

Loni došlo k 32 miliónům pokusů o ukradení hesel, říká Kaspersky

2.5.2024 - | PROTEXT

Slabá a jednoduchá hesla byla pro podvodníky vždy atraktivním cílem, protože jejich prolomení umožňuje zločincům přístup k různým typům dat - osobním údajům, finančním informacím, lékařským záznamům atd. Telemetrie společnosti Kaspersky ukazuje, že v roce 2023 došlo k více než 32 milionům pokusů o napadení uživatelů pomocí nástrojů pro krádež hesel, přičemž v roce 2022 to bylo více než 40 milionů. Tyto alarmující statistiky zdůrazňují rostoucí potřebu vytvářet silná, jedinečná a rozmanitá hesla pro různé účty. Tímto způsobem lze zmírnit rizika kybernetických hrozeb a zajistit bezpečí osob v online prostředí.

Ke zvýšení účinnosti ochrany pomocí hesel doporučují odborníci společnosti Kaspersky následující kroky a postupy:

Vytvářejte silná a zároveň dobře zapamatovatelná hesla pomocí asociací

Asociační přístup spočívá ve vytvoření hesla odvozeného z posloupnosti slov nebo myšlenek, které mají pro uživatele osobní význam, ale nejsou snadno uhodnutelné. Heslo může být založeno například na nějakém citátu, textu oblíbené písně nebo jedinečné kombinaci objektů. Tato metoda umožňuje vytvářet silná hesla, která není třeba si pracně zapamatovávat, což pomáhá zajistit bezpečnost a zároveň snižuje riziko jejich zapomenutí. Například věta „Paříž jsem poprvé navštívil v roce 2008“ by mohla být transformována do hesla „Pjpnv2o:o8“.

Zkuste používat neobvyklá hesla s emoji

Pokud používáte stejné heslo na příliš mnoha místech a nechce se vám vymýšlet něco nového, mohou být netradiční a bezpečnější volbou hesla s emoji. Tyto symboly jsou součástí standardu Unicode, a u některých účtů se dají použít i jako součást hesla. Jednou z největších předností je, že podvodníci zatím nedokážou hesla s emoji prolomit metodou „hrubé síly“, protože běžné hackerské nástroje a slovníky s takovými kombinacemi nepočítají. Podrobnější rozbor podmínek použití a postupů zadávání hesla s emoji najdete zde.

Nebudte líní a nepoužívejte snadno uhodnutelná hesla

Používání „hloupých“ hesel nebo výchozích nastavení, jako jsou „1234“, „password“ nebo „admin“, může způsobit, že osobní údaje a účty budou snadno zranitelné pomocí automatizovaných nástrojů pro odhalování správných kombinací. Vyhledání správné odpovědi a získání přístupu může podvodníkům trvat jen několik sekund. Silné a složité heslo má obsahovat kombinaci písmen, číslic a symbolů, a jeho součástí nemají být osobní údaje, jako jsou jména nebo data narození. Pro kontrolu síly hesla a zmírnění možných rizik lze použít také bezplatné veřejné služby.

Dodržujte staré zlaté pravidlo: samostatné heslo pro každý účet

Tento postup zajišťuje, že když je jeden účet napaden, ostatní zůstanou v bezpečí. Vytvořením jedinečného hesla pro každý účet minimalizujete škody, které může hacker napáchat, pokud se mu podaří nějaké heslo ukrást. Narušení bezpečnosti je omezeno, což pomáhá chránit citlivá data. Podle celosvětového průzkumu má průměrný uživatel přibližně 8 účtů. Zapamatovat si i pouhá 2 nebo 3 dlouhá a složitá hesla (obsahující až 15 symbolů) však může být pro většinu uživatelů nad jejich síly.

V takovém případě je *bezpečné a užitečné přenést odpovědnost za zapamatování všech hesel na správce hesel.*

<https://www.ceskenoviny.cz/tiskove/zpravy/loni-doslo-k-32-milionum-pokusu-o-ukradeni-hesel-rika-kaspersky/2513412>