Průzkum ESET: Čtvrtina českých uživatelů a uživatelek riskuje s hesly, tvoří je z osobních informací

19.4.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Podle posledního průzkumu společnosti ESET zaměřeného na tvorbu a správu našich uživatelských hesel, 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 – výsledky průzkumu byly vyrovnané v rámci všech oslovených věkových skupin. Bezpečnostní specialisté v kontextu kybernetických útoků však upozorňují, že právě ve snaze zapamatovat si heslo můžeme upozadit jeho bezpečnost. Více než čtvrtina dotázaných totiž dále uvedla, že hesla tvoří také z osobních informací. Ty mohou ale být dobře dohledatelné na internetu.

Hesla podle průzkumu nejčastěji tvoříme za použití kombinace malých a velkých písmen a číslic (43 %). Téměř srovnatelné množství dotázaných 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 uživatelů a uživatelek 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.

„Hesla stojí v první linii obrany mezi kyberútočníky a našimi citlivými údaji. Tyto údaje jsou pro ně velice cenné, protože je mohou zpeněžit nebo využít k dalším útokům. Útočníci se k nim snaží dostat třeba za pomoci škodlivých kódů, kterými jsou typicky tzv. infostealery. Ty se řadí mezi spyware, který v Česku dlouhodobě sledujeme. Podle našich dat tyto útoky stále mírně rostou, a to především ve vyspělejších zemích EU a v USA, přičemž mezi oběťmi jsou především uživatelé a uživatelky operačního systému Windows,” říká Vladimíra Žáčková, specialistka kybernetické bezpečnosti společnosti ESET.

„Ještě před několika lety 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 variantou je proto volit např. heslovou frázi, která 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,“ doplňuje Žáčková.

Samotní uživatelé a uživatelky hodnotí bezpečnost hesla 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 % dotázaných. Pro 17 % z nich je však bezpečnostním kritériem i to, zda je heslo dobře zapamatovatelné. Právě na otázku, jak nejčastěji si dotázaní hesla pamatují, odpovídali, že z hlavy – v průzkumu to uvedla více než polovina z nich (54 %). Specializovaný program pro bezpečnou správu přihlašovacích údajů, tzv. správce hesel, využívá dle průzkumu jen 12 % respondentů.

„Pamatovat si všechna naše hesla z hlavy je při dnešním množství služeb a účtů, které používáme, téměř nadlidský úkol. To může opět vést k tomu, že budeme tíhnout k používání jednodušších hesel

nebo stejného hesla pro více účtů, což samozřejmě nahrává kyberútočníkům a snižuje se tím celková úroveň naší digitální bezpečnosti," varuje Žáčková.

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, které různě střídá podle povahy služby (e-shop, sociální sítě, e-mail). Podobně 16 % dotázaných využívá stejný základ hesla, ale doplní k němu pokaždé jiné informace. Jen jedno heslo do všech účtů využívá 7 % respondentů, to je ovšem podle bezpečnostních expertů velice riskantní.

„V průzkumu o používání hesel českými uživateli z roku 2021 vidíme, že klesl počet lidí, kteří unikátní hesla používají, z 32 % v roce 2021 na 24 % v roce 2024. Používání unikátního hesla pro každou službu je přitom 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 uživatele, např. kódem zaslaným v SMS či e-mailu nebo potvrzením přihlášení v ověřovací aplikaci," vysvětluje Žáčková.

Druhý faktor jako další prvek na posílení bezpečnosti svých účtů využívá do důležitých služeb (například do online bankovnictví) polovina dotázaných (48 %). Téměř kdykoli ho pak využívá více než třetina z nich (35 %). Jen 6 % z nich pak uvedlo, že nemá důvěru v službu jako takovou – nechtějí poskytovateli služby sdělovat své telefonní číslo nebo si stahovat další aplikaci.

Uživatelé mohou k tradičnímu přihlašování pomocí hesla využívat i přihlášení bez nutnosti jeho zadávání, např. pomocí otisku prstu. Tento způsob přihlášení volí 44 % uživatelů a uživatelek. 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 %).

Jednou z dalších možností, jak přistupovat ke svým účtům, je přihlášení prostřednictvím jiného účtu – například existujícím e-mailovým účtem nebo účtem na sociálních sítích. Zde mají čeští uživatelé a uživatelky rozporuplné názory na to, jak moc je takové přihlašování bezpečné. Přihlášení prostřednictvím jiného účtu využívá 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 %). Zbývající třetina dotázaných (30 %) tento způsob nevyužívá, protože ho nepovažuje za bezpečný.

Jednoznačněji se dotázaní staví k využívání možností „zapamatovat přihlášení" nebo „nikdy se neodhlašovat". Tyto možnosti opět využívá zhruba polovina dotázaných, 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 %).

„Takzvané sociální nebo jednotné přihlašování využívá informace ze sociálních sítí k usnadnění přihlašování do služeb třetích stran. Svoje přihlašovací údaje uživatel zadá pouze jednou a proces ověření jeho identity pro další službu proběhne bez jeho dalšího zásahu. Rizikem tohoto způsobu přihlašování ale mohou být výpadky služeb sociálních sítí nebo úniky dat, se kterými se tyto sítě potýkají. Úniky dat nebo prolomení hesla k účtu na sociální síti mohou vést až k neoprávněnému přístupu do vašich dalších účtů. Zejména v těchto službách tedy nezapomeňte aktivovat ještě ověření přihlášení dalším faktorem," dodává Žáčková z ESETu.

Sběr dat byl realizován prostřednictvím aplikace Instant Research agentury Ipsos ve dnech 8. až 14. března 2024 na 1000 respondentech v České republice.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-ctvrtina-ceskych-uzivatelu-a-uzivatelek-riskuje-s-hesly-tvori-je-z-osobnich-informaci