8 KROKOV K VYTVÁRANIU SILNÝCH HESIEL

Aké inštrukcie na vytváranie hesiel dať zamestnancom vašej firmy?

01.

HESLO MUSÍ BYŤ JEDINEČNÉ

Pre každý účet vytvorte jedinečné heslo. V prípade prelomenia alebo úniku jedného hesla tak zabránite neoprávnenému prístupu k viacerým zdrojom. Heslo by nemalo byť napísané na nalepovacom štítku alebo v nezašifrovanom súbore uloženom vo vašom firemnom zariadení.

02.

ČÍM DLHŠIE HESLO, TÝM LEPŠIE

Národný inštitút pre štandardy a technológie (NIST) Spojených štátov amerických odporúča používať heslá, ktoré obsahujú minimálne 8 znakov. To zabezpečí prijateľnú úroveň ochrany proti takzvaným útokom hrubou silou.

03.

UPREDNOSTŇUJTE POUŽÍVANIE PRÍSTUPOVÝCH FRÁZ

Vytvorte si frázové heslo, ktoré obsahuje minimálne 30 znakov. Takáto fráza je bezpečnejšia ako slovo s dĺžkou 8 znakov s bežnými obmenami (napríklad zamenenie písmena „e" za číslo „3", písmena „i" alebo „l" za výkričník „!" a podobne). Frázy sú vo svojej podstate ľahšie zapamätateľné, takže väčší počet znakov pri nich nie je z pohľadu používateľa až taký problém.

04.

NEVYNUCUJTE KOMPLEXNÉ PRAVIDLÁ PRI TVORBE HESIEL

Ak sa od používateľov vyžaduje, aby heslo obsahovalo veľké aj malé písmená, aspoň jedno číslo a aj špeciálny znak, len zriedkavo sa tým docieli nastavenie silnejších hesiel. Vedie to naopak skôr k vytváraniu slabších a ťažko zapamätateľných hesiel.

05.

HESLÁ S NIKÝM NEZDIEĽAJTE

Heslá nikdy nezdieľajte s inými ľuďmi vrátane kolegov, nadriadených, rodiny a ani špecialistov IT podpory. Útočníci využívajúci phishingové techniky sa zvyknú vydávať za pracovníkov IT podpory, čo im uľahčuje získanie vášho hesla.

06.

VYHNITE SA OPAKOVANIU ZNAKOV

„XXXX" rozhodne nie je silné heslo. Vyhnite sa taktiež postupnosti znakov (napríklad „1234") a rozpoznateľným vzorom (napríklad „qwerty").

07.

NEPOUŽÍVAJTE BEŽNÉ SLOVÁ ZO SLOVNÍKA

Takéto heslá môžu byť prelomené pri takzvanom slovníkovom útoku. Rovnako to platí aj pre bežné slová v cudzích jazykoch a odborné termíny z rozličných oblastí.

08.

NIKDY NEPOUŽÍVAJTE OSOBNÉ INFORMÁCIE

Osobné informácie môže útočník získať napríklad podľa informácií dostupných vo vašich profiloch na sociálnych sieťach. Ide napríklad o stredné mená, dátumy narodenia, adresy, školy, meno partnera či dieťaťa.