Obiectivele

Suntem in secolul XXI, secolul tehnologiilor. Tehnologiile au ajuns sa fie o parte foarte importanta in viata fiecaruia. Dar pe linga toate plusurile acestia, deasemenea are citeva minusuri, printe care se pot numara si vulnerabilitatile de care se pot folosi alti oameni pentru a va lua datele voastre, pentru a le folosi in scopuri rele, astfel ca sa minimalizam riscul acestor actiuni contra voi astazi va vom povesti despre cum sa va protejati. Aceasta protectie poate mai fi numita si Cybersecurity.

Reguli

Acum va vom prezenta 10 reguli importante ce va vor ajuta sa fiti protejati in mediul online. Initial va vom prezenta slideul cu regula si o imagina relativa regulii, astfel daca stiti despre ce este vorba v-as ruga sa ridicati mina si sa incercati sa povestiti la colegii vostri despre ce stiti, daca vom avea ceva de adaugat o vom face.

1 HTTPS

Poate citiva din voi au putut observa niste litere http sau https insoite de caracterele \\ si : in fata linkului. Aceasta regula consta in litera S de la sfirsit. Litera “S” vine de la Secure ce inseamna ca site-ul este securizat, astfel v-as recomanda sa accesati doar siteuri cu “S” si incercati sa evitati cele care au doar HTTP in fata linkului.

2 wifi public

Incearca sa eviti utilizarea reţelelor wi-fi publice pentru operaţiuni bancare, comerţ on-line sau afaceri personale, deoarece wi-fi-ul public poate fi folosit pentru a lua indirect datele voastre personale, ca parolele voastre de la conturi, care poate duce la furtul acestor conturi.

3 comunitati online

Daca ti-ai facut vre-un cont in vreo comunitate online, ca site-urile de socializare precum facebook, instagram, odnoklasnii, etc fii cit se poate de discret. Nu avea incredere in persoanele necunoscut.

4 oferta

Fii întotdeauna sceptic când primeşti o ofertă ce sună foarte tentant. Aceasta oferta poate fi folosita pentru a face phishing, despre care va voi povesti in scurt timp.

5 Nu rula programe a căror origine nu poate fi verificată, deoarece acestia pot fi virusi care pot ajunge sa provoace daune majore la calcuatorul tau.

6. Evită pe cât posibil memorarea informației personale de către browser.

Aceste date salvate pot fi obtinute foarte usor de catre alte persoane, astfel va pot lua conturile.

7.Foloseşte o soluţie antivirus actualizată zilnic.

Posibil a-ti vazut notificarile ce va propun sa actualizati antivirusul Dvs., dar cred ca putini dintre voi au dat click sa faceti update, gindindu-va ca nu are nicio importanta si aici ati gresit amarnic, deoarce actualizarea antivirusuli este foarte importanta. La fel ca organismul ce se lupta cu vre-un virus il memoreaza, pentru ca data viitoare cind acest virus ataca din nou acelasi organism, el este deja gata si

stie ce actiuni poate intrerpinde pentru a-l elimina, antivirusul se lupta cu virusii,doar ca el nu stie ce actiuni pot fi interprinse impotriva virusilor doar ce au atacat deja calcuator vostru, ci stie virusii ce au atacat un calculator cu acelasi antivirus, astfel se creaza o baza de date folosind toate calcuatoarele, ce face posibila eliminarea virusilor un proces foarte usor,dar daca il veti actualiza calculatorul vostru va fi extrem de vulnerabil la virusi care apar in fiecare zi, deci cind veti vedea notificarea de actualizare a antivirusului nu va leneviti, acualizatil.

8.Evită pe cât posibil căutările riscante.

Cautarile riscante pot sa va duca pe siteurile nesigure.

9.Parolele sunt secrete și îți aparțin.

Niciodata nu da parola ta nimanui, pentru ca se pot folosi de aceasta in scopuri cu consecinte negative pentru voi.

10.Nu intra pe site-uri dubioase.

Deoarece exista siteuri facute special pentru a incerca sa va pacaleasca, astfel puteti descarca virusi.

Hartuirea in mediul online (1)

Hărţuirea pe internet a atins deja cote alarmante, iar victimele fenomenului nu au foarte multe arme la dispoziţie pentru a se proteja de aşa ceva. Principalele arme de atac folosite pe internet pentru a agresa victimele se leagă de înfăţişare şi felul în care se îmbracă (67%). Alte motive frecvente pentru care tinerii sunt hărţuiţi sunt hobby-urile şi preocupările de zi cu zi (30%), situaţia materială a familiei din care provin (13%), rezultatele de la şcoală (12%) şi orientarea sexuală (8%). Două treimi dintre cei hărţuiţi nu au povestit nimănui despre incident, tinerii invocând motive precum teama, lipsa de încredere că ar putea schimba ceva sau faptul că nu au crezut că e necesar să implice şi alte persoane, deşi au fost afectaţi în mod direct de agresiune. Cele mai populare reţele de socializare unde are loc fenomenul de cyberbullying sunt Facebook, Messenger şi, la mare distanţă, Instagram, iar mijloacele de propagare a fenomenului cel mai des folosite sunt mesajele de ameninţare şi cele negative primite în canalul privat, urmate de comentarii negative la fotografii şi furt de identitate.Principalele arme de atac folosite pe internet pentru a agresa victimele se leagă de înfăţişare şi felul în care se îmbracă (67%). Alte motive frecvente pentru care tinerii sunt hărţuiţi sunt hobby-urile şi preocupările de zi cu zi (30%), situaţia materială a familiei din care provin (13%), rezultatele de la şcoală (12%) şi orientarea sexuală (8%). Două treimi dintre cei hărţuiţi nu au povestit nimănui despre incident, tinerii invocând motive precum teama, lipsa de încredere că ar putea schimba ceva sau faptul că nu au crezut că e necesar să implice şi alte persoane, deşi au fost afectaţi în mod direct de agresiune. Cele mai populare reţele de socializare unde are loc fenomenul de cyberbullying sunt Facebook, Messenger şi, la mare distanţă, Instagram, iar mijloacele de propagare a fenomenului cel mai des folosite sunt mesajele de ameninţare şi cele negative primite în canalul privat, urmate de comentarii negative la fotografii şi furt de identitate. Părinţii, rudele, profesorii trebuie să conştientizeze existenţa fenomenului şi să ştie să identifice comportamentul schimbat al victimei şi să intervină când identifică efectele cyberbullingului în comportamentul acesteia. Orice semn care indică modificări ale stării psihologice cum ar fi depresia, anxietatea socială, izolarea, stima de sine scazută, reacţii negative şi stres în privinţa utilizării dispozitivelor trebuiesc chestionate şi verificate. Este util ca victima să reuşească să impună limite. De la blocarea şi raportarea abuzatorului pe reţelele de socializare, la schimbarea parolelor sau a numărului de telefon, până la intervenţiile directe

către abuzator, efectuate într-o manieră cât mai asertivă, fără a-i oferi agresorului satisfacţia pe care o caută. Cel care hărţuieşte va fi mulţumit dacă provoacă victimei suferinţă, de aceea este recomandată evitarea afişării oricărei urme care lasă de înţeles că aceasta a fost afectată.

Reputatia Online (2)

Fa o cautare pe numele tau

Ti-ai cautat pana acum numele pe Google? Pentru ca, daca nu, e cazul sa o faci. Verifica atat rezultatele din Search cat si cele din Google Images. Chiar daca ai constiinta curata, este posibil ca problemele legate de reputatia ta sa provina dintr-o coincidenta de nume.

3. Fii prezent activ pe retelele de socializare

Cand vorbim de reputatie online, vorbim invariabil si despre retelele de socializare. Dupa cum bine stii, acestea au devenit un canal de informare important, iar oamenii sunt foarte deschisi sa isi exprime parerile personale despre orice, fie ele pozitive, fie negative (si stii bine ca vestile proaste circula mai repede).

Ei, in procesul de construire si intretinere a reputatiei tale online, este indicat sa iti creezi profiluri pe principalele platforme de social si sa le populezi cu informatii relevante despre tine.

Orienteaza-te spre Facebook, LinkedIn, Twitter, Google+ iar, daca ai timp, nu lasa deoparte nici Instagram, Pinterest sau YouTube. Ok, nu trebuie sa postezi zilnic pe acestea pentru a-ti intretine reputatia, insa nici sa te culci pe o ureche nu e bine.

Adauga continut nou macar o data pe saptamana (sau o data pe luna) si interactioneaza cu oamenii: raspunde-le la comentarii, distribuie continut valoros de pe alte pagini si fii pregatit sa gestionezi si comentariile negative (raspunde politicos si nu o lua personal, peste tot exista hateri).

4. Optimizeaza-ti prezenta pe aceste site-uri

Daca tot esti prezent pe site-uri si retele de socializare, incearca sa le umpli cu informatii reale/valoroase despre tine, optimizeaza URL-urile si repeta-ti numele (acolo unde poti)

5. Tine lucrurile private in privat

Ce se intampla in Las Vegas ramane in Las Vegas. Ce se intampla pe Google ramane acolo pentru totdeauna si se va intoarce impotriva ta fix atunci cand nu te astepti. Prin urmare, ai grija ce publici in online pentru ca, daca tu nu esti atent la propria reputatie, informatiile negative se vor imprastia ca gandul.

Exista cateva reguli privitoare la prezenta pe Google sau Facebook sau orice alt website: nu publica ce nu vrei sa vada mama ta, nu publica ceva ce nu vrei sa vada seful tau si nu publica orice iti trece prin cap. Totul trebuie privit prin prisma bunului simt, al unei conduite exemplare si trebuie citit si de trei ori inainte de a fi publicat. Pozele cu shot-uri de tequila, priviri incetosate de la bauturi alcoolice sau alte substante, pozele nud, la bustul gol sau in costum de baie nu au ce cauta pe Facebook sau pe Instagram. La fel sta treaba si cu statusurile cu opinii personale discriminatoare, injurioase sau care ar putea jigni alti oameni. Nu au ce cauta online.

Cum recunoastem calculatorul virusat

Calculatorul merge mai lent

Primești mesaje nesolicitate

Programele se pornesc nechemate

Windows-ul se oprește brusc

Protectia antivirus

Scopul antivirusului este de a va proteja de virusii ce va pot provoca daune, in unele cazuri ireparabile pentru calculator. Mai devreme v-am mai povestit despre antivirus.Antivirusii in majoritatea cazurilor costa o gramada de bani. Acest lucru poate fi evitat foarte usor cu ajutorul antivirusilor gratisi. Pe tabla puteti vedea o lista mica de antivirusi gratisi. De asemenea va voi informa despre site-ul virustotal.com care este un site cu scopul de a scana fisierile atasate daca au virusi. [aratam cum se foloseste]

Securitatea informației (3) se ocupă cu protejarea informației și sistemelor informatice, de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea lor. Aici se tratează securitatea informațiilor prin cele trei componente principale: confidențialitatea, integritatea și disponibilitatea. Confidențialitatea este asigurată prin criptarea informației. Integritatea se obține prin mecanisme și algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță. Securitatea informaţiei nu mai trebuie tratată doar din punct de vedere tehnic, ea trebuie inclusă în managementul companiei.
(4) Securitatea informaţiei poate fi pusă la încercare de viruşi, acces neautorizat, procesarea neadecvată de către angajaţii companiei (aşa-numitele erori umane), defecţiuni sau dezastre naturale ce au ca rezultat oprirea sau defectarea echipamentelor IT.
Toate acestea îşi pun amprenta asupra activităţii şi imaginii companiei. Iată de ce această problemă trebuie tratată foarte serios şi inclusă în managementul companiei.
Păstrarea datelor a devenit o problemă tot mai importantă atât datorită faptului că se manipulează un volum tot mai mare de date, dar şi modului de accesare al acestor informaţii care trebuie să fie rapid, eficient, optim din punct de vedere al raportului timp accesare/valoare informaţie.
Nu în ultimul rând, datele stocate trebuie să fie arhivate astfel încât să se asigure o securitate adecvată în ceea ce priveşte persoanele care au acces la ele, dar şi din punct de vedere al concordanţei cu legislaţia privind securitatea şi protecţia informaţiilor. Securitatea aplicatiilor- aplicatiile sunt de 2 tipuri. Locale si cele web, care sunt puse pe internet si au drept scop auditoriul de peste tot cu ajutorul internetului. Astfel aici apar mai multi factori ce pot avea niste efecte negative asupra aplicatiei web. De exemplu vulnerabilitatea de la asa numitii hacker sau crackeri care au drept scopuri atacurile acestor aplicatii. Nicio aplicatie nu este sigura 100%, iar securitatea aplicatiilor consta in minimalizarea maxim posibila a acestor vulnerabilitati. Cei ce ataca aplicatia pot sa colecteze informatie, ca de exemplu informatia personala a utilizatorilor, si deterioarearea informatiilor si a aplicatiei in general.

Spam-ul (5)

Spam-ul reprezinta acele mesaje electronice (email-uri) nesolicitate, care apar in casuta de email fara ca posesorul contului sa autorizeze in prealabil aceasta actiune. In majoritatea cazurilor caracterul principal al email-urilor nesolicitate este comercial, de publicitate pentru produse sau servicii de regula indoielnice, sau de promovare a unor website-uri, actiuni sau ideologii. Alte caracteristici ale spamului

includ:

nu permite posesorului adresei de email sa se dezaboneze si sa nu mai primeasca alte email-uri de la sursa respectiva (privarea de dreptul la optiune);

adresele de email carora li se va expedia mesaje spam sunt colectate fie prin intermediul unor formulare de inregistrare false care se prezinta ca apartinad de diverse site-uri populare, fie acestea sunt procurate contra cost de la organizatii sau persoane (hackari) care le obtin tot prin metode ilegale;

este expediat automat de catre un program software;

sursele de spam sunt greu de identificat, programele care trimit spam sunt plasate ilegal pe calculatoare aleatoare, iar acest proces se face folosind software de tip malware.

In plus, spam-ul ocupa spatiu de stocare din contul de email, efectueaza trafic de date in reteaua de internet care poate incetini trimiterea sau receptionarea de email-uri reale si inrautateste experienta utilizatorului pentru ca acesta este nevoit sa verifice si sa sorteze email-urile bune fata de cele spam, pentru ca apoi sa le stearga; iar acest lucru necesita atentia utilizatorului si un timp alocat pentru curatarea de spam a casutei de email.

Cum sa eviti receptionarea de email-uri SPAM?

Principalul mod de a evita in totalitate email-urile SPAM este sa nu te inregistrezi pe site-uri necunoscute sau nesigure, sa iti ascunzi adresa de email din profilurile publice de pe retelele sociale sau de pe orice site pe care esti inregistrat, sa protejezi calculatorul de virusi atat prin utilizarea precauta a internetului dar si prin folosirea unui antivirus performant , sa nu trimiti email-uri la adrese nesigure si, desigur, sa folosesti doar platforme web sigure de email precum GMail,Yahoo si altele, care au incorporate strategii de identificare si blocare a spam-ului. Un alt aspect ce trebuie luat in considerare atunci cand vine vorba de evitarea spam-ului este si numele adresei de email, o adresa de mail scurta sau prea simpla poate primi SPAM pur si simplu la nimereala, pe baza unor algoritmi ce folosesc sau compun diverse cuvinte populare (cum ar fi prenumele, numele de familie, ani, etc.) pentru a forma adrese de email catre care sa trimita mesaje nesolicitate.

Practic vorbind, este foarte putin probabil ca un cont de email sa nu primeasca niciodata mesaje nesolicitate. Tocmai de aceea trebuie luate masuri si pentru evitarea eventualelor email-uri SPAM iar acest lucru consta in modul in care utilizatorul interactioneaza cu mesajele de email necunoscute.

Acum pe tabla puteti observa un exemplu de spam.

Spyware-ul (6) este un tip se program foarte periculos. El se instalează pe calculator pentru a supraveghea si înregistra orice activitate(tastele apăsate, siturile vizitate, programele folosite si furtul de identitate). Aceste programe se pot instala pe calculator in multe feluri, de obicei se ascund in jocurile gratuite, screensaver-uri sau cursoare animate.

Apar noi toolbar-uri, link-uri, site-uri favorite pe care nu le-ati adăugat in browser. Pagina home, cursorul sau browserul setate anterior s-au schimbat Tastați o adresa de site si sunteți direcționat către un alt

site Apar pop-upuri, chiar daca nu sunteți conectat la internet Calculatorul începe sa funcționeze mai încet; nu doar spyware-urile provoacă încetinirea rulării programelor, dar pot fi una din cauze.

VIDEO DESPRE SPYWARE

COMUNICAREA PE REȚELELE DE SOCIALIZARE

Comunicarea pe rețelele de socializare nu este în totdeauna sigură. Comunicând cu un om străin pe internet cu care niciodată nu v-ați întîlnit în viața reală, n-ai siguranța că cel cu care discuți este cu adevarat cel care se pretinde. Nu poți identifica identitatea acestuia. Nu poti verifica cat este de sincer cu tine celalalt atunci cand aveti o comunicare virtuala. Poti fi tradat, in cazul in care ai prea multa incredere in prietenul cu care ai o comunicare virtuala. În cazul în care ai decis să comunici cu o persoană necunoscută pe internet trebuie să fii foarte atent și anume: să nu divulgi informații personale, să nu trimiți poze cu tine, cu casa ta sau poze din care această persoană poate sustrage informații personale cum ar fi adresa ta aproximativă, lucrurile prețioase din casa sau imagini din care poate fi înțeleasă starea financiară a ta sau a părinților și deasemenea nu-l informa despre plecările de acasă pentru că mulți infractori își pot face planul să îți fure lucruri din casa știind exact cînd nimeni nu va fi acasă. De aceea trebuie să fim atenți cu cine vorbim și să fim foarte precauți când postăm ceva pe rețelele de socializare pentru ca pot avea un conținut cu informații folositoare pentru infractori.

ADRESELE DE E-MAIL PENTRU PHISHING

Prezentarea imaginei exemplu din powerpoint

VIDEO DESPRE PHISING

SECURITATEA ONLINE PENTRU TELEFOANELE MOBILE (7)

Telefonul la fel ca si calculatorul poate fi virusat accesînd diferite site-uri dubioase si descărcînd aplicații neautorizate.

Cîteva reguli de urmat:

Setează o parolă pe telefon şi un PIN pe cartela SIM. Folosirea parolelor va opri hoţii de la încercarea de a accesa telefonul sau să folosească neautorizat cartela SIM în alt telefon, pentru a efectua apeluri. Toate telefoanele au setări de securitate, aşadar familiarizează-te cu ele şi setează-le;

Configurează dispozitivului tău la blocare automată. Dacă telefonul nu a fost utilizat timp de câteva minute, ar trebui să se blocheze automat şi să necesite o parolă sau cod PIN pentru a avea din nou acces la aplicaţii;

Opreşte serviciul GPS când nu îl foloseşti. Pe de o parte, GPS-ul poate te ajută să afli unde trebuie să mergi. Pe de altă parte, acesta poate fi folosit şi de alţii pentru a vedea unde te afli;

Nu salva parolele sau PIN-uri în contactele de persoane inventate pe telefonul tău dacă nu le criptezi într-un mod corespunzător. Este tentant să salvăm parolele în telefon ca și contact, pentru cazul în care le uităm. Acest lucru va ajuta, însă, persoanele rău intenţionate să îţi acceseze conturile, dacă ai pierdut telefonul;

Dacă telefonul tău permite rularea aplicaţiilor descărcate de pe Internet, verifica si setează in momentul instalării la ce date personale permiţi accesul. Permite cu maximă prudenţă accesul la locație, la agenda de contacte şi la mesaje;

Când decizi să reciclezi telefonul tău, asigură-te în primul rând că ai şters toate informaţiile personale. Cele mai multe telefoane au o opţiune de a reveni la setările de la fabrică. Nu uita să scoţi sau să ştergi orice card de memorie introdus.

Cum evităm virusarea telefonului?

Instalează programe de securitate de la dezvoltatorii cu renume;

Fii atent/ă la adresele paginilor web utilizate în mod obişnuit şi asigură-te că nu eşti redirecţionat către alte site-uri;

Nu accesa link-urile pe care le primeşti nesolicitat sau neaşteptat. Chiar şi atunci când acestea par a fi de la prieteni;

Nu accepta solicitările nesolicitate pentru a instala unele programe. Dacă nu știi ce este sau la ce se referă acel program, evită-l. Infractorii, uneori, încearcă să păcălească utilizatorii astfel ca aceştia să descarce software maliţios;

Nu deschide mesaje multimedia (MMS) sau anexe la e-mailuri, nu accesa link-urile din e-mailuri decât atunci când le aștepţi şi ele vin de la o sursă de încredere. Acestea ar putea conţine programe de virusare sau va duce la un site maliţios;

În mod regulat verifică actualizările disponibile pentru sistemul de operare al telefonului. Instalează-le de îndată, cu singura condiţie ca sursa să fie oficială. Aceste actualizări conţin adesea îmbunătăţiri de siguranţă;

Evită conectarea la sursele tip Wi-Fi necunoscute, deoarece acestea pot facilita transferul de viruşi. Conectează-te la reţeaua unui furnizor cunoscut

și care necesită o parolă, deci este criptată.Activează opțiunile care solicită întotdeauna aprobare înaintea conectării la o rețea. De asemenea, funcţia Wi-Fi trebuie oprită în momentul în care nu este folosită;

Opreşte funcția de Bluetooth sau date mobile (Internet) când nu le foloseşti pentru a transfera date, evitând astfel comunicarea cu alte dispozitive. Bluetooth permite conectarea fără fir la dispozitive şi transfer de informaţii la distanţe scurte. În plus, oprirea acestora va prelungi durata bateriei telefonului;

Descărca programe și aplicații doar din magazinele oficiale. Sursele necunoscute pot oferi conținut nelicențiat cu programe de virusare.

Cum detectam un telefon virusat?

Factura serviciilor telefonice a crescut considerabil, brusc fără nici un motiv clar;

În mapa ”expediate”, telefonul conţine email-uri şi mesaje pe care nu le-ai trimis;

Interfaţa cu utilizatorul s-a schimbat, fără ca să faci tu schimbarea;

Contactează furnizorul de servicii pentru instrucţiuni cu privire la modul de a identifica şi elimina programul maliţios

Exemplu imagine din PowerPoint

Prezentarea site-ului nostru de phishing

Cu totii iubim partea teoretica, dar practiva e mai interesanta si mai importanta, deci am venit la voi cu un exemplu live de phishing.

Surse

(1) https://adevarul.ro/tech/internet/hartuirea-online-cyberbullying-ul-cele-mai-mari-probleme-internet-adolescenti-afectati-1_5a1bf67f5ab6550cb895be91/index.html
(2) https://www.gomag.ro/blog/tu-stii-care-este-reputatia-ta-online/
(3) https://ro.wikipedia.org/wiki/Securitatea_informa%C8%9Biei
(4) http://www.datasecurity.ro/?p=6
(5) http://www.adibarbu.ro/2015/07/ce-este-spam-ul-si-cum-se-poate-evita.html
(6) http://www.cumseface.eu/viewtopic.php?t=340
(7) https://siguronline.md/rom/copii/informatii-si-sfaturi/sfaturi-de-utilizare-a-telefonului-mobil