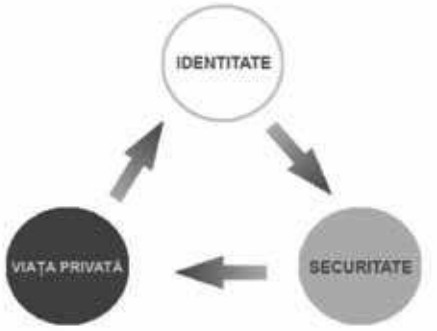
„De la crearea unui cont pe un anumit site am început să primesc nenumărate mail-uri din partea unor impostori care aveau o adresă similară cu cea de la care am primit contul. Am căzut în plasă fără să observ prezența unor mici gafe de genul consoane dublate sau lipsa unor vocale în link-ul trimis pe email. Am realizat acum că totul a fost un atac de phishing pentru a-mi sustrage datele." (Sebastian – 17 ani)

Identitatea digitală este o parte importantă a ***securității online***, fiind strâns corelată cu modul în care este respectată confidențialitatea datelelor personale. De fapt, scopul securității online este de a proteja informația privată împotriva accesului neautorizat, distrugerii sau alterării , iar păstrarea confidențialității reprezintă protecția atributelor, preferințelor și a datelor asociate cu o identitate împotriva dezvăluirii și răspândirii acestora în mediul online.[20]



Rețelele sociale (Facebook, Twitter, LinkedIn etc.), mai populare în rândul adolescenților și tinerilor decât printre adulți, au creat un spațiu nelimitat de proliferare a datelor personale pe Internet. Utilizatorii de Internet dispun în prezent de tehnologia necesară pentru a-și exprima, construi și administra propria identitate digitală, constituită din informațiile postate pe conturile personale sau ale terților de pe rețelele sociale, din contribuțiile de pe blog-uri, forumuri sau website-uri și din urmele lăsate prin simpla navigare pe Internet (log-uri, cookie-uri, phishing). Principala particularitate a mediului online este că o informație (text, imagine) postată la un moment dat poate fi regăsită și consultată de oricine chiar la câțiva ani după difuzare.

Astăzi, se vorbește din ce în ce mai des de **reputația online** a utilizatorului. Îngrijorarea este cauzată de faptul că numeroase informații personale sunt postate online, în mod special, pe rețele de socializare, creând în timp adevărate identități digitale. Interesul pentru reputația online ca expresie a identității digitale a utilizatorului de Internet a pornit de la numeroase situații în care informații confidențiale, uneori compromițătoare, au afectat viața profesională a unor tineri. Un caz celebru este cel al lui Connor Riley, 22 ani, tânără absolventă a Universități din Berkeley, acceptată pentru angajare de către compania Cisco[21]. La ieșirea din sediul companiei, Connor Riley a trimis următorul mesaj prietenilor pe Twitter: „*Cisco mi-a oferit un loc de muncă! Acum trebuie să pun în balanță utilitatea unui salariu gras și faptul că urăsc munca pe care trebuie să o fac*". Neglijența în administrarea contului de Twitter a făcut ca mesajele lui Connor Riley să fie publice și nu adresate doar prietenilor săi, astfel că recrutorii companiei Cisco l-au putut citi. Evident, locul de muncă nu mai era valabil pentru tânăra utilizatoare de Twitter.

Problema **confidențialității și securității pe Internet** nu privește doar informațiile personale pe care alegem să le publicăm online ci și informațiile obținute de către alte

20 Digital Identity, Phillip J. Windley, O'Reilly Media, 2008.

21 Bill Gillies, Conner Riley gives her version of events, www.grownupdigital.com/archive/index.php/2009/03/conner-riley-gives-her-version-of-events/ , 1 martie 2013.

persoane prin intermediul unor sisteme nu întotdeauna transparente. Într-adevăr, multe dintre activitățile desfășurate pe Internet, de la comerțul electronic până la participarea la grupuri jurnalistice, sunt caracterizate de colectarea de date personale ale utilizatorilor. Această colectare poate avea loc într-un mod explicit printr-o cerință dintr-un formular electronic, sau într-un mod secret prin intermediul log-urilor și cookie-urilor. În cazul colectării explicite, utilizatorului i se cere să completeze un formular cu datele personale, în schimbul unor servicii gratuite; această informație este apoi catalogată și utilizată deseori în scopuri comerciale. În acest caz, colectarea de date este reglementată prin legile în vigoare în diferite țări. Informațiile personale însă, sunt de obicei colectate fără știrea utilizatorului prin intermediul unor **log-uri, cookie**-uri și metodei numite **phishing**.

Log-uri (jurnale de sistem)

Log" este un fișier care asigură jurnalizarea tuturor activităților unui sistem informatic sau ale unei rețele. Scopul său principal este de a ajuta administratorul de rețea sau tehnicianul să identifice erorile din sistem sau rețea. O altă intrebuințare a acestor fișiere poate consta în spionarea utilizatorilor și obținerea datelor/ informațiilor acestora.

Cookie-uri

Un alt instrument folosit pentru detectarea urmelor lăsate de utilizator în sistem este cookie-ul. Acestea sunt fișiere care înregistrează obiceiurile online ale utilizatorului și pot avea mai multe utilizări.Spre exemplu, un administrator al unui site îi poate recunoaște pe cei care vizitează site-ul, controla frecvența vizitelor și apoi poate personaliza site-ul în funcție de gusturile utilizatorilor. În plus, cookie-urile sunt utilizate de către furnizori în vederea adaptării conținutului publicitar la fiecare utilizator în parte. O directivă a Uniunii Europene, numită E-Confidențialitate (Directiva 2009/136/CE), dispune modificarea legilor în vigoare în diferite țări și introducerea sistemului *opt-in*, adică obținerea consimțământului a priori (înainte de începerea colectării de date).

Phishing

Mai există și o a treia modalitate de obținere frauduloasă a datelor personale: phishing. Acest cuvânt este folosit pentru a descrie practica de vânare a informațiilor. Bazat pe un tip de fraudă electronică, acest sistem constă, de exemplu, în trimiterea de emailuri prin care utilizatorului i se cere să introducă date personale pentru a se putea bucura în continuare de anumite servicii.

Fișa educatorului privind reputația online (sfaturi Sigur.info)

Sfaturile de mai jos pot constitui elementele de bază în abordarea subiectului reputației online într-o dezbatere la clasă. Așa cum am arătat mai sus, reputația online se construiește în special în cadrul rețelelor de socializare.

Care sunt cele mai importante 5 sfaturi de securitate wireless?
La conexiunea în regim wireless trebuie avute în vedere următoarele reguli de securitate:
• evitarea conectării la Wi-Fi publice, întrucât există hackeri care clonează locaţii de tip free Wi-Fi şi accesează datele personale
• folosirea, de către firme, a conexiunii de tip VPN (Virtual Private Network), prin care datele transmise sunt criptate
• folosirea permanentă a firewall-ului, pentru a preveni eventuale intruziuni
• accesarea de site-uri şi servicii web care nu necesită date personale sau parole de acces personal

Ai încercat vreodată să-ți tastezi numele în fereastra Google și să apeși Caută? Oare informația pe care o găsești este pozitivă sau trimite către niște site-uri cu care n-ai vrea sa fi asociat? În ziua de azi, reputația ta online contează. Angajatorii, colegii și chiar prietenii nu s-ar da în lături de la căutarea online de informații privind persoana ta. Asigură-te că ceea ce găsesc ei nu-ți va cauza probleme.

Construiește-ți profilul cu grijă!

Fii foarte atent cu informația pe care o postezi pe un profil online. Ai aceeași grijă pe care ai avea-o atunci când scrii un cv, spre exemplu. Asigură-te că postările tale te reprezintă, dar în același timp ai grijă ca acestea să nu fie ofensatoare sau deranjante .

Calitatea contează mai mult decât cantitatea.

E frumos să ai cât mai mulți prieteni, dar nu trebuie să adaugi în lista ta chiar pe toată lumea. Fii selectiv în legătură cu persoanele pe care le adaugi ca prieteni. Ține minte că atunci când adaugi pe cineva ca prieten acesta poate vedea toate informațiile despre tine.

O poză face cât o mie de cuvinte.

Deși e distractiv să postăm poze de la petreceri sau poze amuzante, e important să știm că odată postată o fotografie pe Internet ea e aproape imposibil de înlăturat. Poate fi preluată de oricine și folosită fără voia noastră. De aceea e indicat să avem grijă ce poze postăm și în ce ipostaze suntem atunci când suntem fotografiați.

Așa că, înainte să postezi orice pune-ți următoarele întrebări:

De ce postez acest lucru? Postez un anumit „status" sau imagine ca să mă laud sau chiar vreau să transmit un mesaj prietenilor mei?

Ai spune sau arăta lucrul respectiv într-o camera plină cu prieteni si membri ai familiei? Gândește-te cum ar reacționa părinții tăi dacă ar vedea ceea ce vrei să postezi. Vor avea o reacție pozitivă sau negativă? Așa îți poți da seama dacă e înțelept să postezi conținutul sau nu.

Doresc să împărtășesc această amintire? Amintirile sunt o parte frumoasă din viața noastră. De aceea site-uri precum Facebook, Flickr sau Picasa ne îndeamnă să ne postăm imaginile online, însă, odată postate, ele pot rămâne online.

Fișa educatorului privind riscurile de securitate a calculatorului și navigării online (sfaturi Sigur.info)

Informațiile de mai jos pot constitui puncte de plecare și elemente de verificare a cunoștințelor elevilor privind securitatea calculatorului sau telefonului mobil atunci când acestea sunt utilizate pentru navigarea pe Internet. Subiectele de dezbatere pot fi selectate ținând seama de vârsta copiilor sau timpul aflat la dispoziție.

Fișa educatorului privind riscurile de securitate ale calculatorului și ale navigării online

Ca să știm să ne protejăm de pericolele privind securitatea calculatorului și a utilizării Internetului, trebuie mai întâi să înțelegem care sunt acestea. Fără informații, nu ai cum să afli dacă ești sau nu protejat. E bine să te informezi și să nu lași toată treaba pe seama unui antivirus.

Cine sunt autorii? Hackeri & Crackeri

Ce este un Hacker/Cracker? Termenul "hacker" este de cele mai multe ori folosit în mod greșit. Termenul original "hacker" se referea la o persoană entuziastă în legătură cu tot ce ținea de un computer. Cuvântul "cracker" desemnează o persoană care "sparge" sisteme de securitate.

Servicii de escrow - terțe părți într-o tranzacție care recepționează, depozitează și ulterior livrează fonduri sau documente atunci când se constată îndeplinirea anumitor condiții; cont constituit între un debitor și creditor, dar deținut de un terț, nefiind însă discreționar la dispoziția acestuia; este folosit în cazul în care unul dintre ei nu își achită obligațiile contractuale.

Cum pot fi atacat? Crackerii creează programe care scanează porturile calculatoarelor pentru a verifica dacă sunt accesibile. În cazul în care calculatorul nostru apare pe una dintre aceste verificări, crackerul ar putea să decidă să intre în sistemul nostru informatic. Țintele favorite sunt calculatoarele obișnuite, folosite în casă. Datorită conexiunii deschise permanent există o probabilitate mai mare ca porturile calculatoarelor noastre să fie detectate la o simplă scanare. De asemenea, crackerii pot exploata slăbiciuni în sistemul de operare pentru a putea intra.

Cum mă afectează? Pe lângă potențialele informații valoroase pe care le pot obține de pe computerul tău, crackerii îți vor afecta conexiunea la Internet și spațiul de pe hard-disk. Cu aceste resurse ei pot ataca alte sisteme prin intermediul computerului tău. De cele mai multe ori acest lucru se întâmplă fără ca noi să știm.

Prin ce mijloace acționează?

Viruși & viermi informatici

Ce este un virus? Un virus informatic este un program conceput de o persoană care infectează un fișier sau un alt program de pe calculatorul nostru și poate provoca daune , atât la nivelul sistemului de operare cât și la nivelul elementelor fizice ale computerului (hardware). De fiecare dată când programul alterat rulează și virusul este declanșat vor fi infectate și alte programe din același computer.

Ce este un vierme informatic (worm)? Un vierme este tot un program creat pentru a se multiplica. El nu afectează alte fișiere de pe computer, dar se răspândește către alte computere prin e- mail sau prin rețea.

Cum mă pot infecta? Virușii și viermii informatici pot infecta computerele desktop, laptopurile, tabletele, serverele și pot ajunge pe calculatorul nostru prin e- mail, website-uri, fișiere descărcate și altele mijloace, precum DVD-uri, CD-uri sau memorii USB.

Cum mă afectează?

Efectele infectării unui calculator pot fi foarte neplăcute:

- *dezactivarea computerului*
- *adăugarea, modificarea sau ștergerea unor fișiere*

• *formatarea hard-diskului*

• *furtul de informații (precum adresele de e- mail) din computerul tău pentru a trimite viruși prietenilor, colegilor tăi*

• *trimiterea de mesaje spam către contactele tale și alți utilizatori*

Cai troieni

Ce este un cal troian? Deși caii troieni, tehnic, nu sunt viruși, ei sunt programe spion care, sub aparența utilității lor, realizează funcții malefice care permit accesarea neautorizată a unui calculator, respectiv copierea fișierelor și chiar controlarea comenzilor calculatorului penetrat.

Cum mă pot infecta? Cel mai adesea, ei ajung în computerul tău prin intermediul unui program pe care îl descarci gratuit de pe internet (ex. un joc, un program, muzică).

Cum mă afectează? Un troian instalat pe calculatorul tău îi permite unui terț care are acces la codul troianului respectiv să pătrundă în calculatorul tău.

Cel care face acest atac poate să pătrundă în calculator fără a fi detectat și poate accesa sau distruge informația stocată. În mod alternativ, troianul poate fi programat să trimită în mod automat informații către calculatorul atacatorului. Acestea pot include:

• *Informații ale clienților*

• *detalii despre cărțile de credit*

• *parole pentru online banking sau alte parole importante*

• *adrese de e- mail*

• *informații personale, fotografii*

• *atacarea altor computere prin intermediul celui infectat*

Rootkits

Ce este un rootkit? Rootkit-ul este un instrument de disimulare a unei activități prin intermediul unui program, în scopul obținerii și menținerii accesului la un calculator în modul cel mai ascuns cu putință.

Cum mă pot infecta? Există mai multe metode prin care un rootkit poate ajunge pe calculatorul tău precum deschiderea atașamentelor mesajelor spam sau plantarea lor de către persoane care au reușit să pătrundă în computerul tău.

Cum mă afectează? Rootkit-urile au un singur scop: să permită ca un intrus să ne acceseze sistemul și să preia controlul acestuia fără a putea fi detectat de metodele obișnuite de protecție, cum ar fi antivirusul. În una dintre cele mai întâlnite situații, rootkit-urile sunt folosite pentru a lansa mesaje spam în masă sau pentru a ataca alte computere sau rețele. O altă utilizare a rootkit-urilor este de a ascunde troieni, astfel încât să poată fi extrase informații din computer.

Spam

Ce este Spam-ul? Spam/Spamming este o activitate ilegală de trimitere a unor mesaje electronice pe care destinatarul nu le-a solicitat. Adesea, acestea au un caracter comercial, de publicitate pentru produse și servicii dubioase. Practicat în industria e-marketingului și de către proprietarii de site-uri pentru adulți, spamul nu este doar o bătaie de cap și o pierdere de timp, ci și un risc mare la care suntem expuși atunci când utilizăm Internetul.

Cum mă poate ataca? Zilnic, foarte multe baze de date cu adrese de email circulă pe Internet. Există o multitudine de metode prin care spamerii (cei care răspândesc cu intenție spam-uri) ne pot lua adresa de e- mail și ulterior, pot provoca un bombardament de mesaje nedorite care conțin atașamente de tip malware (rău-intenționat).

Următoarele date sunt sugestive pentru activitățile de tip SPAM:

- *80% dintre mesajele spam își au originea în calculatoarele de acasă. Acestea au fost accesate fără voia sau știința utilizatorilor și folosite cu scopul de a trimite mesaje spam.*
- *Furturile și înșelăciunile prin intermediul mesajelor spam cresc zilnic.*
- *95% dintre viruși sunt trimiși prin email.*

Web bug (pixel spion)

Ce este un web bug? Este un fișier imagine, de dimensiuni foarte mici, ascuns într-o pagină web sau un email.

Cum mă poate ataca? Ca multe alte malware, nu știm când un web bug e prezent. Acesta este de cele mai multe ori descărcat în spam și se poate afla pe orice pagină web pe care o vizităm.

Cum mă pot afecta? Un web bug îi poate transmite unui spamer când un email a fost deschis. lÎi poate transmite, de asemenea, ce reclame și pagini web au fost accesate. Un web bug poate descoperi detalii despre sistemul nostru care pot fi foarte utile crackerilor.

Ferestre Pup-up/Pop-under sau Bannere Ad (bannere publicitare)

Ce este un pop-up/pop-under/banner? O reclamă de tip pop-up apare ca o fereastră separată peste pagina web pe care tu o vizualizezi. Fereastra pop-under, în schimb, după cum îi spune și numele, apare sub pagină și este vizibilă abia după ce închizi browserul. Un banner este vizibil pe pagină și poate fi animat sau static.

Care este riscul? Pop-up-urile/pop-under-urile/bannerele ne pot deranja atunci când navigăm, iar unele dintre ele prezintă riscuri serioase, putând purta troieni sau spyware. Din păcate nu putem spune care astfel de bannere sunt periculoase. Ceea ce știm este să nu dam niciodată click pe ele pentru că atunci malware-ul este instalat pe calculatorul nostru.

Cookies

Ce sunt cookies? Când navigăm pe site-uri web, serverele trimit cookies către browser-ul nostru web (ex. Internet Explorer, Mozilla Firefox, Google Chrome) care le stochează pe hard disk. . Acestea sunt fișiere text mici care identifică fiecare utilizator. Când accesezi o altă pagină sau te întorci la website-ul respectiv, serverele web îi cer browser-ului tău acele fișiere cookie ca să recunoască cine ești.

Cum mă pot afecta? Cookies sunt folosite de cele mai multe ori de agenții publicitare pentru a urmări comportamentele noastre online de căutare și cumpărare. Mai multe site-uri pot citi informații din același cookie sau pot partaja informații fără ca utilizatorul să știe.

Deși nu sunt un risc de gradul celor menționate mai sus, fișierele cookie reprezintă un pericol pentru informațiile noastre personale.

Spyware

Ce este spyware-ul? Spyware-ul a depășit virușii la nivel de risc. Statisticile estimează că 80-90% dintre computere au fost deja infiltrate de spyware. Acesta este un software care se instalează pe hard-diskul nostru pentru a colecta informații despre noi și despre obișnuințele noastre online și ransmite toate aceste informații prin conexiune la internet către alte servere fără consimțământul sau știința utilizatorului.

Cum mă poate infecta? Spyware este descărcat de cele mai multe ori prin intermediul programelor gratuite sau prin sisteme peer-to-peer (ex. oCD, DC++).

Cum mă afectează? Spyware-ul poate scana hard-drive-ul nostru și poate căuta informații, cum ar fi datele noastre bancare sau alte detalii personale. De asemenea, poate să schimbe adresa de start a browser-ului, poate scana și înregistra istoria browser-ului și poate monitoriza aspecte ale activităților desfășurate pe calculator. Informațiile sunt transmise mai apoi atacatorului.