Udhezues per incidentet e sigurise ne sherbimet e telekomunikacionit, masat per parandalimin dhe veprimet ne rast se ndodhin

1. Kategorite me te zakonshme te kompromentimit te sigurise dhe integritetit te sherbimeve te telekomunikacionit
   - Kompromentim I informacioneve dhe aseteve
   - Akses I paautorizuar
   - Kode software Keqdashese (Malicious) te marra ne forma te ndryshme nga komunikimet online
   - Trafik email I demshem (malware)
   - Nderhyrje apo tentative per nderhyrje ne rrjeta kompjuterike
   - Scanime te paautorizuara, Probes
   - Phishing
   - Dhunim rregullash te komunikimit online, dhunim I etikes
   - Nxjerrje dhe shperndarje e paautorizuar te dhenave dhe informacionit personal
   - Nderprerje e plote apo degradim I sherbimit per me shume se 1 ore
   - Mosrespektim I perseritur I termave te sherbimit (shpejtesia e internetit, volume I trafikut, etj)
   - Faturim jo I sakte apo tentative per faturim jo te sakte
   - Faqe interneti apo domaine te hapura per te cilat eshte bere publikisht e njohur se duhet te mbyllen
   - Probleme me aksesin e brendshem kompjuterik Wireless apo Wired ne ambjentin tuaj te punes.

2. Cfare duhet te keni parasysh kur perdorni sherbimet e internetit

2.1 Mirembani pajisjet kompjuterike qe keni ne perdorim. Perditesojini ne menyre sa me te rregullt. Perdorni produkte te licensuara, te tregtuara ne menyre te rregullt, jo te piratuara, ndiqni rekomandimet e prodhuesve origjinale te produkteve.

2.2 Perdorni firewall dhe software mbrojtjes antivirus, antispam, antispyware, apo software të tjera për mbrojtjen e lundrimit në rrjet.
Nje software I tille mund te shkarkohet falas

http://www.forticlient.com/#download

2.3 Perdorni dhe mirembani fjalëkalime te sigurta për të mbrojtur lidhjen tuaj wireless në shtëpi, apo per cdo aplikacion qe suporton perdorimin e kredencialeve.Munfohuni te caktoni politikat tuaja te perdorimit te kredencialeve per aplikacionet online.

2.4 Mbroni të dhënat tuaja personale

Përpara se të vendosni të dhënat tuaja, shikoni për shenja të sigurisë që një Web faqe mund të ketë; Web https ("s", e siguruar) dhe një dryn të mbyllur ( ). Asnjëherë mos jepni të dhënat tuaja në përgjigje të një e-maili, apo sms-je.

2.5 Mendoni përpara se të klikoni

Mendoni përpara se të bashkëngjitni skedarë a foto, apo të klikoni mbi një link në një e-mail; në qoftë se ju nuk i njihni dërguesit, ata mund të jenë të rremë. Jini të kujdesshëm kur klikoni link-e të ndryshme në internet.

2.6 Mbroni veten nga emailat qe merrni

Shikoni me kujdes emailat qe merrni, duke vrojtuar mesazhet alarmuese, mesazhet gabim dhe/ose me gabime gramatikore, mesazhet me kërkesa për të dhënat tuaja personale, si numra llogarie, kartë krediti etj. Kini parasysh se cdo kerkese qe u vjen dhe ju kerkon te dhena personale apo te dhena konfidenciale apo pergjigje pyetjsh te caktuara, ne nje forme ose ne nje tjeter ju rrezikon.

2.7 Përdorni ne menyre te sigurte rrjetet sociale

Mosha minimale për t'u regjistruar në një rrjet social, siç është "Facebook", apo "Messenger", është mbi 13 vjeç. Shikoni për mundësinë "Rregullo privatësinë" në Facebook dhe Twitter, për të menaxhuar se cilët mund të shohin profilin tuaj. Kontrolloni se si njerëzit mund t'ju kërkojnë në rrjet dhe të bëjnë komente. Gjithashtu, mësoni se si mund të bllokoni hyrjet e padëshiruara. Mos postoni çdo gjë që ju mendoni. Përzgjidhni me kujdes pranimin e miqve të rinj, si dhe rishikoni periodikisht se çfarë miqtë publikojnë në lidhje me ju.

2.8 Femijet tuaj mos I lini te perdorin internetin ne ambjente te vecuara, po ashtu dhe telefonat celulare.

3. Testoni para se te beni nje hap te dyshimte

Ne rast se keni dyshime mbi nje skedar qe doni te hapni, mund te perdorni faqe te sigurta ku e testoni ate skedar paraprakisht, si me poshte:

https://www.microsoft.com/en-us/wdsi/filesubmission

https://fortiguard.com/faq/onlinescanner

3. Informohuni sa me shume mbi rreziqet e mundshme te perdorimi te internetit dhe praktikat me te mira te mbrojtjes, si psh https://www.fortinet.com/blog/industry-trends/10-steps-for-protecting-yourself-from-ransomware.html
4. Tregohuni proactive duke raportuar incidente e duka marre pjese ne shpendarjen e informacionit mbi risqet potenciale te faqeve te internetit apo aplikacioneve te ndryshme, si psh

   http://url.fortinet.net/rate/submit.php
   http://metal.fortiguard.com/tests/

   dhe ne faqen zyrtare qeveritare

www.cesk.gov.al

5. Mos lini hapur kompjuterin tuaj ne menyre te panevojshme. Perdoreni kur keni nevoje dhe kur mbaroni pune fikeni ose kalojeni ne Sleep mode. Vecanerisht mos lini hapur faqe internet qe mund te perdoren nga hackerat per gjenerim bitcoin-e e monedha te tjera elektronike duke perdorur ne background resurset e pajiajeve tuaja kompjuterike.

7. Per cdo problem me aksesin ne sherbimet e rrjetit, privatesine tuaj, mbrojtjen e femijeve apo problematika te tjera te sigurise dhe sherbimit, kontaktoni ne:

cphdesk@commprog.com

ose ne numrin e telefonit 042413901.

Communication Progress

www.commprog.com

www.commprog.al

www.tekreja.al