UDHËZIME PËR PRINDËRIT DHE EDUKATORËT

FJALËKALIME TË SIGURTA

Rëndësia e fjalëkalimeve të forta dhe të sigurta
Një fjalëkalim i fortë shërben si mbrojtja juaj kryesore kundër aksesit të paautorizuar. Fjalëkalimet funksionojnë si çelësat për llogaritë tuaja online dhe informacionin personal.

Çfarë përbën një fjalëkalim të fortë dhe të sigurt?
Ekspertët e sigurisë rekomandojnë përdorimin e një "fjalëkalimi" në vend të një fjalëkalimi të thjeshtë tradicional. Kjo frazë duhet të jetë relativisht e gjatë - 8-12 karaktere ose më shumë - dhe të përbëhet nga fjalë në dukje të rastësishme të kombinuara me numra, simbole dhe shkronja të mëdha dhe të vogla. Duhet të jetë diçka që mbahet mend personalisht, por e vështirë për t'u hamendësuar nga të tjerët. Informacioni personal dhe/ose fjalët e zakonshme duhet të shmangen. Simbolet, të tilla si përdorimi i “$” në vend të shkronjës “S”, ose përfshirja e simboleve si “&” ose “%” duhet të përfshihen. Megjithatë, duhet të tregohet kujdes; $1ngle NUK është një fjalëkalim i mirë, pasi hajdutët e fjalëkalimeve janë të vetëdijshëm për kombinime të tilla. Në të kundërtën, **Mbf$TJ1ravng** (shkurtim për “My best friend Sam T Jones is a very nice guy”) është një shembull i shkëlqyer i një fjalëkalimi të fortë.

A duhet të ndryshohet fjalëkalimi i sigurisë dhe sa shpesh?
Është e preferuar të ndryshohet fjalëkalimi i sigurisë periodikisht, njësoj si pastrimi i shtëpisë! Kjo praktikë njihet si higjiena kibernetike dhe është thelbësore për sigurinë online.

A rekomandohet të ndani fjalëkalimet e sigurta me të tjerët?
Si rregull i përgjithshëm, fjalëkalimi personal i sigurisë nuk duhet të ndahet kurrë me askënd. Megjithatë, mund të ketë raste kur ndarja e një fjalëkalimi mund të jetë e dobishme, siç është ndarja e fjalëkalimeve të sigurisë së fëmijëve me ju si prindër. Edhe me miqtë, fëmijët nuk duhet të ndajnë fjalëkalime**.** Shpjegoni se ndarja e fjalëkalimeve është si të japësh çelësat e shtëpisë.
Për më tepër, ndërsa mund të duket e qartë, studimet tregojnë se fjalëkalimet e sigurisë zakonisht ndahen në fletëpalosje ngjitëse të bashkangjitura në monitorët e kompjuterëve. Kjo është një ide e keqe. Nëse duhet ta shkruani, sigurohuni që shënimi të jetë i fshehur siç duhet.

A është e sigurt të përdoret i njëjti fjalëkalim në shumë faqe interneti dhe aplikacione?
Jo, nuk është e sigurt. Nëse ndonjë nga llogaritë tuaja hakohet ose nëse dikush i lidhur me atë faqe vjedh fjalëkalimin tuaj, kriminelët mund të përpiqen ta përdorin atë në faqe dhe aplikacione të tjera. Është më mirë të dalloni fjalëkalimet tuaja duke shtuar shkronja, numra ose simbole unike për secilën llogari.

Kuptimi i Autentifikimit Shumëfaktorësh?

Shpesh i referuar si autentifikim me dy faktorë (2FA), autentifikimi me shumë faktorë shton një "hap" shtesë - zakonisht opsional - për të aksesuar një llogari, pajisje ose dokument.
Shërbime të shumta, duke përfshirë platformat bankare dhe të mediave sociale, ofrojnë vërtetim shumëfaktorësh si një opsion për të rritur sigurinë e llogarive tuaja përtej një fjalëkalimi të fortë. Zakonisht, kjo përfshin marrjen e një mesazhi me tekst ose një lloj tjetër mesazhi në një pajisje celulare të regjistruar që përmban një kod që duhet ta futni për të konfirmuar identitetin tuaj. Përveç kësaj, ka aplikacione të disponueshme që mund të gjenerojnë këto kode. Në shumicën e rasteve, nuk do të keni nevojë ta përdorni këtë kod kur të identifikoheni nga një pajisje e njohur, siç është kompjuteri, tableti ose telefoni juaj. Mbani mend se përfshirja e një hapi të dytë për identifikimin (si një kod i dërguar në telefonin tuaj) rrit ndjeshëm sigurinë tuaj!

Rekomandohet fuqimisht të përdorni një fjalëkalim të fortë, së bashku me vërtetimin shumëfaktorësh, sa herë që të jetë e mundur.

Më shumë mënyra për të qëndruar të sigurt

Përdorni një Menaxher Fjalëkalimesh
Ndihmojeni familjen tuaj të qëndrojë e sigurt duke përdorur një menaxher fjalëkalimesh si RoboForm ose LastPass. Këto programe dhe shërbime në internet funksionojnë në kompjuterë personalë dhe pajisje mobile, dhe krijojnë fjalëkalime të forta dhe unike për secilën nga llogaritë tuaja - kështu që nuk keni pse t'i mbani mend të gjitha. Shfletuesit si Chrome, Safari dhe Edge kanë gjithashtu menaxherë fjalëkalimesh falas të integruar. Do t'ju duhet të mbani mend vetëm një fjalëkalim të fortë "master" për të hyrë në program ose në faqen e sigurt që ruan të gjitha fjalëkalimet tuaja. Bëjeni atë fjalëkalim master shumë të fortë - nëse dikush e kupton, ai mund të hyjë në të gjitha llogaritë tuaja.

Kujdes nga sulmet e phishing-ut
Tregoni kujdes para se të klikoni ndonjë lidhje — edhe nëse duket sikur është nga një burim i besueshëm. Nëse një mesazh ju kërkon të identifikoheni, të ndryshoni fjalëkalimin tuaj ose të jepni informacione personale, mund të jetë një mashtrim phishing që përpiqet të vjedhë të dhënat tuaja — mos harroni se mund të jetë i ligjshëm ose pjesë e një mashtrimi phishing të projektuar për të kapur të dhënat tuaja për qëllime dashakeqe. Rekomandohet të shkruani adresën e faqes së internetit (URL) direkt në shfletuesin tuaj në vend që të klikoni lidhjet.

Sigurohuni që pajisjet të jenë të mbrojtura
Softuer keqdashës - viruset dhe programet spiune, si regjistruesit e tastierës (të cilët mund të gjurmojnë shkrimin tuaj), mund të përdoren për të vjedhur fjalëkalimet tuaja të sigurisë. Mbroni pajisjet tuaja duke përdorur softuer antivirus ose anti-malware të përditësuar. Gjithashtu, sigurohuni që sistemi juaj operativ, aplikacionet dhe shfletuesi të jenë të përditësuar plotësisht.

Përdorni Zhbllokimin me Gjurmët e Gishtave ose me Fytyrë në Pajisjet tuaja Mobile
Shumica e telefonave inteligjentë mund të mbrohen me një kod, zakonisht një sekuencë numrash ose një model të vizatuar në ekran. Shumë prej tyre ju lejojnë gjithashtu të regjistroni gjurmët e gishtërinjve, duke ofruar një nivel të lartë sigurie (Jini të sigurt, të dhënat e gjurmëve të gishtërinjve ose të fytyrës mbeten në pajisjen tuaj dhe nuk ndahen me asnjë tjetër.)

Kontrolloni dhe diskutoni rregullisht për llogaritë
Rishikoni rregullisht së bashku llogaritë online të fëmijës suaj. Ndihmojeni në përditësimin e fjalëkalimeve të sigurisë dhe mësojeni si të dallojë çdo gjë të dyshimtë — si mesazhe të çuditshme ose alarme hyrjeje.

Për informacione të hollësishme, vizitoni faqen tonë të internetit www.mksafenet.mk

Kini kujdes para se të klikoni në një lidhje (edhe nëse duket se është nga një faqe e ligjshme) ata kurrë nuk do t'ju kërkojnë të ndryshoni fjalëkalimin tuaj ose të jepni informacione personale.

Ky projekt është financuar me mbështetjen e Komisionit Evropian. Përmbajtja e teksti pasqyron vetëm qëndrimet e autorit, dhe Komisioni Evropian nuk mban asnjë përgjegjësi për përdorimin e mundshëm të informacionit të përfshirë në të.

Bashkëfinancuar nga Bashkimi Evropian