UDHËZUES RRETH INCIDENTEVE MË TË ZAKONSHME TË SIGURISË

Përtë mbrojturklientët e sajdhe në zbatimtë Rregullores Nr.37 datë 29.10.2015 “MbiMasatTeknikedheOrganizativePërtë GarantuarSigurinë dheIntegritetin e RrjeteveDhe/OseShërbimeveTë KomunikimeveElektronike”, shoqëriaACENET shpk, publikonkëtë udhëzuespërpërdoruesit “Rrethincidenteve më të zakonshmetë sigurisë, veprimevedhe/osemjeteveqë duhenndjekurpërtë parandaluarndodhjen e këtyreincidentevedheveprimeveqë duhenndjekur pas ndodhjes së incidentevetë sigurisë” ACENET shpk kujdesetpërju! Me qëllimmbrojtjentuajngaaktivitete me natyrë mashtruese në fushën e komunikimeveelektronike, ACENET shpk dëshiront’ju japë disakëshillatë thjeshta.

I. Krijonifjalëkalimtë fortë që një fjalëkalimtë jetë sa më isigurtë duhetqë të përmbajë minimalisht 8 (tetë) karaktere, ndërtë cilatnumra, gërmatë mëdhadhetë voglasidhesimbole. Nukështë e këshillueshmeqë të përdornitë njëjtinfjalëkalim kudo dhe ta ndani me të tjerët. Mënyrat e duhurapërvendosjen e fjalëkalimeve a) Vendosnifjalëkalimsa më të gjatë Hakeratpërdorinmënyratë shumtapërtë provuartë futen në llogaritë tuaja. Një ngateknikatështë në bazë të një programikompjuterikqë bënkombinimin e shkronjave, numravedhesimboleve. Sa më igjatë të jetë fjalëkalimiaq më igjatë do jetë kyprocesdheaq më ivështirë përtupërfunduar me sukses. b) Bëjenifjalëkalimintuajnjë frazë pakuptimFjalëkalimet e gjata jane të mirë, fjalëkalimet e gjataqë përfshijnë fjalë të rastitdhefraza janë akoma më të mirë. Mos përdornikaraktereqë janë sekuencial në tastierë. c) Përdorninumra, simboledheshkronjatë mëdhadhetë voglaBëninjë përzierjetë rastittë shkronjave me numradhesimbole. P.sh.: Ju mund t ë zëvendësonishkronjën O me numrin 0, oseshkronjën a me simbolin @. Nësefjalëkalimijuajështë një frazë, përpiqunitë kapitalizoniçdoshkronjë të parë të çdofjaleqë përbëjnë frazën. d) Shmangnipërdorimin e informacionit personal Nëse ka informacionpërjuqë është lehtësishtigjetshëmsipshditëlindje, adresë, qytetlindje, shkollë, emrateafërmishosekafshë shtëpiakeetjmundohunimostipërfshini në fjalëkalim. Nësejukërkohettë plotësoninjë pyetjesigurie, zgjidhninjë, përgjigja e së cilësnukështë e dukshme në rrjetetsociale. e) Mos ripërdornifjalëkalime Kur hakeratrealizojnë hakerimetë mëdha p.sh me serverat e emaile-ve, lista e emailevetë hakeruargjenerohen online. Nësejupërdornikëtë llogari me të njëjtinfjalëkalim, atëherë informacionijuajështë lehtësishtiarritshëm. Përdornifjalëkalimeunikepërçdollogari. f) Fillonitë përdorninjë menaxhuesfjalëkalimeshMenaxhuesit e fjalëkalimeve janë shërbimeqë gjenerojnë dheruajnë automatikishtfjalëkalimetë vështirë. Këtofjalëkalimembahen në një lokacionqëndrordhetë enkriptuarqë jumund ta aksesoni me një fjalëkalim Master (mos e humbisnikëtë fjalëkalim). Shumë shërbime janë të lira përt'upërdorurdhevijnë me karakteristikaopsionale, të tilla sisinkronizimiifjalëkalimevetë rejanëpërshumë pajisjedheauditimiisjelljes së fjalëkalimittuajpërtë siguruarqë nuk po përdornitë njëjtin në shumë vende. g) Mbajinifjalëkalimetsa më të fshehtë Mos iajepnifjalëkalimetasnjë personitjetër. Mos e shkruanifjalëkalimin në pajisjentuajnësejeni në rrezen e shikimitnganjë person tjetër. Mos e shkruanifjalëkalimintuaj në letratqë ngjisni në kompjuter. Nëseiruanifjalëkalimettuaja në një material në kompjuter, emërtonimaterialin me një fjalë që nuk ka lidhje me objektin e materialitqë është mbajtjashënim e fjalëkalimeve. h) Ndryshonifjalëkaliminrregullisht Sa më irëndësishëmtë jetë informacionijuaj, aq më shpeshndryshonifjalëkalimin. Sapotandryshoniatë mos e përdorni më atë fjalëkalim.

II. Kujdesnga e-mail-et mashtrueseJeni të lutur të mosjupërgjigjeni email- evemashtruese të cilëtvijnë ngakontakte të panjohuradhekërkojnë informacionpër të dhënattuaja personale, si kartë krediti, numrallogarieetj. Gjithashtuduhet të tregonikujdes në hapjen e link-eve të ndryshme në internet. Disapërkufizime: • Spoof: email që duketsikurvjennganjë burimlegjitim por në faktnukështë i tillë. Shembuj: mund të përfshijnë PayPal ose Apple, dukejuthëneqë keninjë faturë në pritje. • Phishing: një email që mundohet t’jubëjë të hapninjë faqe të caktuardhe të fusni të dhënattuajapërshërbime të mëtejshme, kryesishtdukejukërkuarjuve të shkarkoninjë material. • SpearPhishing: një kombinim i të dyjave më lart, pra email që duketsikurvjennganjë personjuaji i njohurdhepërmbannjë link që judrejton në një faqe të caktuar në internet. • Spam: Spam-et janë të bezdisshëm, por nukkarakterizohenngaqëllime të dëmshme. Mund të përmbajnë buletinelegjitime tek të cilatjujeniabonuar ose email-e që vijnë ngakompani të ndryshme, që në një mënyrë të caktuarkanë siguruaradresëntuaj të emailit. Nukështë shumë e vështirë për të dalluarnjë email të rremë. Duhet të jeni të vetëdijshëmpërçfarë të shikoni. Disamënyrajanë: • A jeniduke e prituratë email që juvjen? • A e njihnidërguesin? • A e njihniadrësen e emailit? • A vjen me nënshkrimin (signature) e pritur? • A është adresa e emailitpjesë e emritqë shfaqet? • A është emailidukejukërkuar të shkoni në një faqe të caktuarqë më pasjukërkon të bënisign in? Është shumë e zakonshmepëremailetphishing të maskojnë qëllimetduke: • Ngarkuarfallsonjë PDF që përmbannjë link drejtnjë faqeje të infektuar; • Kërkuarpagesa, dërgonfatura, ose çështjeqë kanë lidhje me llogaritë. Gjëratqë duhenkontrolluar: • Adresa e dërguesit: Emriqë shfaqetmund të vendosetshumë lehtë si një emerqë ju e njihni por adresa e emailit në vetveteështë totalishttjetërpërtjetër. • Adresa e linkut: Shpeshherë linqet e faqeve të ndryshmejanë të vendosura në imazhedhenukështë gjithmonë e qartë se kujudërgojnë. Mbanimous-in sipërlinkutpër të parë çfarë është përpara se taklikoni. Nëse domain i adresësnukpërkon me domain-in e emailit ose i një shërbimi të njohur te File Sharing si psh.: dropbox.com, atëherë me shumë mundësiështë një email i remë. Një tjetërgjë për tu paturkujdesështë rastikurnjë llogariemaililegjitim i një personi apo kompanieqë junjihni, mund të jetë hakuardhejudërgonjuemailemashtruese. Për tu siguruarngakjopjesë, bëninjë kontroll të mesazhitqë permbanemaili, ose në rastin më dyshueskontrollojeni me dikë tjetërkëtë situatë.

III. Mbronipajisjettuaja Si të mbroniprivatësinë në pajisjentuaj a) Përdornikodkalimi. Kur të vendosnikodkalimi, përdorni të njejtamasasigurieqë do të përdornit në çdopajisjetjetër. Kurrë mos e tregonikodinqë vendosni te persona të tjerë. Mosripërdorni të njëjtinkodqë kenipërdorur në pajisje të tjera. Bëhuniselektiv me aplikacionetqë përdorni. Një aplikacionmund të duket i mirë në pamje të pare, por mund të ketë shumë të panjohurambrapa. Mund të jetë shumë e veshtirë të dallohet sa privatdhe i sigurtë mund të jetë. Përkëtë është më mirë të bëheninstalimengaburime të sigurta siç janë I-tunes, Play Store ose Amazon dhe të shihen mire të dhënat para se të shkarkohenngakëtoburime. Bënishumë kujdes me aplikacionetfinanciare, ku më të mirët e këtyreaplikacionevenukduhet t’jukërkojnë vazhdimisht të fusniinformcaionet e llogarisë në mënyrë që taaksesoniatë. b) Mosklikoni në linqe të dyshimtaShikoni me kujdes URL, kryesishtkuratojukërkojnë të fusniinformacion personal. Shumica e bankave p.sh kanë një faqekujusqarohet se çfarë atakërkojnë. Bënisqarimettuajapërpara se të fusni të dhënat. c) Aktivizonifshirjen në distancë Nëse në një rast të caktuar telefoni juajhumbet, juduhet të jeni në gjendje të fshini të dhënat e rëndësishmeqë keni, në distancë. Kjoështë relativisht e lehtë për t’u bërë pothuajse në të gjithapajisjet. Një Iphone p.sh thjeshtjukërkonju të aktivizoniFind My Phone dhe te logoheni në llogarinë iCloudqë keni. d) Mbani Software të përditësuarPërditesimet e software bëjnë që ju të kenizgjidhjet e funditpërçdoproblematikë. Por është mirë që të mostabënimenjëherë përditësimin, në mënyrë që të keninjë feedback se si është ecuria e këtijpërditësimi. e) Mos u lidhni me rrjetet e hapura te WiFi (open WiFi) përderisatelefonatsillentashmë si mini-pc, shmangni sa të mundenirrjetet e hapuraWiFi, sepseatomund të transmetojnë informacionet e kartës së kredititdhefjalekalimetpaqenë ju në dijeni të kësajgjëje. f) Mbanishënimkodin IMEI Çdotelefon ka një numër serial prej 15 shifrashqë quhet IMEI (INTERNATIONAL MOBILE EQUIPMENT IDENTITY) që mund të vijë në ndihmë në rast se telefoni juaj ka humbur ose është vjedhur. Mundtagjeninga ana e mbrapme e telefonit ose te settings. Mirë është tashkruanidiku, sepsepërshpejtonprocesin e gjetjes së telefonit. g) Bëni Back-up të telefonitrregullishtKyprocesndihmon të keniakses të rregullt te të gjitha të dhënatdhematerialetqë ka telefoni si p.sh foto, muzik, aplikacioneetj. Kjoështë sigurishtshumë e rëndësishme në rast se telefoni juajhumbet, vidhet, por gjithashtumund të vijë në ndihmë në rast se humbet të dhënatgjatë një përditësimit të softit. Sigurohuniqë të bëni Back Up të paktënnjë herë në ditë, ose merrniparasysh të përdornisinkronizimin në iCloud. h) Ruani të dhënat e kartësSimNësevendosni të shisnitelefonin, ka disagjëraqë duhet të bënipërpara se tashisniatë. Ndërgjëratkryesoreqë duhet të bëniështë të hiqnikartënSimdhekartë SD të cilatkanë të dyja të dhëna të rëndësishme. Bëjenikëtë edhekur e çonipërriparimtelefonintuaj, veçanërishtkurnuk e njihnipersoninqë bënriparimin.

IV. Përdorimi i kujdesshëm i rrjeteve sociale Menaxhoniprivatësinë në rrjetet sociale dukezgjedhur se cilëtmund të shohinprofilintuaj. Kontrollonipostimetqë jubëni. Mospublikoni foto të fëmijëvetuaj të cilatjapininformacionmbivendndodhjen e tyre. Përzgjidhni me kujdespersonatqë zgjidhni të bënimiqdhebllokonihyrjet e padëshiruara. Disamënyra 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. • Përdornifjalëkalime të ndryshmepërçdorrjet social që përdorni. • Krijonipyetjettuaja të sigurisë. Kyopsionështë i disponueshëmpërshumicën e rrjeteve sociale. • Nësekeniaplikacion të rrjeteve sociale në telefon, sigurohuniqë pajisjajuaj të jetë e mbrojtur me fjalëkalim. • Tregohuniselektiv me kërkesat e miqësisë. Nësenuk e njihnipersoninmos e pranoniatë. Mund të jetë një llogari e rreme. • Klikonilinqet me kujdes. Llogaritë e rrjeteve sociale hakohenrregullisht. Kujdesunipërgjuhën ose përmbajtjenqë nuktingullon si diçkaqë mikujuajmundtapostonte. • Kujdesuni me atoçkandani. Mosndaniinformacion personal të tipit, adresë shtëpie, informacionefinanciare, numër telefoni, etj. Sa më shumë të postoniaq më e lehtë është që identitetijuaj të vidhet. • Familjarizohuni me politikat e sigurisë së rrjeteve sociale që përdornidherregullojiniatosipasmënyrëstuaj, që të kontrollonikush i shikonpostimettuaja. • Mbronikompjuterintuajdukeinstaluarnjë software antivirusi. Gjithashtusigurohuniqë aplikacioni i lundrimit në internet, sistemi i operimitdheaplikacionet e ndryshme të jenë të përditësuar. • Kujtohuni të dilningallogariajuajkurkenimbaruarpunë.

V. KujdesngatelefonatatmashtrueseJulutemi, mostelefononinumrandërkombëtarë të cilëtnuk i njihni, sepsekëtanumramund të rezultojnë me tarifatepër të larta. Mashtruesitqë gjenerojnë këtothirrje të humburasynojnë që ju të merrnimbrapshtkëtonumrashumë të kushtueshëmndërkombëtarë.