Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË EDICION..

- Hyrje
- Privatësia
- Siguria

Mediat Sociale

Hyrje

Faqet e mediave sociale sikurse janë Facebook, Twitter, Instagram dhe Linkedin janë burime të shkëlqyeshme, që ju lejojnë të bashkëpunoni dhe të ndani informata me njerëz në të gjithë botën. Por me këtë fuqi vijnë edhe rreziqe, jo vetëm për ju por edhe për familjen tuaj, shokët apo punëdhënësin tuaj. Në këtë broshurë ne do të spjegojmë disa nga këto rreziqe dhe si mund të përdoren këto faqe në mënyrë të sigurt.

Botuesi i ftuar

Tanya Baccam është konsulente me përvojë të gjatë e sigurisë. Ajo ka qenë autore në SANS si dhe instruktore për më shumë se një dekadë, duke përfshirë disa lëndë në mesin e së cilave SEC502, SEC542, SEC401, MGT414, AUD507. Mund ta ndiqni në Twitter në **@tbaccam**.

Privatësia

Një brengë e zakontë që lidhet me mediat sociale është mbrojtja e të dhënave tuaja personale. Rreziqet potenciale përfshijnë:

- **Ndikimi në të ardhmen tuaj**: Disa organizata bëjnë kërkime në mediat sociale si pjesë e kontrollit të të kaluarës së dikujt. Nëse ata gjejnë foto inkriminuese ose postime të dyshimta, pa marrë parasysh sa të vjetra janë ato, kjo mund të ndikojë që të mos ju punësojë dikush apo të mos ju promovojë në punë. Poashtu, shumë universitete bëjnë kontrolle të këtilla për vlerësimin e aplikimeve të studentëve. Opsionet e privatësisë mund të mos ju mbrojnë, sepse këto organizata ju kërkojnë t'i bëni "Like" faqeve të tyre apo postimeve, dhe disa nga këto shënime mund të jenë arkivuar në faqe tjera.
- **Sulme kundër jush**: Sulmuesit kibernetikë mund të analizojnë postimet tuaja dhe t'i përdorin ato që të qasen në informatat tuaja apo të organizatës ku punoni. Për shembull, ata mund t'i përdorin informatat që ju ndani që të qëllojnë pyetjen e fshehtë që ju keni për të ndërruar fjalëkalimet tuaja, apo të krijojnë emaile të veçanta kundër jush të njohura me emrin "spearfishing", ose të thërrasin dikë në organizatën tuaj duke pretenduar që jeni ju. Përveç këtyre mënyrave dikush edhe mund të tentojë të ndërhyjë fizikisht, duke identifikuar vendin ku ju punoni apo jetoni.
- **Dëmtimi pa dashje i punëdhënësit tuaj**: Kriminelët apo konkurrentët mund të përdorin kundër punëdhënësit tuaj çfarëdo informate të ndjeshme që ju mund të postoni për organizatën ku punoni. Poashtu, postimet tuaja mund të shkaktojnë dëm reputacional për organizatën tuaj. Sigurohuni që keni verifikuar politikat e organizatës ku punoni para se të postoni çfarëdo detaji për punën tuaj, sepse postimet në media sociale mund te jenë duke u monitoruar.

Mbrojtja më e mirë është të kufizoni sasinë e informatave që postoni. Është e vërtetë që opsionet e privatësisë mund t'ju ofrojnë një lloj mbrojtjeje, por kini parasysh që ato janë nganjëherë konfuze dhe ndërrohen shpesh pa vetëdijen tuaj. Ajo që mendonit që ishte private në një moment mund të bëhet lehtësisht publike për arsye të ndryshme. Gjithashtu, duhet ta dini që privatësia e postimeve tuaja është poaq e sigurt sa njerëzit me të cilët e ndani atë informatë. Sa më shumë shokë

Mediat Sociale

e kontakte me të cilët e ndani një informatë, aq më shumë rritet probabiliteti që ajo informatë të bëhet publike. Ju duhet të mendoni që çdo gjë që postoni mundet apo do të bëhet publike dikur dhe do të mbetet përgjithmonë në Internet.

Në fund, kini kujdes se çka postojnë edhe shokët tuaj për juve. Nëse postojnë diçka të papërshtatshme, kërkojini që ta largojnë. Nëse ju refuzojnë apo ju injorojnë në kërkesën tuaj, kontaktoni me faqen e mediumit social edhe kërkoni që ta largojnë atë përmbajtje për ju. Në të njejtën kohë, kini respekt edhe për atë që postoni ju për të tjerët.

Faqet e mediave sociale janë zbavitëse dhe të fuqishme, por kini kujdes se çfarë informata dhe me kë i shpërndani.

Siguria

Në vazhdimësi të brengave që duhet të keni për privatësinë, më poshtë do të gjeni disa hapa dhe këshilla se si t'i mbroni llogaritë tuaja në mediat sociale dhe aktivitetet online.

- **Qasja apo Logini**: Mbroni të gjitha llogaritë tuaja me një fjalëkalim të fortë dhe unik dhe mos e ndani këtë fjalëkalim me askë. Poashtu, disa media sociale ofrojnë autentifikim më të fortë, si autentifikimi në dy hapa. Gjithmonë aktivizoni këto mënyra autentifikimi sa herë të jetë e mundur. Në fund, mos e përdorni llogarinë që keni në mediat sociale për t'u qasur në llogari tjera, sepse nëse dikush e kompremeton atë llogari atëherë të gjitha llogaritë tjera janë të ekspozuara ndaj rrezikut.
- **Rregullimet e privatësisë**: Nëse i përdorni këto rregullime të privatësisë, sigurohuni që t'i keni rishikuar dhe testuar rregullisht. Mediat sociale shpesh i ndërrojnë këto rregullime dhe është e lehtë të bëni gabime. Poashtu, ka shumë aplikacione dhe shërbime që lejojnë që të dijnë vendndodhjen tuaj bashkë me përmbajtjen që postohet (e njohur si 'geotagging'). Kontrolloni shpesh këto detaje nëse doni ta mbani fshehur vendndodhjen tuaj fizike.
- **Enkriptimi**: Mediat sociale përdorin enkriptimin e njohur si HTTPS që të mbrojnë komunikimin tuaj online. Disa faqe si Twitter dhe Google+ e aktivizojnë këtë shërbim qysh në fillim, por disa shërbime tjera ju kërkojnë juve ta aktivizoni manualisht. Shihni në rregullimet e faqes së medias sociale dhe aktivizojeni shërbimin HTTPS si lidhje e përhershme sa herë të jetë e mundur.
- **Emaili**: Kini kujdes nga emailet që pretendojnë të jenë nga faqe të mediave sociale, sepse këto mund të maskohen fare lehtë dhe të jenë sulme nga kriminelët kibernetikë. Mënyra më e mirë t'i përgjigjeni mesazheve të tilla është të hyni në faqen e mediumit social, ndoshta nga ndonjë link i ruajtuar më herët dhe të lexoni apo përgjigjeni në mesazhe apo njoftime.
- **Linqe apo vegëza të dëmshme**: Kini kujdes nga linqet e ndryshme të dyshimta ose mashtrimeve që postohen në faqe të mediave sociale. Sulmuesit i përdorin mediat sociale që të shpërndajnë sulmet e tyre. Fakti që një mesazh mund të duket i postuar nga një shok nuk do të thotë që vërtet është postuar nga ata, sepse llogaria e tyre mund të jetë keqpërdorur. Nëse një familjar i juaj apo një shok ka postuar një mesazh të pazakontë të cilin nuk

Mediat Sociale

mund ta verifikoni menjëherë (si për shembull njoftim që mund të jenë plaçkitur dhe kanë nevojë për ju t'i dërgoni para), atëherë thirrini në telefon apo kontaktojini në ndonjë mënyrë që të konfirmoni që vertetë ata e kanë postuar atë mesazh.

- **Aplikacionet mobile**: Shumë faqe të mediave sociale ju ofrojnë edhe aplikacione për telefonat mobilë në mënyrë që t'i qaseni llogarisë nga aty. Sigurohuni që i keni shkarkuar këto aplikacione nga faqe të sigurta dhe që telefoni juaj i mençur mobil të jetë i mbrojtur me fjalëkalim të fortë. Nëse telefoni juaj është i pambrojtur kur ju ndodh ta humbisni, çdokush do të ketë qasje në faqet e mediave sociale përmes telefonit tuaj dhe do të fillojnë të postojnë në emrin tuaj.

Faqet e mediumeve sociale janë mënyra shumë të përshtatshme për të qenë në kontakt me botën. Nëse i ndiqni këshillat e theksuara në këtë artikull, ju do të mund të shijoni një eksperience më të sigurt. Për të mësuar më shumë se si ta përdorni faqen e mediumit social në mënyrë më të sigurt, ose të raportoni aktivitete të paautorizuara, kontrolloni faqen për siguri të faqes së mediumit social që përdorni.

Mëso më shumë

Regjistrohuni në buletinin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen http://www.securingthehuman.org.

Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyese profesioniste e gjuhës angleze në OSBE.

Burimet

Pasfrazat:	http://www.securingthehuman.org/ouch/2015#april2015
Verifikimi në dy hapa:	http://www.securingthehuman.org/ouch/2013#august2013
Përdorimi i sigurt i aplikacioneve Mobile:	http://www.securingthehuman.org/ouch/2015#january2015
Edukimi i fëmijëve mbi sigurinë kibernetike:	http://www.securingthehuman.org/ouch/2015#june2015
Siguria e Facebook-ut:	https://www.facebook.com/safety

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano