1. Hartuirea online

Ce este hărțuirea online, numită în limbajul uzual **cyber bullying**? Este un termen lansat de Bill Belsey, specialist canadian în educație, care l-a definit astfel: *"Cyber bullying-ul implică utilizarea tehnologiilor informaționale și comunicaționale pentru a sprijini un comportament deliberat, repetat și ostil desfășurat de către un individ sau grup, care este destinat să aducă prejudicii altor persoane".*

Înainte de a apela la instrumentele legale, ar fi bine să distingem acele acțiuni și manifestări care cad sub incidența acestui fenomen, și anume:

- **bârfa:** emiterea în mediul online a unor declarații speculative ce denigrează o persoană sau instigă un grup de persoane în a adopta un comportament restrictiv;
- **hărțuirea:** luarea în batjocură constant și deliberat o persoană, prin postarea de mesaje publice, poze ce pot afecta integritatea psihică a individului;
- **urmărirea online:** hărțuirea intimidantă cu scopul de a aduce conflictul și în viața reală. De exemplu, de a solicita întrevederi în viața reală prin a amenința cu răfuială fizică;
- **trolling:** provocarea unor persoane să acționeze agresiv, prin insultarea implicită;
- **comentarii:** postarea de răspunsuri negative, denigrante la adresa unor persoane, la adresa unor fotografii, clipuri video sau mesaje lansate de o anumită persoană;
- **profiluri false:** crearea unor profiluri false create de agresorii pe internet, ce împrumută identitatea altor persoane pentru a facilita comunicarea cu victimele lor; sub protecția anonimatului, agresorii își amenință victimele sau, aleatoriu, folosesc identitatea victimei în raport cu alte persoane;
- **sexting:** distribuirea de materiale pornografice minorilor, utilizând mijloacele electronice de comunicație.

Aceste acțiuni constituie niște abuzuri în adresa persoanei. În primul rând, este bine să știm ce instrumente tehnice putem folosi pentru a opri un asemenea comportament din partea terților. Dacă hărțuirea se realizează pe o rețea de socializare (*facebook, odnoklassniki, instagram, twitter* etc.), trebuie să cunoașteți că aceste platforme au opțiuni de a raporta comentariile abuzive, hărțuirea sau așa numitul spam. A nu se ignora această opțiune ce vi se pune la dispoziție, ori ea chiar poate duce la închiderea contului de pe care sunteți molestat.

Soluții tehnice ar fi mai multe, de a vă seta contul în așa fel încât să fie mai puțin accesibil persoanelor cu care nu sunteți “prieteni”. Acestea nu sunt măsuri de ordin legal, dar cel puțin vă protejează și nu vă expune atât de mult riscului de a fi hărțuit în mediul online. În cazul în care hărțuirea se realizează în afara rețelelor de socializare, de exemplu prin comentarii defăimătoare pe anumite site-uri sau bloguri, primul pas ar fi să notificați proprietarul site-ului prin a solicita ștergerea informației care vă defăimează.

Atunci când mijloacele tehnice nu v-au permis să soluționați problema apărută, iar hărțuirea continuă, în mod sigur, ați putea apela la organele competente: poliție, procuratură, instanța de judecată într-un final. Pentru a ne apăra drepturile ar exista două căi:

- fie prin depunerea unei plângeri penale, contravenționale;
- fie prin înaintarea unei acțiuni civile în instanța de judecată.

2. Reputatia online

Exista o gramada de interpretari gresite in ceea ce priveste gestionarea reputatiei online. Unii afirma ca aceasta se limiteaza la monitorizarea platformelor de social, altii presupun ca e ceva legat de relatii publice in timp ce altii habar n-au cu ce se mananca acest concept.
Adevarul e undeva la mijloc. Gandeste-te la gestionarea reputatiei tale online ca la o asigurare: nu te gandesti la ea cand nu ai nevoie insa esti recunoscator ca o ai atunci cand dai de necaz.
Conceptul de management a reputatiei online este relativ nou, motiv pentru care multe persoane (printre care si antreprenori) nu acorda importanta – inca – propriei imagini publice de care sunt urmariti pe web. Practic, managementul reputatiei online consta in actiuni de monitorizare, diminuare sau eliminare a materialelor negative pe care oamenii le gasesc despre tine online.
In articolul de astazi vei citi despre cum sa afli ce spune internetul despre tine dar si 4 ponturi eficiente care iti permit sa influentezi pozitiv propria imagine online.

1. 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.

Este deja celebru cazul co-fondatorului **BrandYourself.com**, Pete Kistler. Prin 2008, acesta a descoperit adevaratul motiv pentru care companiile la care a aplicat nu il cheama nici macar la un interviu. Se pare ca pe Google mai existau o multime de alti Pete Kistler, printre care se numara si un individ suspectat de trafic de droguri. Si aici observam impactul reputatiei potentialilor angajati asupra angajatorilor.

Dar inchipuie-ti ce s-ar intampla daca un potential investitor iti cauta numele pe Google si descopera un tip cel putin dubios, pe care il confunda cu tine? Cate sanse crezi ca mai ai sa obtii fondurile de care ai nevoie?

Pentru a preveni astfel de situatii, iti recomand sa setezi **alerte Google** pentru numele tau, adresa, numele business-ului/brandului tau si sa limitezi notificarile la una pe zi, pentru a le primi direct pe email.

2. Cumpara-ti un domeniu cu numele tau

O modalitate de a te asigura ca rezultatele legate de numele tau sunt relevante si contribuie la reputatia ta online este sa iti cumperi **un domeniu cu numele tau**, unde sa publici continut specific despre tine si afacerea ta. Ok, aceasta activitate presupune ceva efort insa te asigur ca iti va influenta puternic si pozitiv reputatia online.

Ce poti sa publici aici? Scrie informatii despre tine si despre activitatea ta, scrie pe tematici nisate (de exemplu, daca vinzi cadouri handmade poti scrie despre acestea si, bonus, sa trimiti link-uri spre site-ul tau) sau poti sa publici un CV.

De asemenea, aici poti publica link-uri spre articole interesante si comentariile pe care le ai de adaugat asupra subiectelor discutate.

Un site sau un blog te ajuta si daca exista informatii negative legate de numele tau. Prin publicarea unui continut interesat si informatii valoroase poti sa “ingropi” rezultatele negative si sa le trimiti pe pozitii mai joase, mai putin vizibile.

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).

De exemplu, pe profilul de LinkedIn, ai posibilitatea sa iti personalizezi adresa URL. In loc sa apara ceva de genul: https://www.linkedin.com/in/dcosmin?authType=name&authToken=_b13&trk=hp-feed-liker-name&csrfToken=ajax%3A1865808058782602747 poti personaliza URL-ul astfel: https://www.linkedin.com/in/dcosmin/ro.

Si daca tot vorbeam anterior de blog sau site personal, iti recomand sa afisezi link-uri spre profilurile tale pe retelele de socializare. Aceasta actiune iti va intari prezenta in online.

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.

3. Cum recunoastem un calculator virusat?

1. *“Computerul vorbeste cu mine“* - Apar pe ecran tot felul de ferestre “pop-up” si mesaje publicitare, precizand ca PC-ul este infectat si ca are nevoie de protectie. Acesta este un exemplu tipic de infectare. Este vorba fie de un program spion (“spyware”) in computer sau de o infectare cu un antivirus fals (numit si “rogueware“).

2. *“Computerul meu functioneaza extrem de incet“* - Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. In cazul in care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, facandu-l sa functioneze mai greu decat de obicei.
3. *“Am aplicatii care nu pornesc”* - De cate ori ati incercat sa porniti o aplicatie din meniul start sau de pe desktop si nimic nu se intampla? Uneori se poate deschide chiar un alt program. Ca si in cazul anterior, poate fi vorba de orice alta problema, insa este cel putin un simptom care va spune ca ceva nu este in regula.

4. *“Nu ma pot conecta la Internet sau acesta ruleaza extrem de incet“* -Pierderea accesului la Internet este un alt semn al infectarii, desi poate fi cauzat si de probleme legate de furnizorul de Internet sau router. Pe de alta parte, este posibil sa aveti o conexiune la Internet care functioneaza mult mai greu decat de obicei. Daca ati fost infectat, malware-ul se poate conecta la o anumita adresa de Internet sau poate deschide anumite conexiuni separate, limitand astfel viteza de accesare a Internetului sau chiar facand imposibila folosirea acestuia.

5. *“Cand ma conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate”* - Acesta este cu siguranta un alt semn al infectarii cu malware. Multe fisiere virale sunt concepute special pentru redirectarea traficului de Internet catre anumite website-uri, fara consimtamantul utilizatorului, sau chiar sa imite anumite website-uri, creand impresia unui site legitim.

6. *“Unde au disparut fisierele mele?“* - Sa speram ca nimeni nu va pune aceasta intrebare, desi anumite atacuri sunt concepute special pentru criptarea sau stergerea anumitor fisiere si chiar mutarea documentelor dintr-un loc in altul. Daca va gasiti in aceasta situatie, este cazul sa incepeti sa va faceti griji.

7. *“Antivirusul meu a disparut, firewall-ul este dezactivat”* - O alta actiune tipica a amenintarilor de pe Internet este dezactivarea sistemelor de securitate (antivirus, firewall, etc) instalate pe calculator. Daca un singur program s-ar opri, poate ca ar fi vorba de o eroare de software, dar daca toate componentele de securitate s-ar dezactiva, aveti cu siguranta computerul infectat.

8. *“Computerul meu vorbeste in alta limba”* - Daca limba anumitor aplicatii se schimba, ecranul apare inversat, “insecte” ciudate incep sa “manance” ecranul, este posibil sa aveti un sistem infectat.

9. *“Imi lipsesc fisiere necesare pentru a rula jocuri, programe etc”* - Din nou, acest lucru ar putea fi un semn de infectare, desi este posibil sa fie vorba de o instalare incompleta sau incorecta a acelor programe.

10. *“Computerul meu, practic, a innebunit”* - In cazul in care computerul dumneavoastra incepe sa actioneze singur sau sa trimita email-uri fara sa stiti, daca aplicatii sau ferestre de Internet se deschid singure, in mod sporadic, sistemul ar putea fi compromis de malware.

In toate scenariile prezentate mai sus sau daca aveti cea mai mica banuiala ca aveti computerul infectat, Panda Security va recomanda sa cautati aplicatii de securitate alternative la cele pe care le aveti instalate (daca aveti!).

Nu este nevoie sa le dezinstalati pe cele curente, puteti folosi programe antivirus online, gratuite, cum ar fi Panda ActiveScan.

4. Protectie antivirus

BENEFICII

Cu ajutorul unei protectii antivirus, echipamentele si informatiile sunt protejate, astfel incat acestea nu sunt afectate de virusii informatici.

SOLUTII

Exista multe solutii antivirus pe piata. Important in cazul unei astfel de solutii este nivelul de protectie pe care il ofera. Sunt mai multe metode de a identifica virusi, astfel in alegerea solutiei antivirus este important sa tinem cont de acest lucru. Un alt aspect important este frecventa cu care solutia antivirus isi face actualizarile privind semnaturile virusilor. Practic, exista o baza de date pentru fiecare produs antivirus care contine semnaturile virusilor informatici cunoscuti, iar aceasta se actualizeaza constant.

Un alt aspect important este pe ce echipamente folosim solutii antivirus. Este bine ca protectia antivirus sa fie pe mai multe nivele. Daca avem un echipament de retea prin care este filtrata antivirus toata informatia care vine din internet dar statiile de lucru nu au o solutie proprie antivirus este posibil ca un utilizator sa foloseasca un stick usb si sa infecteze toata reteaua.

Pentru echipamentele de retea care filtreaza traficul internet in si dinspre internet sunt solutiile oferite de Fortinet si Juniper. Pentru statiile de lucru si servere exista solutiile antivirus oferite de Bitdefender, Kaspersky, Microsoft Forefront.

RECOMANDAREA NOASTRA

Solutiile de protectie antivirus au nenumarate beneficii, raportate la pierderile pe care le poate suferi compania in cazul unui infectari cu virusi, de aceea nu trebuie neglijate. Pentru a beneficia de protectie maxima a sistemelor de operare, va recomandam sa apelati la sfatul unui specialist, care va poate alege cea mai buna solutie.

5. Securitatea informatiei

Confidențialitatea este asigurată prin criptarea informației.
În criptografie, **criptarea** este procesul de mascare a informației pentru a o face ilizibilă fără cunoștințe speciale. În prezent, este utilizată în protejarea unei mari varietăți de sisteme, precum e-comerț, rețele de telefonie mobilă și ATM-urile băncilor.

Criptarea poate fi folosită pentru a asigura discreția și/sau intimitatea, dar și alte tehnici sunt necesare pentru a face comunicațiile sigure. În mod particular verificarea integrității și autenticității unui mesaj, de exemplu un cod de autentificare a mesajelor (CAM) sau semnături digitale. Alt motiv este protecția împotriva analizei traficului.

Criptarea sau ascunderea codului de software este folosit în protecția copierii de software împotriva ingineriei inverse, analiza aplicațiilor neautorizată, crack-uri și pirateria software.

Integritatea se obține prin mecanisme și algoritmi de dispersie. În esenta, integritatea datelor presupune definirea regulilor care restrâng valorile valide pentru o coloana a unui tabel. Restrictiile de integritate sunt definite pentru tabele si prin urmare toate vederile si sinonimele tabelelor sunt supuse restrictiilor de integritate. Daca o instructiune DML încearca sa efectueze o actiune care violeaza o restrictie de integritate, este generata o eroare si tranzactia este derulata înapoi.

Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță.

6. Cum sa fac o parola sigura?

#1. Utilizează o parolă care are cel puțin 12 caractere, tipurile acestora fiind diferite.

#2. Combină corect caracterele tale, utilizând propoziții create de tine.

Spre exemplu, alegi propoziția „Mama mea s-a născut în Edineț pe 15 octombrie 1965”. O scurtare potrivită ar fi mmsniep15o65. Acum, începi parola cu majusculă și schimbi, spre exemplu, litera „o” cu semnul exclamării „!”, acesta fiind caracterul tău special. În rezultat, primești Mmsniep15!65. Lista de caractere speciale o găsești **aici**, însă fii sigur că pagina web pe care te înregistrezi le acceptă pe toate.

#3. Nu utiliza sportul tău preferat, numele actorului, filmului sau trupei tale preferate.
Cuvinte ca „football” și „hockey” au ajuns în clasamentul celor mai rele parole, învață lecția dată. Nu utiliza nici numele iubitului tău, celui mai bun prieten sau a cuiva din familia ta.

#4. Nu alege cuvinte extrem de simple și evidente.
Cuvântul „casa” pentru parola ta este o alegere oribilă. Nici substituirile evidente cu caractere speciale nu sunt întocmai potrivite, cum ar fi „c@s@”.

#5. Evită utilizarea anului tău de naștere.
Cel puțin, nu îl utiliza complet, alege doar o cifră sau două. Vezi cum a avut loc prescurtarea anului în pasul #1.

#6. Adaugă un prefix la parolă, constituit din 3 – 4 caractere.
Evită să utilizezi prefixul serviciului electronic la care tu scrii parola. Spre exemplu, nu utiliza „yahoo” dacă faci parola pentru mailul tău pe yahoo.com. Nu utiliza nici numele iubitului tău sau numele tău de familie. La urma urmei, utilizează prefixele utilizate în procesul de derivare al cuvintelor, cum ar fi „ante”, „inter”, „post”.

#7. Adaugă și un sufix constituit din 3 – 4 caractere.
Însă, dacă ai utilizat un tip de prefixe, evită să utilizezi același tip de sufixe. Poți adăuga primele 4 litere ale numelui tău de utilizator, ale personajului tău preferat dintr-o carte istorică sau orice altceva ce știi sigur că nu va fi public. Spre exemplu, dacă personajul tău preferat este Ștefan cel Mare, atunci alegi „stef” drept sufixul parolei tale.

Astfel, dacă luăm parola din pasul #1 și o combinăm cu restul pașilor, obținem „***anteMmsniep15!65stef***”, parolă care pare a fi indestructibilă.

7. Securitatea in retelele Wi-Fi

Protocolul RADIUS este folosit în mediul rețelelor pentru autentificare, autorizare şi evidență. El poate rula pe multe tipuri de dispozitive (routere, servere, switch-uri, modemuri, concentratoare VPN, etc). RADIUS lucrează prin crearea şi criptarea unui tunel între dispozitivul de rețea şi un server RADIUS. Remote Authentication Dial-In User Service y RADIUS facilitează administrarea centralizată a utilizatorilor, ceea ce este important pentru mai multe dintre aceste aplicații. Mulți dintre furnizorii de servicii internet au zeci de mii, sute de mii sau chiar milioane de utilizatori. Utilizatori care se adaugă şi elimină continuu pe parcursul zilei, şi informația de autentificarea a utilizatorului se modifică constant. Administrarea centralizată a utilizatorilor în această setare este o cerință operațională.

Metode de criptare - WPA y WPA-PSK (WPA Preshared Key sau WPA-Personal) este o metodă mult mai sigură decât WEP. WPA2 este metoda cea mai sigură de criptare, fiind o variantă îmbunătățită a metodei WPA. y Şi aceste criptări (WPA şi WPA2) pot fi sparte dacă parola conține puține caractere sau este un cuvânt aflat în dicționar. Pentru a face imposibilă spargerea acestei criptări folosiți parole lungi, generate aleator.

8. Spam-urile

1. Ce este SPAM-ul? Cum vad utilizatorii un mesaj de tip SPAM si cum vede un specialist fenomenul?

Definitia spune, pe scurt, ca **spamul este orice mesaj nesolicitat**. Din nefericire insa (pt cei din industria antispam), utilizatorii uneori fac abuz de ceea ce ofera produsele antispam pentru a bloca nu neaparat "mesajele nesolicitate", ci mesajele "nedorite".

Utilizatorul vede spamurile proprii, mai multe sau mai putine,mai variate sau mai putin variate, de cele mai multe ori doar cate o mostra din fiecare tip. Specialistul le vede pe toate, vede valuri intregi de spam, din toate categoriile (meds, diploma etc.)pt ca de la sursa ele asa pleaca (in valuri = e-mailuri care seamana foarte mult, atat ca subiect cat si ca layout, dar care difera totusi pe alocuri, tocmai pentru a fi detectate mai greu de filtrele antispam).

2. Care sunt pericolele la care sunt expusi utilizatorii când deschid astfel de mesaje?

Ar fi doua foarte importante. Primul este reprezentat de **mesajele de tip phishing**. Acestea pot fi extrem dedaunatoare, pentru ca ele pretind a veni din partea unei institutii (uneori bancare, uneori nu) si de vreme ce mesajele de acest tip inca exista (si chiar creste numarul lor) inseamna ca sunt suficient de multe victime pentru ca afacerea sa aiba succes.

Cel de-al doilea pericol care exista este **infectarea calculatorului prin deschiderea unui link periculos** dintr-un spam, prin download-ul si rularea unui executabil, prin deschiderea unui eventual atasament infectat etc. Dupa infectarea calculatorului, pericolele pot sa capete forme variate in functie de tipul de malware cu care s-a infectat: virus, worm, troian,spyware, adware.

Cum se pot feri utilizatorii de mesajele spam?

Utilizatorii trebuie sa aiba **un produs de Securitate complet**, care sa contina si modulul Antispam. In lipsa lui, utilizatorul nu va fi niciodata protejat 100%. Ni se poate intampla si noua, celor care lucram in domeniul securitatii sa nu ne dam seama imediat atunci cand vedem un e-mail daca e spam/phishing sau nu. Pentru ca, de exemplu, atunci cand vedem un IP (de la care a fost trimis e-mailul) sau un URL, nu putem sti cu certitudine ce reputatie are fara sa facem cautari suplimentare.

9. Spyware & Keyloggers

Programele spion sau ***spyware*** sunt o categorie de software rău intenționat, atașate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de chat pornografic, etc.), care captează pe ascuns date de marketing (prin analiza site-urilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ș.a.m.d.) și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

Programele spion care nu extrag date de marketing, ci doar transmit reclame se numesc *adware*.

Există programe spion care modifică modul de comportare a unor motoare de căutare (Google, Yahoo, MSN, etc.), pentru a trimite utilizatorul contra voinței sale la site-uri (scumpe) care plătesc comisioane producătorului programului spion.

Unele programe spion abuzează de calculatorul utilizatorului pentru a face pe ascuns calcul distribuit (de exemplu operațiuni contabile pentru firme din India). Din motivul că procesorul lucrează și pentru altcineva, programele spion încetinesc calculatorul. Ele pot uneori să blocheze conexiunea la internet (ca efect neintenționat).

În general, chiar după ștergerea programelor gratuite care au instalat programul spion, acesta rămâne în continuare activ. Există și numeroase programe anti-spion, dar atenție: unele dintre ele sunt *false antispyware* - inducând utilizatorul în eroare deoarece ele însele conțin programe spion mascate.

Programele de tip spion nu sunt considerate viruși informatici, deoarece, în general, ele nu caută să infecteze programe (ci doar infectează calculatorul cu acordul mai mult sau mai puțin conștient al utilizatorului), și nici să atace calculatoarele altor persoane (de exemplu, prin răspândire automată prin e-mail). Ele sunt considerate doar amenințări la adresa sferei private a utilizatorilor. Unele programe antivirus nu detectează niciun fel de program spion, ci doar viruși, troieni, viermi, bombe logice, ș.a.m.d. Producătorii de programe spion au tot interesul ca produsele lor să nu fie considerate viruși, din moment ce a răspândi viruși este ilegal, având consecințe civile și penale; dacă toate antivirusurile ar începe să vâneze produsele lor, producătorii ar suferi pierderi economice însemnate.

Modul de pătrundere[modificare | modificare sursă]

În 99 % din cazuri programul spion este instalat de însuși utilizatorul calculatorului, în mod voit sau și nevoit, adică citind sau necitind licența programului conținând *spyware*, prin aceea că la instalare apasă pe butonul virtual „*Da, sunt de acord*”. Există și situri cu descărcare tip *drive-by*, care se folosesc de mecanisme de escamotare a securității programelor *browser* pentru a instala pachete de programe spion.

Pentru înlăturarea programelor spion sunt folosite programele *antispyware*. În anul 2005, veniturile producătorilor de soluții antispyware au depășit la nivel mondial 100 de milioane de dolari[6].

10. Comunicare pe retelele sociale

#1. Poza de profil/poze

Peste 75% din profilurile false aparțin unor fete, majoritatea având poză de profil sexy. Numărul pozelor pe Facebook este un indicator bun, mai ales varietatea lor. Persoanele care creează profiluri false de cele mai multe ori nu folosesc multe poze. Suficiente ca să umple un album și atât.

Astfel, dacă vedeți că pozele sunt cam din aceeași perioadă, nu diferă mult și sunt mai mult de la ședințe foto, atunci precis sunt luate din vreo revistă/pictorial. La fel, puteți vedea când acestea au fost încărcate, dacă pozele au fost încărcate în perioada când a fost creat profilul și de atunci nu au fost schimbări, atunci e un profil fals.

Profilurile care au avatare în loc de poze nu sunt neapărat profiluri false, mai mult anonime, uneori.

Puteți descărca poza și să o căutați pe Google, vedeți ce minuni vă apar.

#2. Elemente de familie și prieteni

Dacă o persoană nu are poze comune cu alți utilizatori, în care mai multe persoane sunt etichetate (și aici nu vorbesc de pozele de sărbători cu ouă, brazi și iepurași), inclusiv poze cu iubitul sau iubita, mama, colegii de clasă, colegii de lucru, sau animalele de companie, atunci cel mai probabil este un profil fals.

Oricât de securizat profil nu ar avea cineva, oricum lasă urme publice despre individualitatea sa.

#3. Paginile la care a dat „Like”

O persoană își poate ascunde pozele, poate fi secretoasă și să nu pună poze cu oameni dragi, însă la sigur își va etala preferințele în materie de like-uri.

Un profil adevărat în medie are peste vreo 30 like-uri la pagini din domenii variat diferite (uneori te-a rugat un prieten să dai like, alte ori din greșeală, sau a trebuit să dai like să citești vreun articol, și ele se adună).

Profilurile false au 3 – 5 like-uri, și dacă este un profil fals de promovare, atunci sunt like-urile la pagini care pot fi într-un fel grupate în jurul unei persoane, agenție, partid.

#4. Actualizările
Actualizările ce apar pe profile false sunt, de obicei, linkuri cu o anumită tematică (mai ales a ceea ce încearcă să promoveze), share-uri de la paginile administrate și mai puțin păreri și opinii proprii, însă dacă și sunt doar axate pe un subiect-latimotiv.

Profilurile false, de cele mai multe ori, nu sunt etichetate în locuri și evenimente. De asemenea, statut-urile și check-in-urile aproape lipsesc.

#5. Discuții
Conturile false, de obicei, nu intră în discuții, dacă nu le trebuie, și de cele mai multe ori nu vor răspunde la mesajele care le au, iar dacă vor răspunde, va fi mai mult laconic de genul: mulțumesc, da, merci, nu știu, vai ce drăguț.

În cazul conturilor false politice, aceștia vor comenta doar la paginile care scriu despre partidul lor sau vor intra în dezbateri la stările persoanelor publice, repetând aceeași idee.

Dacă vor fi persoane cu care își mai lasă mesaje pe pereți sau la stări, atunci și celălalt profil este fals.

#6. Prietenii și numărul de prieteni

O persoană cu mulți prieteni obține un număr mai mare de feedback, mai multe felicitări la ziua de naștere.

Profilurile false, chiar dacă au un număr mare de prieteni, publică un conținut mai puțin popular, astfel încât dacă o persoană are peste 1.500 prieteni și la ultimele 10 postări aproape că nici nu are feedback, atunci profilul e fals, iar actualizările sunt scrise de formă.

Dacă suspectați un profil că e fals și vedeți că o persoană îi comentează mai mult și în același stil, celălalt profil tot este fals.

#7. Informație din profil
De cele mai multe ori profilurile false sunt profile care nu folosesc setări se securitate și actualizările sunt publice. Informația despre unde au învățat sau unde s-au născut, fie e prea detaliată, ori lipsește.

În prieteni au persoane publice sau persoane influente de pe Facebook, pentru a putea eticheta acele persoane în spam.

Nu sunt „in a relationship” și cum menționam și la poze, nu au membri de familie listați (pentru asta ar trebui să creeze o familie falsă).

Când îi întrebați de ce ar trebui să-i adăugați, vă vor spune chestii generale, vor încerca inițial să flirteze, după asta nu vor mai răspunde la mesaje.

11. Adresele phishing

Ce înseamnă activitatea de phishing

De obicei, activitatea de phishing se face prin e-mailuri, anunțuri sau prin intermediul unor site-uri care arată la fel ca site-urile pe care le folosești deja. De exemplu, e posibil ca cineva care practică phishing să îți trimită un e-mail care arată ca și cum a fost trimis de banca ta, astfel încât să îi transmiți informații despre contul tău bancar.

E-mailurile sau site-urile de tip phishing pot să îți ceară:

- nume de utilizator și parole, inclusiv modificări de parolă;
- codul numeric personal;
- numărul contului bancar;
- codurile PIN (numere de identificare personală);
- numărul cardului de credit;
- numele dinainte de căsătorie al mamei tale;
- data nașterii.

Evită atacurile de phishing

Tratează cu atenție e-mailurile pe care le primești de la un site care îți solicită informații personale. Dacă primești astfel de e-mailuri:

1. nu da clic pe niciun link și nu transmite niciun fel de informații personale până când confirmi că e-mailul este real.
2. dacă expeditorul are o adresă Gmail, raportează abuzul din Gmail la Google.

Notă: Gmail nu îți va solicita niciodată prin e-mail informații personale precum parola.

Când primești un e-mail care pare suspect, iată câteva lucruri pe care e recomandat să le verifici:

- verifică dacă adresa de e-mail și numele expeditorului corespund;
- verifică dacă e-mailul este autentificat;
- plasează cursorul peste linkuri înainte de a da clic pe ele. Dacă adresa URL a linkului nu corespunde cu descrierea acestuia, e posibil să te direcționeze către un site de tip phishing.

- verifică antetele mesajelor pentru a te asigura că antetul „from” nu afișează un nume greșit.
  Important: în cazul în care crezi că adresa ta Gmail a fost piratată, recuperează-ți contul Gmail compromis înainte de a trimite sau de a deschide alte e-mailuri.

12. Cookie

Atunci când navighezi pe internet, întâlnești des termenul de *"cookie"*. Multe saituri web te informează în legătură cu utilizarea lor și îți cer permisiunea de a le folosi. Browserele web au multe setări pentru gestionarea cookie-urilor și există chiar și extensii de browser care pot să blocheze cookie-urile. Chiar dacă știi că aceste cookie-uri nu sunt niște prăjituri, poate nu știi ce sunt cu adevărat și care este rolul lor pe internet. De aceea, în acest articol, îți explicăm ce sunt cookie-urile, ce fac și cum funcționează, precum și ce tip de cookie-uri este cel mai des folosit pe internet. Hai să începem:

Ce sunt cookie-urile de pe internet?

Cookie-urile sunt fișiere care stochează informații despre tine, browser-ul tău web și comportamentul tău pe internet. Ele sunt fișiere foarte mici păstrate pe PC-ul sau dispozitivul tău, ce pot fi folosite de saiturile sau de aplicațiile web pentru a ajusta experiența ta online.

Ce fac cookie-urile?

Cookie-urile sunt transmise între un expeditor (de obicei un sait web sau o aplicație web) și un destinatar (dispozitivul tău). Un cookie este creat și interpretat de către expeditor, în timp ce destinatarul doar îl păstrează și îl trimite înapoi dacă expeditorul cere asta.

Atunci când navighezi pe internet, expeditorul este serverul care găzduiește un sait web și destinatarul este browser-ul web care vizitează acel sait. Scopul lor este de a identifica utilizatorul, de a verifica activitatea lui din trecut pe acel sait și de a oferi conținut specific bazându-se pe aceste date.

Când un utilizator vizitează un sait web pentru prima dată, serverul stochează un anumit cookie în browser-ul său. La toate vizitele succesive acestei prime vizite, serverul își va cere cookie-ul pentru a-l citi și a încărca o anumită configurație a saitului web care să fie cea mai potrivită pentru acel utilizator. Poți vedea cookie-urile ca pe o etichetă pe care serverele le aplică fiecărui utilizator, citindu-le apoi pentru a identifica utilizatorii.

Această identificare este extrem de utilă mai ales pe saituri web unde datele în timp real ale utilizatorului sunt critice. De exemplu, atunci când vizitezi un magazin online, nu ai putea cumpăra nimic fără ajutorul cookie-urilor. Magazinele nu ar putea să te identifice și să îți atribuie un coș de cumpărături fără acestea deoarece, de fiecare dată când încărci o nouă pagină, magazinul te-ar privi ca pe un nou utilizator și ar crea un nou coș.

Cum puteti opri cookie-urile?

Dezactivarea si refuzul de a primi cookie-uri pot face anumite site-uri impracticabile sau dificil de vizitat si folosit. De asemenea, refuzul de a accepta cookie-uri nu inseamna ca nu veti mai primi/vedea publicitate online.

Este posibila setarea din browser pentru ca aceste cookie-uri sa nu mai fie acceptate sau puteti seta browserul sa accepte cookie-uri de la un site anume. Dar, de exemplu, daca nu sunteti inregistat folosind cookie-urile, nu veti putea lasa comentarii.

Toate browserele moderne ofera posibilitatea de a schimba setarile cookie-urilor. Aceste setari se gasesc de regula in „optiuni” sau in meniul de „preferinte” al browserului dvs.
Pentru a intelege aceste setari, urmatoarele linkuri pot fi folositoare, altfel puteti folosi optiunea „ajutor” a browserului pentru mai multe detalii.