašování vyplatí? Dvoufaktorové ověření poskytuje pokročilejší vrstvu ochrany, která je klíčová u aplikací jako je například internetové bankovnictví. Dvoufaktorové ověření přidává další faktor ověření totožnosti přihlašujícího. Základním pilířem tohoto ověřování je fakt, že přídavný faktor je pro útočníka **velmi náročné získat nebo duplikovat**, ať už z pohledu limitovaného času nebo osobní vzdálenosti. Z toho důvodu se útočník už nemůže dostat v přihlašovaní dál, i když se mu třeba podařilo uloupit naše heslo.

### Jak můžeme používat vícefaktorové ověřování v praxi?

Po zadání a úspěšném ověření našeho uživatelského jména a hesla se nám zobrazí výzva k další formě prokázání totožnosti, například pomocí PINu z ověřovací aplikace nebo otisku prstu. Po zdárném ověření dalšího požadovaného faktoru získáme přístup ke svému účtu. Toto sekundární ověření může mít mnoho podob a pro zjednodušení je dělíme do 3 kategorií faktorů:

* **Faktor znalosti** (něco, co znáte): typický pro jednofaktorové ověření, tedy nejčastěji kombinace uživatelského jména a hesla, PIN nebo bezpečnostní otázky.
* **Faktor vlastnictví** (něco, co máte): například důvěryhodné zařízení, telefon, jednorázové heslo zaslané SMSkou, platební karta, klíč, nebo bezpečnostní hardwarový token.
* **Faktor biometrie** (něco, co jste): nejpoužívanější jsou otisk prstu, sken očnice, rozpoznání obličeje či hlasu.

Pravděpodobně jste se již v běžném životě setkali s vícerými zmíněnými ověřovacími mechanismy. Faktor znalosti, tedy například heslo, je nejpoužívanější. Jako druhý faktor se často využívá jednorázového hesla poslaného SMSkou nebo potvrzení přihlášení přes aplikaci na mobilním telefonu. Stále častěji díky vybavenosti mobilních zařízení používá i faktor biometrie, tedy například otisk prstu. Rozšířený je také faktor vlastnictví, tedy například potvrzení na druhém zařízení. Aby dvoufaktorové ověřování poskytovalo požadovanou úroveň zabezpečení, je nutné kombinovat **dva odlišné faktory**. Použití dvou různých obyčejných hesel za sebou se tedy nepovažuje za dvoufaktorové ověření. Zároveň je třeba vzít do úvahy, že některé mechanismy ověření jsou silnější než jiné.

|  |
| --- |
| **Vyzkoušejte si...** přidat dvoufaktorové ověřování ve svém účtu Microsoft (O365). <school-specific> [Jednoduchý návod](https://support.microsoft.com/cs-cz/account-billing/jak-pou%C5%BE%C3%ADvat-dvoustup%C5%88ov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-s-%C3%BA%C4%8Dtem-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4) na oficiálních stránkách vás procesem lepšího zabezpečení účtu povede krok po kroku. Zvládne to i úplný začátečník. Pokud chcete takto zabezpečit i jiné služby a aplikace, je obvykle oficiální návod nejlepším místem, kde začít: najdete tam nejen informaci o tom, zda daná služba 2FA <odkaz na slovník> podporuje, ale jak tuto funkci případně zapnout. |

Tak si to shrneme: využití jakékoli formy dvoufaktorového ověření nás dostane mimo dosah většiny útoků. Přitom stačí udělat při přihlašování **jenom o jeden krok navíc**. I dvoufaktorové ověření muže být samozřejmě prolomeno, ale útočník už musí vynaložit mnohem větší úsilí než v případě obyčejného hesla. Zároveň je v současnosti nastavení 2FA jednodušší než kdy dříve, takže je na čase začít tuto bezpečnostní metodu využívat.

## Správce hesel

Kolik máme na internetu různých účtů a k nim hesel? Schválně, zkuste si je někdy spočítat. No a v ideálním případě byste měli mít na každé z nich unikátní dlouhé heslo. Je opravdu reálné si je všechna pamatovat? Pokud to zvládáte, jste zázrak přírody.

Řešení existuje v podobě velmi pohodlného a bezpečného nástroje jménem **správce hesel**. Co je jeho úkolem? Jedná se vlastně o jakýsi trezor, který zašifrovaně střeží naše hesla. Funguje jako databáze, kam si hesla ukládáme. Správců hesel existuje celá řada: může být ve formě doplňku do prohlížeče, může to být ale i zašifrovaná databáze u vás na počítači. Většina správců hesel pak dokonce za nás i hesla při přihlašování vyplňuje, takže je ve správci nemusíme zdlouhavě dohledávat.

|  |
| --- |
| **Pozor!** Ukládání hesla do prohlížeče (třeba do Google Chrome nebo Mozilla Firefox) není to samé, co skutečný správce hesel. Ne že by se snad prohlížeče nesnažily takto uložená hesla zabezpečit... Správa hesel ovšem není primární funkce vašeho prohlížeče a svá hesla chcete svěřit nástroji, který se tomu věnuje prioritně – má tedy odladěné šifrování a další náležitosti. Navíc, pokud hesla uložená ve webovém prohlížeči nejsou chráněna master heslem (viz dále), jsou uložena ve formě prostého (nezašifrovaného) textu – každý si je tak může jednoduše přečíst v nastavení prohlížeče. |

Všichni správci hesel mají jedno společné: do všech se přihlašujete jedním heslem, takzvaným **master heslem**. Od momentu, kdy si správce hesel zařídíte, je to jediné heslo, které je si třeba pamatovat. Je jako velký zlatý klíč k vaší pokladnici. Správce hesel po uložení hesla zašifruje, takže i kdyby se k vaší databázi dostal někdo cizí, bez master hesla nezmůže doopravdy nic. Master heslo tedy musí být opravdu silné.

|  |
| --- |
| **Pozor!** Své master heslo opravdu nikdy nikdy nesmíte zapomenout. Jinak se do svého trezoru a ke svým uloženým heslům nedostanete. U těch správců hesel, které nabízejí 2FA, rozhodně doporučujeme této možnosti využít. |

|  |
| --- |
| **Vyzkoušejte si...** správce hesel! Jenže kterého? Doporučit jednoho správce hesel není zrovna lehký úkol: přicházejí v různých podobách. Mohou být **zdarma i placení**, mohou fungovat jako **samostatný program** na vašem zařízení (tzv. *on-device*) nebo **v cloudu** a jako doplněk do prohlížeče. Mezi nejvyužívanější správce (*a mezi nejdůvěryhodnější dle aktuálních testů*) patří například [KeePassCX](https://keepassxc.org/) (*on-device*), [Bitwarden](https://bitwarden.com/) (*dostupná verze zdarma nenabízí 2FA*) nebo často využívaný [LastPass](https://www.lastpass.com/) (*dostupná verze zdarma, umožňuje i některé typy 2FA*). Na co se zaměřit, když správce budete vybírat, vám [přiblíží tento článek](https://www.dtest.cz/clanek-6761/jak-vybrat-spravce-hesel).  **Rozhodovací paralýza?** Instalace a používání každého z nich se liší: pokud se necítíte na to sami vybírat z dostupných možností, určitě neprohloupíte, když zvolíte **LastPass** a budete se řídit [tímto podrobným návodem](https://security.muni.cz/cybercompass/passwords/lastpass-tutorial). |

## Heslové desatero

V závěru tohoto modulu ještě jeden bonus: heslové desatero připomínající nejdůležitější zásady práce s hesly.

|  |
| --- |
| 1.Chraňme každý účet/aplikaci/zařízení jiným jedinečným heslem! 2.Používejme dlouhá frázová hesla (nejméně 12 znaků), která obsahují minimálně 3 slova!  3.Zadávejme své přihlašovací údaje v soukromí a chraňme je od zvědavých očí! 4.Využívejme ověřený správce hesel! 5.Na webech, kde lze zkontrolovat síla našeho hesla, nevyplňujeme svá skutečná hesla! 6.Používejme vícefaktorové ověření! 7.Nikdy svá hesla nikomu neříkejme ani neposílejme!  8.Hlídáme si trendy v oblasti tvoření hesel. 9.Naše hesla nikdy nesmí být spojitelná s naší identitou (např. *JezdimTramvaji...DoPraceX90*) 10. Dáváme pozor, na co klikáme a nikdy neotevíráme phishingové e-maily či podezřelé přílohy! |

|  |
| --- |
| **Pozor!** **Co dělat, když se něco pokazí?** V případě, že došlo k bezpečnostnímu incidentu nebo máte podezření, že mohlo být narušeno vaše kyberbezpečí, obracejte se na <school-specific: doplňte kontaktní osobu nebo popište proces řešení kyberbezpečnostních incidentů>. |