Discutie:

Cat de des accesati internetul pe zi?

Cati utilizeaza retele de socializare?

Cati detin antivirus / profil inchis pe retele de socializare?

Elev1:

1)Internet - spațiu virtual în care oricine indiferent de cultură, sex și vârstă pot beneficia de informație și divertisment

2)Spam – mesaje electronice nesolicitate cu caracter comercial de cele mai multe ori. Desi spam-ul in sine nu este un program malitios, el le poate contine sau sa va retrimita la ele. Cum de actionat cu spam-ul? Din inbox trimiteti mesajul spre box ”spam” sau ignorati acest tip de mesaje.

3)Cookie-urile – fisiere care stocheaza informatie despre actiunile utilizatorului pe web. Nu au caracter nociv , unele site-uri nu pot functiona fara ele. Pentru ce sunt necesare? Cookie-urile sunt utilizate pe site-uri cu sistemul ”cos de cumparaturi” sau pentru autentificare.

4)Spyware – software malitios atasat de obicei la aplicatii gratuite. Ele analizeaza domeniul de interes a utilizatorului si le folosesc in continuare pentru a transmite utilizatorului publicitate .

5)Keylogger- program care inregistreaza fiecare bataie pe tastatura si salveaza cele introduce intr-un fisier. Astfel instalatorul keyloggerului poate obtine informatia voastra personala. Keyloggerul poate cauza pierderea parolelor si a datelor de autentificare.

6) Phising – ar fi o imbinare dintre spam si keylogger dupa functie caci aceasta reprezinta o modalitate de furt a datelor precum a contului bancar printr-un mesaj de genul ”Sunteti al 1000 vizitator, completati formularul si primiti 500USD”. Uneori mesajele pot veni pe posta electronica fiind scrise intr-o maniera oficiala. Niciodata nu dezvaluiti datele voastre personale pe internet chiar daca aceasta actiune pare a fi sigura.

7)Parazitii: avem 3 tipuri de paraziti : viruși, troieni si viermi.

\*Virus – program care se instaleaza singur si provoaca pagube in sistemul de operare sau in elementele hardware.

\*Troian – program care se downloadeaza impreuna cu un alt program, deschizand ”usa” unei alte persoane. Acea persoana poate liber s ava exploateze datele din calculator.

\*Vierme – program care instalindu-se se multiplica. Se pot raspandi la alte calculatoare prin messenger, torrents, email. El infecteaza sistemul informatic.

Elev2:

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.

Discutie in doi despre antivirusi si cautare sigura pe internet.

Elev2:

Securitatea Wifi(sfaturi)

**ALEGE WPA sau WPA2**. Acesta e primul si cel mai important pas pe care il poti face. Alege una din optiunile de criptare WPA sau WPA2. Nu e o idee buna sa folosesti standardul **WEP**deoarece e foarte usor de spart. Totodata, foloseste o parola mai lunga, care sa contina litere, numere si caractere speciale. Daca faci asta, poti spune ca ai rezolvat problema in proportie de 50%.

**SCHIMBA-TI PAROLELE INITIALE.** Majoritatea routerelor folosesc username-ul “admin” sau “administrator”, alaturi de o parola de genul “123456”. Alege un nou username si o noua parola. Daca vrei, poti schimba setarile si pentru contul de vizitator. Totodata, e bine sa dezactivezi si optiunea care permite autentficarea de la distanta. **Pentru un plus de securitate, dezactiveaza si posibilitatea de a folosi contul de administrator prin conexiune wireless.** Insa, de acum incolo, daca vrei sa modifici setarile routerului, va trebui sa folosesti un cablu.

**MODIFICA SSID-ul.** Dupa ce ai schimbat parola de administrator, trebuie sa schimbi si numele initial SSID. Soft-ul routerului va atribui un nume implicit, care le poate da posibililor atacatori indicii pretioase. Cum ar fi chiar faptul ca inca nu ti-ai schimbat parola initiala. Un nume diferit nu va atrage atentia si te va ajuta apoi sa-ti gasesti repede reteaua, daca stai la bloc, de exemplu. Daca tot esti aici, ar fi bine sa dezactivezi si optiunea “**SSID Broadcast**”. Nu e insa obligatoriu. Desi aceasta facilitate e utila pentru identificarea retelei si pentru o trecere  mai usoara de la un hotspot Wi-Fi la altul, transmiterea numelui retelei e ca o invitatie deschisa pentru hackeri. Aceasta modificare e cu dus si intors pentru ca, la fel de bine, o retea ascunsa poate starni mai mult interes din partea unui atacator cu experienta.

**VERIFICA CINE SE CONECTEAZA LA RETEAUA TA**. Majoritatea routerelor ofera aceasta posibilitate. Mai mult, poti seta un numar maxim de conexiuni permise, sau o anumita gama de IP-uri pentru fiecare dispozitiv. De exemplu, daca acasa te vei conecta la reteaua Wi-Fi doar prin intermediul unui laptop si a unui smartphone, nu are rost sa lasi mai mult de doua conexiuni posibile simultan. **Pentru mai multa protectie poti activa si optiunea de filtrare a adreselor MAC**. Inainte, trebuie sa ai conectate la router toate dispozitivele pe care le folosesti, pentru a le vedea adresele MAC.

**Nu FOLOSI WPS.** Protocolul **Wi-Fi Protected Setup** cedeaza usor in fata atacurilor de tip brute-force. In plus, o vulnerabilitate majora descoperita in 2011 le permite hackerilor sa afle un PIN WPS in doar cateva ore, iar apoi, cu ajutorul lui, iti pot afla si cheia WPA-WPA2.

**ACTUALIZEAZA FIRMWARE-ul.** E o masura esentiala. Producatorii fac periodic update-uri de firmware pentru aproape toate routerele. Procedeaza insa cu atentie, mai ales in cazul modelelor vechi. Routerele noi iti ofera insa posibilitatea unui upgrade fara dureri de cap.

**FOLOSESTE UN FIREWALL.** Routerul tau deja actioneaza ca un firewall hardware, iar de la UPC, de exemplu, alaturi de [cel mai rapid Internet din Romania, Fiber Power](http://www.upc.ro/internet/), poti sa iti achizitionezi, cu doar 5 RON, antivirusul [SmartGuard](http://www.upc.ro/internet/extra/smartguard/) care iti ofera si o solutie completa, inclusiv anti-spyware si firewall. Si asta fara ca viteza ta pe web sa fie afectata. Nu e nevoie asadar de solutii de securitate scumpe.

Discutie pe tema: Hartuire online + film

Elev2:

Sfaturi pentru securitatea informatiilor pe internet.

**1. Utilizeaza motoarele de cautare care nu colecteaza date**

Google si-a creat deja o reputatie nefasta cu privire la colectarea datelor despre utilizatori. Pentru anonimat complet online, foloseste DuckDuckGo, singurul motor de cautare ce garanteaza siguranta utilizatorilor impotriva colectarii de date. Alte variante mai putin infricosatoare decat Google sunt Bing si Ixquick.

**2. Foloseste un serviciu VPN**

Cele mai multe servicii VPN de calitate nu sunt gratuite, dar iti ofera o conexiune sigura la internet care previne colectarea informatiilor despre tine de catre site-urile vizitate, dar si de catre furnizorul de internet.

**3. Vizualizeaza email-ul ca text**

Elimina complet amenintarile malware din email, ce se pot strecura si in poze, vizualizand toate mesajele email ca text, mai ales intr-un manager de mail local ca Outlook si Thunderbird.

**4. Foloseste parole complexe**

[Parolele complexe](http://www.hit.ro/stiinta-generala/Ghid-cum-sa-ti-securizezi-activitatea-online), notate pe hartie, raman cel mai bun mod de a-ti proteja conturile. Multe managere de parole promit siguranta, dar pot avea probleme tehnice care le intrerup serviciul exact atunci cand ai mai multa nevoie de ele. Foloseste parole complexe si noteaza-ti-le pe o hartie separata de numele de utilizator si de site.

**5. Utilizeaza o adresa de mail secundara**

Cele mai multe servicii online necesita o adresa de email, motiv pentru care este important sa ai cel putin doua adrese de posta electronica. Cea personala si cea secundara, in care vei observa cum se aduna spam-ul pe masura ce o folosesti mai mult.

**6. Profita de update-urile automate**

Update-urile automate ofera siguranta sporita in mod rapid. Utilizeaza-le, indiferent daca este vorba de sistemul de operare sau browser, mai ales in cazul plugin-urilor problematice, ca [Flash](http://www.hit.ro/software/Microsoft-va-rezolva-vulnerabilitatea-Flash-din-IE-10-printr-un-patch) si [Java](http://www.hit.ro/stiinta-generala/De-ce-este-timpul-sa-renunti-la-Java).

**7. Foloseste un firewall bun**Indiferent daca optezi pentru firewall-ul nativ al sistemului de operare sau pentru cel oferit de un program antivirus, asigura-te ca este activat non-stop pentru protectie cat mai buna impotriva atacurilor informatice.

**8. Limiteaza-ti tranzactiile online**

Comertul online este in crestere si dupa el cresc in mod proportional si incercarile de frauda online. Cand ai de facut tranzactii online, fa-le doar dintr-o retea securizata si pe un site sigur (https://).

**9. Nu lasa computerul conectat la retele cand nu il folosesti**

Sansele unui atac informatic scad usor atunci cand gadgeturile nu sunt conectate permanent la retea, inclusiv in momentele cand nu sunt folosite. Inchide PC-ul cand nu il folosesti pentru a-l expune mai putin la riscuri.

**10. Protejeaza-ti smartphone-ul**

Daca ai internet pe telefon si utilizezi mai multe conturi, securizeaza-ti telefonul cu un cod de securitate. Introducerea lui de fiecare data cand deschizi ecranul este un efort, dar stii astfel ca nimeni nu-ti va accesa informatiile din telefon.

Elev1: Discutie pe tema actiuni ilegale pe internet (downloadare torrent, drept de autor)

Discutie:

Sfaturi pentru navigarea sigura pe internet

• Aveți grijă cum postați fotografii cu dvs. sau cu familia! Restricționați accesul necunoscuților la profilul dvs. Nu uitați că fotografiile sau filmulețele, odată postate, pot rămâne pentru totdeauna pe alte computere şi servere, chiar dacă veți șterge postarea inițială.  
• Nu tot ceea ce citiți sau vedeți pe internet este adevărat. Oricine poate crea pagini web sau poate posta știri, fotografii, filme. Fotografiile și filmele pot fi trucate pe calculator cu ușurință. Pentru a verifica dacă o informație este reală, verificați mai multe surse de informare.  
• Atenție! Frazele sau pozele preluate dintr-un material de pe internet trebuie însoţite de precizarea sursei, pentru a nu fi considerat plagiator.  
• Păstrați secretă parola de e-mail și nu o dezvăluiți nici măcar prietenilor! Dacă bănuiți că parola v-a fost descoperită, schimbați-o imediat! În acest fel nimeni nu vă poate citi mesajele personale și nu vă poate folosi contul pentru a trimite e-mail-uri care par din partea dvs.  
• Când vă creați adresa de e-mail, folosiți un pseudonim, o prescurtare şi în niciun caz numele întreg, data nașterii sau orice altceva ce poate fi cunoscut sau recunoscut despre dvs. cu ușurință.  
• Parola e bine să aibă cel puţin 12 caractere, să conţină litere, cifre şi semne de punctuaţie şi să fie cât mai greu de ghicit, chiar şi pentru cei care vă cunosc foarte bine. Nu folosiți datele de naştere sau alte cuvinte pe care cei din jur ştiu că le preferați şi pe care le-ar putea ghici.  
• Pentru protecţia computerului, scanați ataşamentele de e-mail înainte de a le deschide.  
• Nu descărcați și nu instalați programe pirat sau pe care nu le cunoașteți; ele pot distruge date din calculatorul dvs.  
• Navigarea pe Internet este sigură când vă personalizați browser-ele să nu rețină parole, date de identificare și să nu dea accept la comunicarea oricăror date motivate ca fiind „în interes statistic” etc.  
• Puteți oricând să vă opriți din navigarea pe internet sau să refuzați continuarea unei discuții pe chat, dacă s-a întâmplat ceva care nu v-a plăcut sau care v-a speriat.  
• Dacă primiți e-mail-uri, fișiere, fotografii sau programe de instalare de la cineva pe care nu-l cunoașteți sau care vi se par suspecte, nu le deschideți, ștergeți-le imediat. Ele pot avea viruși sau programe care pot citi date de pe calculatorul dvs. Cereți ajutorul unei persoane specializate când observați că nu mai funcționează normal computerul.