UDHËZUES PËR PRINDËRIT DHE MËSUESIT

SIGURIA KIBERNETIKE

Pse është e rëndësishme siguria digjitale?
Pajisjet dhe llogaritë online të pasigurta mund të kompromentojnë seriozisht privatësinë, stabilitetin financiar dhe madje edhe sigurinë personale. Për më tepër, një pajisje e pasigurt mund të përhapë programe keqdashëse dhe ta vërë në rrezik mjedisin tuaj më të gjerë online.

Cilat janë hapat më të rëndësishëm për të qëndruar të sigurt?

- Përdorni fjalëkalime të forta dhe unike - dhe mos i ndani kurrë ato
- Shmangni klikimin në lidhje ose mesazhe të dyshimta
- Installoni softuer sigurie të besueshëm
- Përditësoni rregullisht aplikacionet dhe sistemin tuaj
- Shkarkoni vetëm aplikacione nga burime të besueshme
- Kini kujdes nga mashtrimet dhe phishing-u në internet

A janë fëmijët dhe adoleshentët në rrezik?
Po. Të rinjtë janë veçanërisht të prekshëm ndaj kërcënimeve digjitale. Kurioziteti dhe prania e tyre e shpeshtë në internet i bëjnë ata të ndjeshëm ndaj mashtrimeve, hakerimit dhe përmbajtjes së dëmshme. Ata gjithashtu shpesh janë në shënjestër të vjedhjes së identitetit. Kjo është arsyeja pse edukimi i hershëm për sigurinë dixhitale është thelbësor - për t'i pajisur të rinjtë me njohuritë dhe zakonet që do t'i ndihmojnë ata të mbrojnë veten dhe të tjerët në internet.

Çfarë është autentifikimi me dy faktorë?

Autentifikimi me dy faktorë (2FA), i njohur edhe si autentifikim shumëfaktorësh, shton një shtresë shtesë sigurie në llogaritë tuaja online. Ngjashëm me përdorimin e një karte bankomati, kërkon dy gjëra: diçka që e dini (fjalëkalimin tuaj) dhe diçka që keni (zakonisht telefonin tuaj).

Kur përpiqeni të hyni nga një pajisje e re ose e panjohur, do të merrni një kod të përkohshëm me anë të SMS-it, aplikacionit ose email-it që duhet ta futni së bashku me fjalëkalimin tuaj. Ky hap ndihmon në verifikimin se jeni ju ai që po përpiqeni të hyni në llogarinë tuaj.

Ne rekomandojmë aktivizimin e 2FA-së kudo që është e disponueshme.

KSi mund të krijoj një fjalëkalim të sigurt dhe të lehtë për t'u mbajtur mend?
Imagjinoni një fjali që mund ta mbani mend lehtë - diçka si: "E takova Marta Petrovën në shkollën e mesme Josip Broz në vitin 2012."
Tani merrni shkronjën e parë të secilës fjalë, shtoni numra dhe një simbol të veçantë për të formuar një fjalëkalim të fortë: ➡ **IMMPaJBHSin#12**
Për ta bërë edhe më të sigurt, personalizojeni atë për secilën faqe interneti duke shtuar shkronja që e identifikojnë atë - si "**Fb**" për Facebook ose "**Ig**" për Instagram: ➡ **IMMPaJBHSin#12Fb**

Çfarë është "phishing-u"?
Fishingu është kur Ju merrni një email ose mesazh të rremë që duket se është nga një burim i besueshëm - si banka ose shkolla juaj - që ju kërkon të klikoni një lidhje dhe të identifikoheni. Por lidhja çon në një faqe të rreme të projektuar për të vjedhur informacionin tuaj të identifikimit, informacionin e kartës së kreditit ose informacionin personal. Është një nga mënyrat më të zakonshme që hakerat fitojnë akses në llogari.

Më shumë këshilla sigurie

Kini kujdes ku klikoni.

Disa faqe interneti duken të sigurta, por në të vërtetë janë të dizajnuara për t'ju mashtruar. Ato mund të infektojnë pajisjen tuaj me programe keqdashëse. Këto faqe të rreme shpesh ofrojnë përmbajtje "falas" ose tërheqëse, siç janë filmat, lojërat e fatit ose materiale për të rritur.

Gjithashtu, kini kujdes nga “clickjacking” - lidhje në mediat sociale që duken interesante, por që çojnë në faqe të padëshiruara ose të dëmshme, ose madje postojnë përmbajtje në profilin tuaj.

Si të dalloni një lidhje të rreme?
Kriminelët kibernetikë janë të aftë në krijimin e lidhjeve të rreme.

- **Kontrolloni për HTTPS.** Edhe pse nuk është e pagabueshme, një faqe interneti e sigurt do të fillojë me https://. Megjithatë, edhe aktorët e këqij mund të marrin certifikata SSL, prandaj mos u mbështetni vetëm në këtë.
- **Shikoni me kujdes URL-në.** Lidhjet e rreme shpesh kanë gabime drejtshkrimore ose karaktere shtesë. Për shembull, go0gle.com në vend të google.com.
- **Mos u besoni lidhjeve të shkurtuara.** Shërbime si bit.ly fshehin URL-në e vërtetë. Përdorni një mjet zgjerimi URL ose shmangni klikimin.
- **Kini kujdes me thirrjet emocionale dhe fjalët që përcjellin urgjencë**. Fraza si "Llogaria juaj do të bllokohet!" ose "Klikoni këtu për të marrë shpërblimin tuaj!" janë truke të zakonshme.

Mendo para se të klikosh!

Përditësoni softuerin dhe aplikacionet tuaja

Mbajeni gjithmonë të përditësuar sistemin tuaj operativ, shfletuesin dhe aplikacionet. Përditësimet rregullojnë dobësitë e sigurisë dhe mbrojnë pajisjen tuaj. Aktivizoni përditësimet automatike dhe pas çdo përditësimi, kontrolloni cilësimet e privatësisë - ato mund të rivendosen në cilësimet fillestare.

Më shumë këshilla për të qëndruar të sigurt në internet

- Kini kujdes nga mashtrimet. Kini kujdes nga bamirësitë e rreme, mesazhet nga "miqtë" që kërkojnë para ose thirrjet emocionale pas fatkeqësive.
- Kini kujdes se çfarë shkarkoni. Shmangni shkarkimin e aplikacioneve, skedarëve ose softuerëve nga burime të panjohura.
- Përdorni mbrojtje nga programet keqdashëse. Mbrojeni pajisjen tuaj me aplikacione të besueshme sigurie. Për një listë mjetesh, vizitoni: **www.mksafenet.mk**

Faqet e internetit të rreme ose të hakuara përbëjnë një rrezik serioz për pajisjen dhe të dhënat tuaja

Për më shumë informacion, vizitoni www.mksafenet.mk

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.

www.mksafenet.mk

Bashkëfinancuar nga Bashkimi Evropian