UDHËZUES RRETH INCIDENTEVE MË TË ZAKONSHME TË SIGURISË

Për të mbrojtur klientët e saj dhe në zbatim të Rregullores Nr.37 datë 29.10.2015 "Mbi Masat Teknike dhe Organizative Për të Garantuar Sigurinë dhe Integritetin e Rrjeteve Dhe/Ose Shërbimeve Të Komunikimeve Elektronike", shoqëria MIRBONET, publikon këtë udhëzues për përdoruesit "Rreth incidenteve më të zakonshme të sigurisë, veprimeve dhe/ose mjeteve që duhen ndjekur për të parandaluar ndodhjen e këtyre incidenteve dhe veprimeve që duhen ndjekur pas ndodhjes së incidenteve të sigurisë" MIRBONET kujdeset për ju! Me qëllim mbrojtjen tuaj nga aktivitete me natyrë mashtruese në fushën e komunikimeve elektronike, MIRBONET dëshiron t'ju japë disa këshilla të thjeshta.

I. Krijoni fjalëkalim të fortë që një fjalëkalim të jetë sa më i sigurtë duhet që të përmbajë minimalisht 8 (tetë) karaktere, ndër të cilat numra, gërma të mëdha dhe të vogla si dhe simbole. Nuk është e këshillueshme që të përdorni të njëjtin fjalëkalim kudo dhe ta ndani me të tjerët. Mënyrat e duhura për vendosjen e fjalëkalimeve a) Vendosni fjalëkalim sa më të gjatë Hakerat përdorin mënyra të shumta për të provuar të futen në llogaritë tuaja. Një nga teknikat është në bazë të një programi kompjuterik që bën kombinimin e shkronjave, numrave dhe simboleve. Sa më i gjatë të jetë fjalëkalimi aq më i gjatë do jetë ky proces dhe aq më i vështirë për tu përfunduar me sukses. b) Bëjeni fjalëkalimin tuaj një frazë pa kuptim Fjalëkalimet e gjata jane të mirë, fjalëkalimet e gjata që përfshijnë fjalë të rastit dhe fraza janë akoma më të mirë. Mos përdorni karaktere që janë sekuencial në tastierë. c) Përdorni numra, simbole dhe shkronja të mëdha dhe të vogla Bëni një përzierje të rastit të shkronjave me numra dhe simbole. P.sh.: Ju mund t ë zëvendësoni shkronjën O me numrin 0, ose shkronjën a me simbolin @. Nëse fjalëkalimi juaj është një frazë, përpiquni të kapitalizoni çdo shkronjë të parë të çdo fjale që përbëjnë frazën. d) Shmangni përdorimin e informacionit personal Nëse ka informacion për ju që është lehtësisht i gjetshëm si psh ditëlindje, adresë, qytet lindje, shkollë, emra te afërmish ose kafshë shtëpiake etj mundohuni mos ti përfshini në fjalëkalim. Nëse ju kërkohet të plotësoni një pyetje sigurie, zgjidhni një, përgjigja e së cilës nuk është e dukshme në rrjetet sociale. e) Mos ripërdorni fjalëkalime Kur hakerat realizojnë hakerime të mëdha p.sh me serverat e emaile-ve, lista e emaileve të hakeruar gjenerohen online. Nëse ju përdorni këtë llogari me të njëjtin fjalëkalim, atëherë informacioni juaj është lehtësisht i arritshëm. Përdorni fjalëkalime unike për çdo llogari. f) Filloni të përdorni një menaxhues fjalëkalimesh Menaxhuesit e fjalëkalimeve janë shërbime që gjenerojnë dhe ruajnë automatikisht fjalëkalime të vështirë. Këto fjalëkalime mbahen në një lokacion qëndror dhe të enkriptuar që ju mund ta aksesoni me një fjalëkalim Master (mos e humbisni këtë fjalëkalim). Shumë shërbime janë të lira për t'u përdorur dhe vijnë me karakteristika opsionale, të tilla si sinkronizimi i fjalëkalimeve të reja nëpër shumë pajisje dhe auditimi i sjelljes së fjalëkalimit tuaj për të siguruar që nuk po përdorni të njëjtin në shumë vende. g) Mbajini fjalëkalimet sa më të fshehtë Mos ia jepni fjalëkalimet asnjë personi tjetër. Mos e shkruani fjalëkalimin në pajisjen tuaj nëse jeni në rrezen e shikimit nga një person tjetër. Mos e shkruani fjalëkalimin tuaj në letrat që ngjisni në kompjuter. Nëse i ruani fjalëkalimet tuaja në një material në kompjuter, emërtoni materialin me një fjalë që nuk ka lidhje me objektin e materialit që është mbajtja shënim e fjalëkalimeve.

h) Ndryshoni fjalëkalimin rregullisht Sa më i rëndësishëm të jetë informacioni juaj, aq më shpesh ndryshoni fjalëkalimin. Sapo ta ndryshoni atë mos e përdorni më atë fjalëkalim.

II. Kujdes nga e-mail-et mashtruese Jeni të lutur të mos ju përgjigjeni email- eve mashtruese të cilët vijnë nga kontakte të panjohura dhe kërkojnë informacion për të dhënat tuaja personale, si kartë krediti, numra llogarie etj. Gjithashtu duhet të tregoni kujdes në hapjen e link-eve të ndryshme në internet. Disa përkufizime: • Spoof: email që duket sikur vjen nga një burim legjitim por në fakt nuk është i tillë. Shembuj: mund të përfshijnë PayPal ose Apple, duke ju thëne që keni një faturë në pritje. • Phishing: një email që mundohet t'ju bëjë të hapni një faqe të caktuar dhe të fusni të dhënat tuaja për shërbime të mëtejshme, kryesisht duke ju kërkuar juve të shkarkoni një material. • Spear Phishing: një kombinim i të dyjave më lart, pra email që duket sikur vjen nga një person juaji i njohur dhe përmban një link që ju drejton në një faqe të caktuar në internet. • Spam: Spam-et janë të bezdisshëm, por nuk karakterizohen nga qëllime të dëmshme. Mund të përmbajnë buletine legjitime tek të cilat ju jeni abonuar ose email-e që vijnë nga kompani të ndryshme, që në një mënyrë të caktuar kanë siguruar adresën tuaj të emailit. Nuk është shumë e vështirë për të dalluar një email të rremë. Duhet të jeni të vetëdijshëm për çfarë të shikoni. Disa mënyra janë: • A jeni duke e pritur atë email që ju vjen? • A e njihni dërguesin? • A e njihni adrësen e emailit? • A vjen me nënshkrimin (signature) e pritur? • A është adresa e emailit pjesë e emrit që shfaqet? • A është emaili duke ju kërkuar të shkoni në një faqe të caktuar që më pas ju kërkon të bëni sign in? Është shumë e zakonshme për emailet phishing të maskojnë qëllimet duke: • Ngarkuar fallso një PDF që përmban një link drejt një faqeje të infektuar; • Kërkuar pagesa, dërgon fatura, ose çështje që kanë lidhje me llogaritë. Gjërat që duhen kontrolluar: • Adresa e dërguesit: Emri që shfaqet mund të vendoset shumë lehtë si një emer që ju e njihni por adresa e emailit në vetvete është totalisht tjetër për tjetër. • Adresa e linkut: Shpesh herë linqet e faqeve të ndryshme janë të vendosura në imazhe dhe nuk është gjithmonë e qartë se ku ju dërgojnë. Mbani mous-in sipër linkut për të parë çfarë është përpara se ta klikoni. Nëse domain i adresës nuk përkon me domain-in e emailit ose i një shërbimi të njohur te File Sharing si psh.: dropbox.com, atëherë me shumë mundësi është një email i remë. Një tjetër gjë për tu patur kujdes është rasti kur një llogari emaili legjitim i një personi apo kompanie që ju njihni, mund të jetë hakuar dhe ju dërgon ju emaile mashtruese. Për tu siguruar nga kjo pjesë, bëni një kontroll të mesazhit që permban emaili, ose në rastin më dyshues kontrollojeni me dikë tjetër këtë situatë.

III. Mbroni pajisjet tuaja Si të mbroni privatësinë në pajisjen tuaj a) Përdorni kod kalimi. Kur të vendosni kod kalimi, përdorni të njejta masa sigurie që do të përdornit në çdo pajisje tjetër. Kurrë mos e tregoni kodin që vendosni te persona të tjerë. Mos ripërdorni të njëjtin kod që keni përdorur në pajisje të tjera. Bëhuni selektiv me aplikacionet që përdorni. Një aplikacion mund të duket i mirë në pamje të pare, por mund të ketë shumë të panjohura mbrapa. Mund të jetë shumë e veshtirë të dallohet sa privat dhe i sigurtë mund të jetë. Për këtë është më mirë të bëhen instalime nga burime të sigurta siç janë I-tunes, Play Store ose Amazon dhe të shihen mire të dhënat para se të shkarkohen nga këto burime. Bëni shumë kujdes me aplikacionet financiare, ku më të mirët e këtyre aplikacioneve nuk duhet t'ju kërkojnë vazhdimisht të fusni informcaionet e llogarisë në mënyrë që ta aksesoni atë. b) Mos klikoni në linqe të dyshimta Shikoni me kujdes URL, kryesisht kur ato ju kërkojnë të fusni informacion personal. Shumica e bankave p.sh kanë një faqe ku ju sqarohet se çfarë ata kërkojnë. Bëni sqarimet tuaja përpara se të fusni të dhënat. c) Aktivizoni fshirjen në distancë Nëse në një rast të caktuar telefoni juaj humbet, ju duhet të jeni në gjendje të fshini të dhënat e rëndësishme që keni, në distancë. Kjo

është relativisht e lehtë për t'u bërë pothuajse në të gjitha pajisjet. Një Iphone p.sh thjesht ju kërkon ju të aktivizoni Find My Phone dhe te logoheni në llogarinë iCloud që keni. d) Mbani Software të përditësuar Përditesimet e software bëjnë që ju të keni zgjidhjet e fundit për çdo problematikë. Por është mirë që të mos ta bëni menjëherë përditësimin, në mënyrë që të keni një feedback se si është ecuria e këtij përditësimi. e) Mos u lidhni me rrjetet e hapura te WiFi (open WiFi) përderisa telefonat sillen tashmë si mini-pc, shmangni sa të mundeni rrjetet e hapura WiFi, sepse ato mund të transmetojnë informacionet e kartës së kreditit dhe fjalekalimet pa qenë ju në dijeni të kësaj gjëje. f) Mbani shënim kodin IMEI Çdo telefon ka një numër serial prej 15 shifrash që quhet IMEI (INTERNATIONAL MOBILE EQUIPMENT IDENTITY) që mund të vijë në ndihmë në rast se telefoni juaj ka humbur ose është vjedhur. Mund ta gjeni nga ana e mbrapme e telefonit ose te settings. Mirë është ta shkruani diku, sepse përshpejton procesin e gjetjes së telefonit. g) Bëni Back-up të telefonit rregullisht Ky proces ndihmon të keni akses të rregullt te të gjitha të dhënat dhe materialet që ka telefoni si p.sh foto, muzik, aplikacione etj. Kjo është sigurisht shumë e rëndësishme në rast se telefoni juaj humbet, vidhet, por gjithashtu mund të vijë në ndihmë në rast se humbet të dhënat gjatë një përditësimit të softit. Sigurohuni që të bëni Back Up të paktën një herë në ditë, ose merrni parasysh të përdorni sinkronizimin në iCloud. h) Ruani të dhënat e kartës Sim Nëse vendosni të shisni telefonin, ka disa gjëra që duhet të bëni përpara se ta shisni atë. Ndër gjërat kryesore që duhet të bëni është të hiqni kartën Sim dhe kartë SD të cilat kanë të dyja të dhëna të rëndësishme. Bëjeni këtë edhe kur e çoni për riparim telefonin tuaj, veçanërisht kur nuk e njihni personin që bën riparimin.

IV. Përdorimi i kujdesshëm i rrjeteve sociale Menaxhoni privatësinë në rrjetet sociale duke zgjedhur se cilët mund të shohin profilin tuaj. Kontrolloni postimet që ju bëni. Mos publikoni foto të fëmijëve tuaj të cilat japin informacion mbi vendndodhjen e tyre. Përzgjidhni me kujdes personat që zgjidhni të bëni miq dhe bllokoni hyrjet e padëshiruara. Disa mënyra si të jeni të sigurtë në rrjetet sociale: • Përdorimi i një fjalëkalimi të vështirë për t'u gjetur. Sa më i gjatë të jetë fjalëkalimi, aq më i sigurtë është. • Përdorni fjalëkalime të ndryshme për çdo rrjet social që përdorni. • Krijoni pyetjet tuaja të sigurisë. Ky opsion është i disponueshëm për shumicën e rrjeteve sociale. • Nëse keni aplikacion të rrjeteve sociale në telefon, sigurohuni që pajisja juaj të jetë e mbrojtur me fjalëkalim. • Tregohuni selektiv me kërkesat e miqësisë. Nëse nuk e njihni personin mos e pranoni atë. Mund të jetë një llogari e rreme. • Klikoni linqet me kujdes. Llogaritë e rrjeteve sociale hakohen rregullisht. Kujdesuni për gjuhën ose përmbajtjen që nuk tingullon si diçka që miku juaj mund ta postonte. • Kujdesuni me ato çka ndani. Mos ndani informacion personal të tipit, adresë shtëpie, informacione financiare, numër telefoni, etj. Sa më shumë të postoni aq më e lehtë është që identiteti juaj të vidhet. • Familjarizohuni me politikat e sigurisë së rrjeteve sociale që përdorni dhe rregullojini ato sipas mënyrës tuaj, që të kontrolloni kush i shikon postimet tuaja. • Mbroni kompjuterin tuaj duke instaluar një software antivirusi. Gjithashtu sigurohuni që aplikacioni i lundrimit në internet, sistemi i operimit dhe aplikacionet e ndryshme të jenë të përditësuar. • Kujtohuni të dilni nga llogaria juaj kur keni mbaruar punë.

V. Kujdes nga telefonatat mashtruese Ju lutemi, mos telefononi numra ndërkombëtarë të cilët nuk i njihni, sepse këta numra mund të rezultojnë me tarifa tepër të larta. Mashtruesit që gjenerojnë këto thirrje të humbura synojnë që ju të merrni mbrapsht këto numra shumë të kushtueshëm ndërkombëtarë.