ВОДИЛКИ ЗА РОДИТЕЛИ И НАСТАВНИЦИ

БЕЗБЕДНОСНИ ЛОЗИНКИ

Важноста на силните безбеднносни лозинки
Силната лозинка е ваша примарна одбрана од неовластен пристап. Лозинките функционираат како клучеви до вашите онлајн сметки и лични податоци.

Што претставува силна безбедносна лозинка?
Се препорачува користење сложена наместо едноставна, традиционална лозинка. Лозинката потребно е да биде релативно долга од 8-12 знаци или повеќе, составена од навидум случајни зборови комбинирани со броеви, симболи и големи и мали букви. Истата може да содржи нешто што лично полесно се помни, но тешко е за останатите да го погодат. Потребно е да се избегнуваат лични податоци и/или вообичаени зборови.

Се препорачува да се вклучат симболи, како што е употребата на „$“ наместо буквата „S“ или вклучување симболи како „&“ или „%“. Сепак, потребно е да комбинацијата да биде претпазлива; $1ngle HE е добра лозинка, бидејќи крадците на лозинки се свесни за ваквите комбинации. Спротивно на тоа, Mbf$TJ1ravng (скратено од „Мојот најдобар пријател Сем Т. Џонс е навистина многу фин човек“) е одличен пример за силна лозинка.

Дали треба да се менува безбедносната лозинка и колку често?
Се препорачува периодично да се менува безбедносната лозинка, исто како чистење на куќата! Оваа практика е позната како сајбер хигиена и е клучна за безбедноста на интернет.

Дали се препорачува да се споделуваат безбедносни лозинки со други?
Општо правило е личната безбедносна лозинка никогаш да не се споделува со други. Сепак, постојат случаи кога споделувањето може да биде корисно, како што е споделувањето на безбедносните лозинки на децата со вас како родители. Дури и со пријателите, децата не треба да ги споделуваат своите лозинки. Објаснете дека споделувањето лозинки е како давање на клучеви од сопствената куќа.

Дали е безбедно да се користи истата лозинка на повеќе страници и апликации?
Не, не е безбедно. Доколку некој од вашите профили е хакнат (има неовластен пристап) или во случај некој поврзан со таа страница ви ја украде лозинката, криминалците може да се обидат да ја користат на други страници и апликации.

Повеќефакторската автентикација

Честопати нарекувана двофакторска автентикација (2FA), мултифакторската автентикација додава дополнителен – обично опционален – „чекор“ за пристап до профил, уред или документ.

Покрај силната безбедносна лозинака, постојат бројни услуги, вклучувајќи банкарски платформи и платформи за социјални медиуми, кои обезбедуваат мултифакторска автентикација како опција за подобрување на безбедноста на вашите профили. Ова вклучува примање текстуална порака или друг вид порака на регистриран мобилен уред што содржи код што мора да го внесете за да го потврдите вашиот идентитет. Достапни се и апликации што можат да ги генерираат овие кодови. Во повеќето случаи, нема да треба да го користите овој код кога се најавувате од препознаен уред, како што е вашиот компјутер, таблет или телефон. Имајте на ум дека вклучувањето втор чекор при најавување (како на пример код испратен на вашиот телефон) значително ја зголемува вашата безбедност!

Секогаш кога постои можност се препорачува користење силна безбедносна лозинка заедно со мултифакторска автентикација.

Останати начини да останете безбедни

Користете менаџер за лозинки
Помогнете му на вашето семејство да остане безбедно со користење на менаџер за лозинки како RoboForm или LastPass. Овие програми и веб-услуги функционираат на персонални компјутери и мобилни уреди и создаваат силни, уникатни лозинки за секоја од вашите профили - така што не мора да ги запомните сите. Прелистувачите како Chrome, Safari и Edge исто така имаат бесплатни вградени менаџери за лозинки. Потребно ќе биде да запомните само една силна „главна“ лозинка за да пристапите до програмата или безбедната страница што ги чува сите ваши лозинки. Направете ја таа главна лозинка многу силна и имајте на ум дека доколку некој ја добие, може да пристапи до сите ваши профили.

Не наседнувајте на „фишинг“ напади
Бидете посебно внимателни пред да кликнете на линк, дури и доколку доаѓа од сигурен извор. Доколку добиете порака во која се бара од вас да се најавите, да ја промените вашата лозинка или да дадете други лични податоци. Тоа може да биде легитимно или да биде измама со „фишинг“ напад каде што информациите што ги внесувате се преземаат од хакер. Доколку се сомневате, најавете се рачно со внесување на она што знаете дека е URL-то на страницата во прозорецот на вашиот прелистувач.

Обезбедете дека вашите уреди се безбедни
Малициозен софтвер, вклучувајќи „логери на тастатура“ што ги снимаат сите ваши притискања на копчиња, се користат за кражба на лозинки и други информации. За да ја зголемите безбедноста, проверете дали користите ажуриран софтвер против малициозен софтвер и дали вашиот оперативен систем, апликации и прелистувач се ажурирани.

Користете препознавање преку користење на отпечатоци од прсти или лице на вашиот телефон
Повеќето телефони можат да бидат заклучени на единствениот начин преку внес на код, низа броеви или можеби шема што ја цртате на екранот. Некои телефони ви дозволуваат да регистрирате отпечатоци од прсти, што е прилично безбедно. Некои апликации, особено финансиските, ви дозволуваат да ги отворите преку скенирање на отпечаток од прст или лице. (Вашиот отпечаток од прст или скенирање на лице останува на вашиот телефон и не им се доставува на компаниите.)

Редовно проверувајте и разговарајте за профилите
Редовно прегледувајте ги заедно онлајн профилите на вашето дете. Помогнете му во ажурирањето на безбедносните лозинки и научете го како да препознава што е сомнително - како на пример чудни пораки или известувања за најавување.

За подетални информации, посетете ја нашата интернет страна: www.mksafenet.mk

Бидете внимателни пред да кликнете на линк (дури и доколку изгледа дека е од легитимна страница) на која се бара да ја промените лозинката или да ги внесете ваши лични податоци!

Ко-финансирано од Европска Унија