

**OUCH!**

Si të identifikoni se të dhënat tuaja janë hakuar

Pavarësisht se çfarë lloji të pajisjeve apo aplikacionesh përdorni, probabiliteti është i madh që të keni ndonjë incident të sigurisë kibernetike dhe të hakohen të dhënat e juaja. Në tekstin e mëposhtëm mund të gjeni disa udhëzime që ju ndihmojnë të identifikoni se a janë hakuar të dhënat tuaja dhe nëse po, si të veproni?

Llogaritë tuaja online

- Familja ose miqtë thonë se po marrin mesazhe ose ftesa të pazakonta nga llogaria juaj për të cilat ju e dini se nuk i keni dërguar.
- Fjalëkalimi juaj në një llogari nuk funksionon më, edhe pse e dini se fjalëkalimi është i saktë.
- Ju pranoni njoftime nga faqe të ndryshme të internetit se dikush ka hyrë në llogarinë tuaj edhe pse ju e dini se nuk keni hyrë vetë. Mos klikoni në asnjë lidhje në njoftime të tilla për të kontrolluar llogarinë tuaj; në vend të kësaj, shkruani vetë adresën e ueb faqes në shfletuesin tuaj, përdorni faqen tuaj të ruajtur më parë ose hyni në llogarinë tuaj nga një aplikacion celular.

Kompjuteri, telefonat e mençur ose pajisjet tjera të mençura

- Programi juaj i antivirusit gjeneron një alarm se sistemi juaj është i infektuar. Sigurohuni që është programi juaj i antivirusit po e gjeneron alarmin dhe jo një dritare e rastësishme që shfaqet nga një faqe interneti që përpiqet t'ju mashtrojë që të instaloni ndonjë aplikacion ose program qëllimkeq. Nëse nuk jeni të sigurt? Hapni dhe kontrolloni programin tuaj të antivirusit për të konfirmuar nëse kompjuteri juaj është vërtetë i infektuar.
- Ju shfaqet një dritare aty për aty që thotë se të dhënat në pajisjen tuaj janë enkriptuar/koduar dhe ju duhet të paguani një shpërblim për të rikthyer të dhënat tuaja.
- Duket se aplikacionet ose programet në pajisjen tuaj janë duke u hapur në të njëjtën kohë dhe si pasojë janë duke e penguar njëra tjetrën dhe po hapen shumë ngadalë.
- Gjatë shfletimit në ueb faqe të ndryshme, shpesh ridrejtoheni në faqe që nuk dëshironi t'i vizitoni ose shfaqen faqe të reja të padëshiruara.

Llogaritë bankare

- Ka shpenzime të dyshimta ose të panjohura në kartën tuaj të kreditit ose llogarinë bankare që ju e dini se nuk i keni bërë.

Si të veproni – Si të riktheni kontrollin mbi llogaritë tuaja?

Nëse dyshoni se të dhënat tuaja janë hakuar, qëndroni të qetë; do ta kaloni këtë. Nëse të dhënat e hakuara janë të institucionit, mos u përpiqni ta rregulloni vetë problemin; raportojeni atë menjëherë. Nëse është një pajisje ose llogari personale që është hakuar, këtu janë disa hapa që mund të ndërmerrni:

- **Rikuperimi i llogarive tuaja online:** Nëse keni ende qasje në llogarinë tuaj, identifikohuni nga një pajisje e besuar që nuk është e infektuar dhe rivendosni fjalëkalimin tuaj. Pasi të identifikoheni, sigurohuni që të vendosni një fjalëkalim të ri, unik dhe të fortë, sa më kompleks dhe të gjatë, aq më mirë. Mos harroni, secila prej llogarive tuaja duhet të ketë një fjalëkalim të ndryshëm. Gjithashtu, nëse është e mundur aktivizoni Verifikimin/Autentifikimin me shumë faktorë (MFA) për llogaritë tuaja, duke siguruar që sulmuesit kibernetikë nuk mund të hyjnë prapë në llogarinë tuaja. Nëse nuk keni më qasje në llogarinë tuaj, kontaktoni faqen e internetit dhe informoni se llogaria juaj është marrë nën kontroll nga dikush tjetër.
- **Rikuperimi i kompjuterit, telefonave të mençur ose pajisjet tjera të mençura:** Nëse programi juaj i antivirusit nuk është në gjendje të rikuperojë kompjuterin e infektuar ose dëshironi të jeni më të sigurt e të siguroni pajisjen tuaj më shumë, konsideroni riinstalimin e sistemit operativ dhe rikonfigurimin e kompjuterit. Kjo shpesh kërkon fshirjen ose zëvendësimin e diskut e më pas riinstalimin dhe përditësimin e sistemit operativ.
- **Rikuperimi i llogarive bankare:** Për problemet me kartën tuaj të kreditit ose ndonjë llogari tjetër bankare, telefononi menjëherë bankën ose kompaninë tuaj të llogarisë bankare. Telefononi bankën duke përdorur një numër telefoni të besueshëm, si p.sh. numrin e telefonit të shënuar në pjesën e pasme të kartës suaj bankare, numrin e printuar në pasqyrat tuaja financiare ose vizitoni faqen e tyre të internetit. Monitoroni shpesh gjendjet dhe raportet tuaja bankare. Përveç kësaj, konsideroni vendosjen e një limiti për shumën e mjeteve financiare që mund të shpenzoni gjatë një blerjeve me kredit kartën tuaj bankare.

Nëse dyshoni se keni qenë preh e ndonjë sulmi kibernetikë, raportoni menjëherë incidentin te Sektori i Mbrojtjes Kibernetike në MM.

Shënim:

Materiali është marrë nga Instituti për administrim dhe siguri të sistemeve - SANS dhe është përshtatur në buletin (Newsletter) nga Sektori i Mbrojtjes Kibernetike, në kuadër të Departamentit për Komunikim dhe Teknologji Informative.

Ju lutem nëse keni ndonjë paqartësi, mos hezitoni të na kontaktoni.