

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **69** ze dne **14.5.2024**

Hlavně si je dobře pamatovat – jak moc riskujeme s hesly?

Dle posledního průzkumu od ESET se více než polovina z nás spoléhá na to, že si hesla bude pamatovat z hlavy. To však v kybersvětě není úplně dobrý nápad.

Heslo. Roky prověřený zámek v online světě a často naše jediná pojistka před tím, aby se k našim datům a financím nedostal někdo nepovolaný. Asi tak není příliš překvapivé, že hesla jsou hlavními cíli řady kyberútoků a některé škodlivé kódy se na jejich krádež přímo specializují – je to například spyware nebo password stealery.

Podle posledního průzkumu od ESETu považujeme za bezpečné heslo takové, které je dostatečně dlouhé, složité a jedinečné pro každou z využívaných služeb. Více než polovina z nás se však spoléhá na to, že si taková hesla bude pamatovat z hlavy. Jak má ale bezpečné heslo vypadat a čemu bychom se radši při jejich tvorbě a uchovávání měli vyhnout? Na to se podíváme v dnešním článku.

Jméno králíka, narozeniny ani adresa do hesla nepatří

Hesla podle průzkumu nejčastěji tvoříme kombinací malých a velkých písmen a číslic (43 %). Téměř srovnatelné množství z nás pak k těmto údajům přidává ještě speciální znaky (38 %).

Výsledná podoba hesla se ale dále liší. Zatímco pětina z nás používá náhodný shluk znaků, písmen a čísel (22 %) a necelá třetina pak tzv. heslovou frázi (30 %), čtvrtina českých uživatelů a uživatelék stále tvoří hesla na základě osobních informací, jako je například jméno domácího mazlíčka, datum narození anebo adresa (26 %). Jednoduchá slovní spojení, jako je např. „heslo123“, používá 12 % dotázaných.

Vytvořit správné heslo z pohledu kyberbezpečnosti je občas trochu oříšek. Ještě pár let zpátky byla za silné heslo považovaná náhodná kombinace velkých a malých písmen, speciálních znaků a čísel. Lidé tak začali volit sice složitá, ale krátká hesla. Dnešní automatizované nástroje na prolamování hesel využívané například v útocích tzv. hrubou silou ale dokážou taková hesla uhodnout během několika minut.

Lepší je tak zvolit např. heslovou frázi – větu nebo spojení slov, které dává smysl jen nám. Ani ta by ale neměla přímo souviset s našimi osobními údaji nebo informacemi o naší rodině a koníčcích – útočníci si je totiž mohou snadno zjistit například z veřejných informací na sociálních sítích.

Cvičit paměť se v případě hesel spíš nevyplatí

Bezpečnost hesla hodnotíme podle průzkumu nejčastěji podle jeho složitosti (64 %), délky a také podle toho, zda je heslo unikátní pro každou využívanou službu (obě kritéria shodně 26 %). Používání bezpečnostní aplikace (například správce hesel) jako kritérium bezpečnosti je důležité pro 24 % z nás. Pro 17 % je však bezpečnostním kritériem i to, zda je heslo dobře zapamatovatelné.

A právě na otázku, jak nejčastěji si heslo pamatují, dotázaní odpovídali, že z hlavy – uvedla to více než polovina z nich (54 %). Specializovaný program pro bezpečnou správu přihlašovacích údajů, tzv. správce hesel, využívá dle průzkumu jen 12 % respondentů.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **69** ze dne **14.5.2024**

Podle čeho se pozná bezpečné heslo?

Pamatovat si všechna naše hesla z hlavy je při dnešním množství služeb a účtů, které používáme, ale téměř nadlidský úkol. To může opět vést k tomu, že budeme používat jednodušší hesla nebo stejné heslo pro více účtů, což samozřejmě nahrává kyberútočníkům.

Hesla posílí druhý faktor

Pravidlo „jedno unikátní heslo pro jeden účet“ dodržuje dle výsledků průzkumu čtvrtina z nás (24 %). Třetina (31 %) uvedla, že má několik hesel, která pro přihlášení do různých účtů střídá. Necelá pětina (18 %) pak volí způsob, kdy má několik hesel, která různě střídá podle povahy služby (e-shop, sociální síť, e-mail). Podobně 16 % dotázaných uživatelů a uživatelék využívá stejný základ hesla, ale doplní k němu pokaždé jiné informace.

Jen jedno heslo do všech účtů využívá 7 % dotázaných, to je ovšem podle bezpečnostních expertů velice riskantní. Používání unikátního hesla pro každou službu je dle nich jednou z nejdůležitějších zásad pro bezpečnost našich online účtů. Nezbytné je také využívání vícefázového ověřování, kdy je při přihlášení kromě hesla vyžadováno ještě dodatečné ověření např. kódem zaslaným v SMS či e-mailu nebo potvrzením v ověřovací aplikaci.

Druhý faktor jako další prvek na posílení bezpečnosti svých účtů využívá do důležitých služeb (například do online bankovníctví) polovina dotázaných (48 %). Téměř kdykoli ho pak využívá více než třetina (35 %).

Mimo tradiční přihlašování pomocí hesla můžeme využívat i přihlášení bez nutnosti jeho zadávání, např. pomocí otisku prstu. Tento způsob přihlášení volí 44 % uživatelů a uživatelék. Rozpoznání tváře pak využívá pětina z nich (21 %). Jako další metodu uváděli dotázaní i přihlášení pomocí tzv. přístupových klíčů – passkeys (11 %). Více než třetina z nás však podobné způsoby přihlášení bez zadání hesla nevyužívá (35 %).

Práci s hesly si rádi zjednodušíme

Další dostupnou možností je také přihlašování prostřednictvím jiného účtu – například existujícím e-mailovým účtem nebo účtem na sociálních sítích. Zde však podle průzkumu máme rozporuplné názory na to, jak moc je takové přihlašování bezpečné.

Přihlášení prostřednictvím jiného účtu využívá dle průzkumu více než polovina dotázaných, přičemž třetina se domnívá, že se nejedná o příliš bezpečnou metodu (32 %). Další čtvrtina si však myslí, že je to bezpečné a pohodlné (26 %). Zbývajících třetina dotázaných (30 %) tento způsob nevyužívá, protože ho nepovažuje za bezpečný.

Jednoznačněji se dotázaní staví k využívání možností „zapamatovat přihlášení“ nebo „nikdy se neodhlášovat“. Tyto možnosti opět využívá zhruba polovina, ale více se jich kloní k tomu, že se nejedná o bezpečné metody (38 %). Jako bezpečné vnímá tyto možnosti 13 % z nich. Čtvrtina dotázaných nepovažuje tyto funkce za bezpečné a nevyužívá je (24 %) a pětina se vždy z účtu odhlásí (21 %).

Zdroj: Avcentrum ČR