

Krijoni fjalëkalime të forta

Praktikat më të mira të fjalëkalimeve të forta duhet të jenë prioriteti i të gjithëve, pasi është rritur forca punëtore që punon në distancë dhe sasia e informacionit e shkëmbyer dixhitalisht në bazë ditore.

Pavarësisht rritjes së rëndësisë publike që i kushtohet sigurisë së të dhënave, një pjesë e madhe e popullsisë përdor fjalëkalim të dobët për llogaritë e tyre profesionale dhe personale. Sipas Google, 24% kanë përdorur fjalën "password", "Qwerty" ose "123456" si fjalëkalim të llogarisë së tyre, ndërsa vetëm 34% e ndryshojnë fjalëkalimin e tyre shpesh.

Fjalëkalimet e thjeshta janë telashe për punonjësit, rrjetin dhe të dhënat. Nëse ato gjenden lehtësisht nga një haker, mund të rrezikohen, të dhënat e logimit për rrjetin, emailin, aplikacionet në renë kompjuterike, emailt personale, e-bankat dhe faqet e tregtisë elektronike.

Çdo logim është një shans për një kriminel kibernetik që të hakojë rrjetin e kompanisë dhe të vjedhë të dhëna.

Si pjesë e trajnimit dhe fushatave të ndërgjegjësimit për sigurinë, përdorni mësimet për sigurinë e fjalëkalimeve, buletinet dhe posterat, për t'i kujtuar punonjësve bazat e forta të krijimit të fjalëkalimeve.

Përdorni këto praktika më të mira të fjalëkalimeve të forta

Kriminelët kibernetikë e dinë se shumica e njerëzve krijojnë fjalëkalime që janë të lehta për t'u mbajtur mend dhe se do e ripërdorin të njëjtin fjalëkalim në shumë llogari. Prandaj, gjithçka që ata duhet të bëjnë, është hakimi në njëren prej llogarive që të hyjnë me lehtësi në pjesën tjetër të llogarive.

Duhet të përdorni këto shtatë praktika më të mira të përdorimit të fjalëkalimeve dhe krijimit të fjalëkalime të reja:

1. Mos përdorni numra ose shkronja vijuese si fjalëkalim

Për shembull, mos përdorni 1234, 9876, asdfg, qwerty, etj.

2. Mos përfshini vitin e lindjes ose muajin/ditën e lindjes në fjalëkalimin tuaj

Mos harroni se kriminelët kibernetikë mund ta gjejnë lehtësisht këtë informacion duke kërkuar në llogaritë tuaja të rrjeteve sociale.

3. Përdorni një kombinim prej të paktën tetë shkronjash, numrash dhe simbolesh

Sa më i gjatë është fjalëkalimi dhe sa më shumë larmi karakteresh të përdoren, aq më e vështirë është të hamendesohet nga hakerat. Për shembull, K03\$zj8Li! është një kombinim unik i shkronjave të mëdha dhe të vogla, numrave dhe simboleve.

4. Kombinoni fjalë të ndryshme të palidhura

Mos përdorni fraza nga këngët e njohura, nga filma ose shfaqje televizive. Përdorni tre ose katër fjalë të gjata. Për shembull, 8UjkNeMesTeDeborS.

5. Mos përdorni emra ose fjalë që gjenden në fjalor

Zëvendësoni shkronjat me numra ose simbole për ta bërë të vështirë gjetjen e fjalëkalimit. Ose përdorni qëllimisht gabime drejtshkrimore. Për shembull, k0935htn3060rr për "kopsht në oborr".

6. Përdorni një soft si menaxher fjalëkalimesh për të ruajtur te gjitha fjalëkalimet

Mos i ruani fjalëkalimet në një dokument në kompjuterin tuaj. Është praktikë e mirë të përdorni mjetin e menaxherit të fjalëkalimeve të instaluar nga ekipi i IT/suportit për të ruajtur të gjitha fjalëkalimet profesionale dhe personale.

7. Mos ripërdorni fjalëkalimet tuaja

Çdo pajisje, aplikacion, faqe interneti dhe program softuerik kërkon një fjalëkalim unik dhe të fortë. Nëse një kriminel arrin të hamendesojë një nga fjalëkalimet e tua, ai do ta përdorë këtë për të tentuar të hakojë të gjitha llogaritë tuaja personale dhe profesionale.

Bëni kujdes të mos i jepni kurrë fjalëkalimet tuaja askujt, si kolegëve tuaj, ekipit të IT/suportit, personelit të shërbimit ndaj klientit, anëtarëve të familjes dhe miqtë.

Duhet të tregoni mjaft kujdes ndaj emaileve phishing, mesazheve smishing dhe thirrjet telefonike vishing që kërkojnë informacionin rreth fjalëkalimit tuaj - mos u përgjigjini ose mos jepni asnjë informacion personal duke përfshirë fjalëkalimin, datën e lindjes, adresën ose detajet e kartës së kreditit.

Informacione që nuk duhet t'i përfshini kurrë në fjalëkalimet tuaja

Nuk duhet të përfshini informacionin e mëposhtëm kur përditësoni fjalëkalimet aktuale dhe krijoni fjalëkalime të reja:

1. Emri i kafshës shtëpiake që keni.
2. Ditëlindja juaj apo e anëtarëve të familjes.
3. Çdo fjalë që lidhet me hobin, punën ose interesat tuaja.
4. Një pjesë të adresës suaj të shtëpisë duke përfshirë qytetin, rrugën, numrin e shtëpisë/apartamentit.
5. Emrin tuaj ose emrin e një anëtari të familjes.

Kriminelët kibernetikë kërkojnë në internet për informacione rreth viktimave të cilat u duhen për të hakuar fjalëkalimet e tyre. Duke patur të dhëna të tilla si, vendin ku jetoni, interesat dhe familjen tuaj, ata mund të hamendesojnë fjalëkalimin tuaj.

Nëse në ndonjë nga fjalëkalimet keni përdorur informacion personal ose profesional, duhet patjetër ti ndryshoni ato duke ndjekur praktikën më të mirë të mësipërme të fjalëkalimeve.

Si të mbroni dhe të siguroni fjalëkalimin e rrjeteve tuaja sociale

Shumë faqe interneti, aplikacione dhe mjete ju lejojnë që të identifikoheni duke përdorur llogaritë në Facebook, Twitter, Instagram ose rrjete sociale të tjera. Përdorimi i këtij funksionaliteti përveç përfitimit që nuk keni nevojë të krijoni një emër përdoruesi dhe fjalëkalim të ri, ju bën të prekshëm ndaj rrjedhjeve të të dhënave (data breach) të rrjeteve sociale.

Nëse një kriminel kibernetik ka kredencialet e llogarisë suaj në Facebook, ai mund të hyjë në çdo uebsajt, aplikacion ose mjet tjetër në të cilin jeni identifikuar me anë të Facebook-ut.

Më poshtë listohen disa këshilla se i të mbroni dhe siguroni fjalëkalimet e rrjeteve sociale:

1. Mos i ripërdorni fjalëkalimet dhe duhet t'i ndryshoni ato shpesh. Edhe nëse keni krijuar një fjalëkalim të fortë, mos e ripërdorni atë në shumë rrjete sociale, faqe interneti dhe aplikacione.
2. Përdorni një mjet për menaxhimin e fjalëkalimeve për të ruajtur fjalëkalimet tuaja. Përdorni mjetin e menaxhimit të fjalëkalimit të instaluar nga ekipi i IT/suporti, për të ruajtur fjalëkalimet personale dhe profesionale. Disa nga menaxherët më të njohur të fjalëkalimeve janë Dashlane, Keeper dhe LastPass. Mos i ruani fjalëkalimet në një skedar në kompjuterin ose smartfonin tuaj.
3. Përdorni autentifikimin me dy faktorë. Nëse një kriminel kibernetik hamendeson emrin e përdoruesit dhe fjalëkalimin e rrjetit tuaj social, autentifikimi me dy faktorë e detyron kriminelin që të këtëe dhe një PIN të sigurt për t'u identifikuar. Prandaj ju do të njoftoheni për përpjekjet e tij për tu loguar, dhe do të kuptoni që fjalëkalimi juaj është hakuar. Nëse e merrni këtë njoftim, refuzoni loginin dhe ndryshoni menjëherë fjalëkalimin dhe emrin e përdoruesit.
4. Mos hyni në llogari ose faqe interneti me kredencialet tuaja të rrjetit social. Nëse kredencialet tuaja në Facebook janë komprometuar, hakeri mund të hyjë në çdo aplikacion dhe faqe interneti që përdorin kredencialet tuaja të loginit në Facebook.
5. Kushtojini vëmendje kërkesave për miqësi, mesazheve dhe miqve të rinj. Jini të kujdesshëm ndaj kërkesave për miqësi në Facebook ose Instagram nga njerëzit që nuk kanë postime. Kriminelët kibernetikë mund të hakojnë llogarinë e mikut tuaj, t'ju dërgojnë një kërkesë për miqësi dhe më pas të fillojnë të mbledhin informacione rreth jush që do ta përdorin për të hakuar llogaritë tuaja. Nëse llogaria juaj e rrjetit social është hakuar, bëjeni publike duke postuar diçka të tillë si: "Kujdes, llogaria ime është hakuar. Mos iu përgjigj kërkesave të miqve, mesazheve të drejtpërdrejta ose bisedave nga llogaria ime."
6. Ji dyshues dhe i kujdesshëm. Mos u besoni emaileve që ju premtojnë se do ju rivendoset (reset) fjalëkalimi juaj. Asnjë kompani nuk do t'ju dërgojë kurrë një email për rivendosjen e fjalëkalimit ose verifikimin e llogarisë.

Ju jeni mjeti më e mirë i mbrojtjes nga sulmet kibernetike dhe hakimeve. Krijoni fjalëkalime të forta.