ВОДИЛКИ ЗА РОДИТЕЛИ И НАСТАВНИЦИ

САЈБЕР БЕЗБЕДНОСТ

Зошто е важна дигиталната безбедност?
Незаштитените уреди и онлајн сметки може сериозно да ја загрозат вашата приватност, финансиска стабилност, па дури и лична безбедност. Уште повеќе, еден небезбеден уред може да прошири малициозен софтвер и да го изложи на ризик поширокото онлајн опкружување.

Кои се најважните чекори за да останете безбедни?

- Користете силни и единствени лозинки – и никогаш не ги споделувајте
- Избегнувајте кликнување на сомнителни линкови или пораки
- Инсталирајте доверлив безбедносен софтвер
- Редовно ажурирајте ги вашите апликации и систем
- Преземајте апликации само од проверени извори
- Бидете внимателни на онлајн измами и фишинг

Дали децата и тинејџерите се изложени на ризик?
Да. Младите се особено ранливи на дигитални закани. Нивната љубопитност и честото присуство онлајн ги прави подложни на измами, хакирање и штетна содржина. Тие, исто така, често се цел на кражба на идентитет. Затоа, раното образование за дигитална безбедност е клучно – за да ги оспособи младите со знаење и навики што ќе им помогнат да се заштитат себеси и другите во онлајн просторот.

Што е двофакторска автентикација?

Двофакторската автентикација (2FA), позната и како повеќефакторска автентикација, додава дополнителен слој на безбедност на вашите онлајн сметки. Слично на користењето банкоматска картичка, потребни се две работи: нешто што го знаете (вашата лозинка) и нешто што го имате (обично вашиот телефон).

Кога ќе се обидете да се најавите од нов или непрепознаен уред, ќе добиете привремен код преку СМС, апликација или е-пошта што мора да го внесете заедно со вашата лозинка. Овој чекор помага да се потврди дека вие сте оној што се обидува да пристапи до сметката. Препорачуваме да го овозможите 2FA каде и да е достапно.

Како можам да создадам лозинка што е безбедна и лесна за запомнување?
Замислете реченица што лесно можете да ја запомните - нешто како: „Ја запознав Марта Петрова во средното училиште Јосип Броз во 2012 година.“
Сега земете ја првата буква од секој збор, додадете броеви и посебен симбол за да формирате силна лозинка: ➡ **IMMPaJBHSin#12**
За да ја направите уште побезбедна, персонализирајте ја за секоја веб-страница со додавање букви што ја идентификуваат - како „**Fb**“ за Facebook или „**Ig**“ за Instagram: ➡ **IMMPaJBHSin#12Fb**

Што е „фишинг“?
Фишинг е кога ќе добиете лажна е-пошта или порака што изгледа како да е од доверлив извор - како вашата банка или училиште - со која ве замолуваат да кликнете на линк и да се најавите. Но, линкот води до лажна страница дизајнирана да ги украде вашите податоци за најавување, кредитна картичка или лични информации. Тоа е еден од најчестите начини на кои хакерите добиваат пристап до сметки.

Повеќе совети за безбедност

Внимавајте каде кликнувате

Некои веб-страници изгледаат безбедно, но всушност се дизајнирани да ве измамат. Тие можат да го инфицираат вашиот уред со малициозен софтвер. Овие лажни страници често нудат „бесплатна“ или привлечна содржина, како филмови, коцкање или материјал за возрасни.

Внимавајте и на clickjacking - линкови на друштвените медиуми што изгледаат интересно, но водат до спам или штетни страници, па дури и објавуваат содржина на вашиот профил.

Како да препознаете лажен линк?

Сајбер-криминалците вешто ги прават лажните линкови .

- **Проверете за HTTPS.** Иако не е безгрешна, безбедната веб-страница ќе започне со https://. Сепак, дури и лошите актери можат да добијат SSL сертификати, затоа не потпирајте се само на ова.
- **Внимателно погледнете ја URL-адресата.** Лажните линкови често имаат правописни грешки или дополнителни знаци. На пример, go0gle.com наместо google.com.
- **Не верувајте на скратени линкови.** Услуги како bit.ly ја кријат вистинската URL-адреса. Користете алатка за проширување на URL-адресата или избегнувајте кликнување.
- **Бидете внимателни со емотивни апели и зборови кои повикуваат на итност.** Фрази како „Вашата сметка ќе биде заклучена!“ или „Кликнете тука за да ја добиете вашата награда!“ се вообичаени трикови.

Размислете пред да кликнете!

Ажурирајте го софтверот и апликациите

Секогаш ажурирајте го вашиот оперативен систем, прелистувач и апликации. Ажурирањата ги поправаат безбедносните недостатоци и го штитат вашиот уред. Вклучете ги автоматските ажурирања и по секое ажурирање, проверете ги поставките за приватност - тие може да се вратат на стандардните.

Повеќе совети за да останете безбедни на интернет

- Внимавајте на измами. Бидете претпазливи со лажни добротворни организации, пораки од „пријатели“ кои бараат пари или емоционални апели по катастрофи.
- Внимавајте што преземате. Избегнувајте преземање апликации, датотеки или софтвер од непознати извори.
- Користете заштита од малициозен софтвер. Заштитете го вашиот уред со сигурни безбедносни апликации. За список на алатки, посетете ја страницата: **www.mksafenet.mk**

Лажните или хакираните веб-страници се сериозен ризик за вашиот уред и податоци

За повеќе информации, посетете ја www.mksafenet.mk

Текстот ги одразува само ставовите на авторот, и Комисијата не може да се смета за одговорна за каква било употреба на информациите содржани во неа.

Ко-финансирано од Европска Унија