MINISTERUL EDUCAȚIEI

Daniel Popa

INFORMATICĂ ȘI TIC

Manual pentru clasa a VI-a

EDITURA DIDACTICĂ ȘI PEDAGOGICĂ S.A.

CUPRINS

Protecția datelor personale pe Internet

Amintește-ți!

1. Lucrați în perechi. Discută cu un coleg despre pericolele la care vă expuneți atunci când navigați pe Internet. Faceți împreună o listă cu acestea și găsiți o soluție pentru fiecare.

Descoperă!

2. Caută pe Internet informații despre „securitatea online pentru copii". Citește 2-3 dintre articolele găsite pe prima pagină în motorul de căutare și extrage ideile comune. Citește articolul de la această adresă http://www.sigur.info/siguranta-online/copii-pe-internet/copii.html. Ce alte adrese ai găsit?

Important

Internetul este un spațiu public la care oricine are acces. Dacă o persoană postează informații despre sine (poze, date personale etc.) e ca și cum ar avea un panou publicitar în mijlocul orașului pe care ar publica aceste informații. Oricine poate avea acces la informațiile publicate de persoana respectivă și le poate folosi precum dorește.

Dacă o persoană poate fi identificată direct sau indirect pe baza unor informații sau date, atunci acestea pot fi considerate **date personale**.

Datele personale pot fi:

ale persoanei: nume, prenume, CNP, imagine (poză), ADN, amprente;

despre persoană: sex, rasă, vârstă;

în legătură cu persoana: adresă de domiciliu, ocupație.

Exemplu: În afirmația „Un elev din orașul București ..." se întâlnesc date anonime, deoarece nu se poate identifica persoana. Însă, afirmația „Elevul Totescu Kalin, elev la Școala nr. 7 din București ...", conține suficiente date (personale) pentru a identifica persoana.

Identitatea virtuală este creată de o persoană pentru a fi reprezentarea sa în spațiul virtual. De obicei este un cont protejat de o parolă pe o rețea de socializare, într-un joc video, într-un sistem de comunicare pe Internet.

Exersează!

3. Realizează următoarele căutări pe Internet: „imagini modificate", „Bean gladiator". Printre căutările obținute, ai găsit și imaginea alăturată care nu este una reală. De unde a pornit modificarea imaginii? Din ce cauză crezi că a fost modificată? Cum ai proceda, dacă ai găsi pe Internet o imagine cu tine modificată?

4. Caută pe Internet informații despre tine. Ce date ai găsit? Caută informații despre o celebritate sau o persoană foarte cunoscută în România. Ce informații personale ai găsit despre aceasta?

Amintește-ți!

5. Care sunt regulile pe care trebuie să le respecți pentru a fi în siguranță pe Internet?

Descoperă!

6. Caută pe Internet informații despre „furtul de identitate pe Internet". Descrie în două sau trei propoziții ce este furtul de identitate. De ce crezi că cineva ar fura identitatea altcuiva?

Important

Furtul de identitate pe Internet este o fraudă în care o persoană își însușește datele personale ale altcuiva în vederea furtului de bani sau obținerii de alte beneficii.

Metode de furt de identitate pe Internet:

• Furt de identitate prin e-mail sau site-uri specializate (phishing): se cer date personale pentru a primi o recompensă.

• Solicitare de informații la navigarea pe Internet: date „necesare" pentru a crea un cont.

• Prin rețele sociale (informații oferite public): imagini postate pe acestea, locul de muncă, adresa, numărul de telefon etc.

Utilizare de software specializat: programe care înregistrează apăsările de taste, ecranul.

Cum te poți proteja de furtul de identitate pe Internet:

Nu publica pe rețelele sociale date despre tine (data nașterii, adresa, numărul de telefon etc.).

•Nu răspunde mail-urilor care îți cer date personale pentru a primi o recompensă.

•Dacă trebuie să-ți faci un cont pe un site, completează minimum de date necesare.

•Dacă ți se cer informații personale pe un site și nu știi ce să faci, întreabă părinții sau un adult în care ai încredere dacă trebuie sau nu să furnizezi acele informații.

•Asigură-te că ai instalată pe calculator o suită de securitate.

•Alege parole complicate pentru conturile tale și nu folosi aceeași parolă pe mai multe conturi.

•Dacă trebuie să folosești calculatoare publice, pentru a evita furtul de identitate, repornește calculatorul respectiv, pornește browser-ul în modul incognito, iar la final pornește din nou calculatorul.

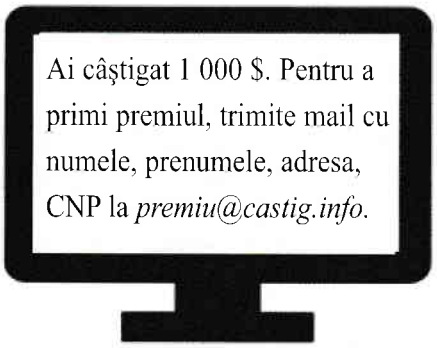
Exersează!

7. Lucrați în echipe. Împreună cu 3 colegi caută informații despre furtul de identitate pe Internet. Fiecare dintre voi alege o metodă utilizată pentru furtul de identitate și o metodă de prevenire a acestuia. Folosind informațiile adunate, faceți o listă cu cele mai folosite metode privind cele două categorii. Pentru fiecare listă, ordonați rezultatele obținute în funcție de cel mai mare număr de apariții pe Internet.

8. Citește mesajul din imaginea alăturată.

a) Cum ai proceda dacă ai primi un astfel de mesaj? De ce?

b) Ce fel de metodă de furt de identitate ai recunoscut în acest mesaj?



9. Caută pe Internet și află „de ce avem nevoie de securitatea cibernetică". Dacă printre rezultatele tale s-au aflat și site-urile: sri.ro, bitdefender.ro, nume.blogspot.ro, în care dintre acestea ai avea încredere? De ce?

10. Lucrați în echipe. Împreună cu 4 colegi discută despre cum ați învățat în clasa a V-a să vă creați parole sigure. Căutați pe Internet reguli pentru crearea și utilizarea unei parole sigure. Citiți câteva articole despre acest subiect și, pentru fiecare dintre regulile de mai jos, numărați de câte ori apare. Ce alte reguli ați mai găsit?

a) Parola trebuie să fie lungă, minimum 8 caractere.
b) Parola trebuie să conțină litere mici, litere mari, cifre și semne.
c) Nu folosi cuvinte din dicționar în parolă.
d) Nu folosi aceeași parola pe mai multe conturi.
e) Schimbă periodic parola conturilor importante.

11. Care dintre parolele de mai jos le consideri a fi sigure? De ce?
a) parola1;
b) anaaremere;
c) 4n4_aR3_m3r3;
d) AoCpApRc$3.

12. Caută pe Internet informații despre cele mai nepotrivite parole. Este vreuna dintre parolele tale asemănătoare celor găsite?

13. Caută pe Internet informații despre cât valorează datele tale cu caracter personal. O căutare în limba engleză ar aduce mai multe informații față de o căutare în limba română.

Informează-te!

• O persoană are dreptul:

a) să cunoască numele operatorului care colectează informațiile, scopul în care sunt prelucrate datele și firma/persoana către care pot fi transferate datele care colectează informațiile;

b) să primească într-o formă inteligibilă o copie a datelor personale deținute de un operator de date cu caracter personal și să solicite eliminarea, blocarea sau ștergerea datelor, dacă acestea sunt incomplete, inexacte sau obținute prin mijloace care nu respectă legea;

c) să se opună prelucrării datelor cu caracter personal;

d) să beneficieze de confidențialitatea comunicațiilor on-line;

e) să fie informată dacă datele personale deținute de un operator de date/firmă au fost pierdute sau furate.

• Atunci când îți creezi un cont de e-mail sau un cont pe un site trebuie să-ți dai acordul pentru prelucrarea datelor personale. În acei termeni și condiții pentru care îți dai acceptul, ești informat despre tot ce poate face firma respectivă cu datele tale personale, ce drepturi și îndatoriri ai.

Știai că...?

- Poți să creezi parole după o propoziție sau frază. De exemplu: Din propoziția: „Ana are 5 mere și 7 pere.", se poate obține parola Aa_5ms_7p, folosind prima literă a fiecărui cuvânt și punând simbolul _ în fața cifrelor. Poți să-ți creezi propriile reguli de formare a parolei pornind de la acest exemplu.
- Firmele care adună sau prelucrează date cu caracter personal trebuie să informeze clienții atunci când colectează date cu caracter personal care îi privesc.

Măsuri de siguranță în utilizarea Internetului. Utilizarea soluțiilor de securitate

Amintește-ți!

1. Lucrați în perechi. Discută cu un coleg despre regulile pe care trebuie să le respectați pentru securitatea datelor personale. Ce măsuri de securitate vă amintiți din clasa a V-a?

Descoperă!

2. Lucrați în echipe. Împreună cu 4 colegi, întocmește o listă cu tipuri de programe care pot cauza probleme calculatorului. Scrieți în dreptul fiecărui tip de program ce știți despre el: ce face, cum acționează etc.

3. Caută pe Internet informații despre malware (software rău intenționat). Compară ceea ce ai găsit cu lista obținută la exercițiul anterior.

Important

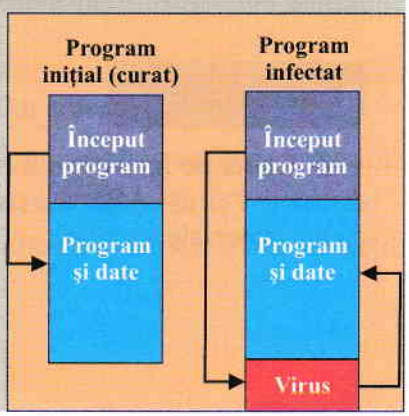
Cuvântul **malware**, rezultat din unirea cuvintelor malicious și software, este folosit pentru a identifica un software proiectat să se infiltreze și/sau să avarieze sistemul unui computer, fără consimțământul proprietarului.

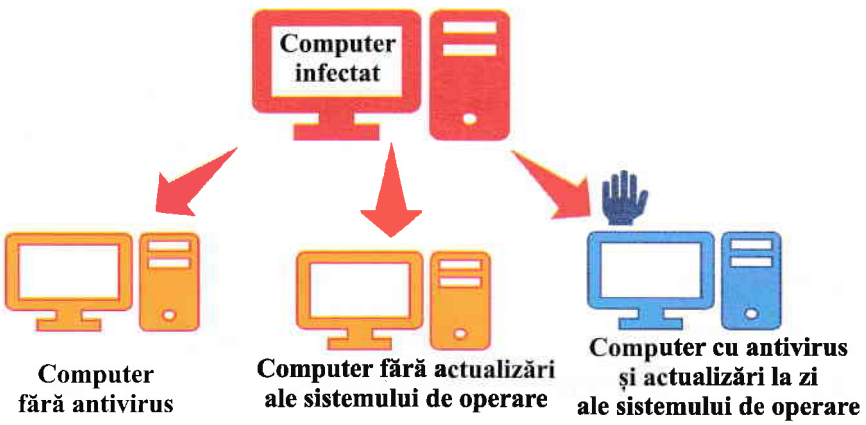
Exemple de programe malware: viruși, viermi, cai troieni, spyware, adware și alte programe rău intenționate.

a) Virusul, probabil cel mai cunoscut tip de software dăunător, este un program de mici dimensiuni care se atașează de un program.

Cum funcționează? La pornirea programului afectat, mai întâi pornește virusul, care se instalează în memoria calculatorului, apoi virusul lansează în execuție programul original. Odată prezent în memorie, virusul caută alte fișiere care nu au fost infectate pentru a le infecta.

b) Viermele este un program care se poate răspândi fără acțiunea directă a utilizatorului, copiindu-se singur în rețea, pe discuri (memory stick-uri, harddisk-uri externe etc.).





c) Calul troian este un program care are funcționalități ascunse, oferind accesul, de la distanță, la computerul pe care rulează aplicația. Un cal troian poate fi ascuns într-un sistem de operare sau într-un program descărcat de pe Internet. **Atenție!** Existența unui antivirus pe calculator nu garantează că aplicația de tip cal troian nu își va atinge scopul.

d) Spyware este un program care raportează cuiva (de obicei realizatorului programului) ce faci, ce site-uri vizitezi, ce tastezi pe un site (parole, cont bancar etc.), care este comportamentul tău pe Internet. O mare parte din acele toolbar-uri (bare cu unelte, butoane instalate în browser), care îți oferă diverse servicii pe Internet, au rolul de spyware. Un exemplu de spyware este în dreapta.

e) Adware este o variantă de spyware care doar adaugă/aduce reclame pe calculatorul tău.

f) Ransomware este un tip de malware care blochează accesul utilizatorului calculatorului la unele fișiere sau chiar la propriul calculator și cere plata unei recompense. Cel mai adesea, programul criptează datele de pe calculator și în schimbul unei sume de bani realizatorul programului trimite cheia pentru decriptarea datelor.

Exersează!

4. Caută pe Internet informații despre cei mai distructivi viruși. Află câte sisteme au infectat și ce daune materiale au creat.

Descoperă!

5. Lucrați în echipe. Împreună cu 3 colegi caută pe Internet informații despre cel mai bun antivirus. Alegeți mai multe surse și analizați-le. Determinați prețul mediu pentru o suită de securitate. Ce este mai scump: să achiziționezi un antivirus sau să repari daunele provocate de malware? De ce?

Important

Un program antivirus are rolul de a găsi și elimina malware și de a proteja computerul de aceștia. Datorită numeroaselor tipuri de amenințări, un simplu antivirus nu este suficient, ci este necesară o suită de programe de securitate.

Acestea sunt câteva dintre companiile care dezvoltă programe antivirus.

McAfee WEBROOT avast EMSISOFT F-Secure TREND MICRO
Norton Bitdefender KASPERSKY eset

O soluție de securitate completă ar trebui să ofere:

a) Scanare de fișiere la cerere – adică să poți verifica ce fișiere dorești pentru a determina dacă acestea sunt infectate cu malware sau nu.

b) Scanare de fișiere la acces – atunci când încerci să deschizi un fișier, soluția de securitate analizează, înainte de a permite deschiderea acestuia, dacă fișierul prezintă pericol sau nu.

c) Analiza site-urilor vizitate – soluția de securitate urmărește ce site-uri vizitezi și blochează accesul la site-urile periculoase sau te anunță că vei vizita un site care ar putea dăuna computerului tău (site-ul e cunoscut că livrează software dăunător) sau ție (site de phishing).

d) Protecție bazată pe comportament – aplicația de securitate verifică pentru fiecare aplicație instalată în computerul tău dacă are un comportament asemănător cu cel al programelor malware.

e) Scanare vulnerabilități software – soluția de securitate verifică dacă sistemul de operare și aplicațiile instalate nu au vulnerabilități.

Exersează!

6. Lucrați în echipe. Împreună cu 3 colegi caută pe Internet informații despre principalele suite de securitate și completați într-un tabel, pentru fiecare aplicație, dacă oferă sau nu soluții de securitate completă.

7. Lucrați în perechi. Alături de un coleg alege o suită de securitate care oferă atât soluții gratuite, cât și contra cost. Comparați cele 2 soluții. Pe care ai alege-o? Dar colegul tău? De ce?

8. Caută pe Internet „antivirus fals". Despre ce este vorba? Cum acționează un astfel de program? Cum te poți feri de un antivirus fals?

9. Folosește motorul de căutare preferat pentru a determina ce suite de securitate oferă protecție împotriva aplicațiilor de tip ransomware.

Știai că...?

- *Creeper* a fost primul virus, scris în 1971, de către Bob Thomas. Virusul se multiplica și afișa mesajul „I'm the creeper: catch me if you can" (*Eu sunt ticălosul, prinde-mă, dacă poți*). Pentru „vânarea" lui a fost scris un alt program numit *Reaper* (Secerătorul).

- Programele de tip malware pot fi folosite ca arme. Stuxnet este numele unui malware despre care se crede că a fost creat pentru a afecta programul nuclear al Iranului. Stuxnet se infiltra pe un calculator prin intermediul unui stick USB infectat și infecta orice stick introdus în computer. Dacă găsea atașat la computer un dispozitiv ce putea controla o centrifugă folosită la îmbogățirea uraniului, programul de tip malware dădea comandă respectivului dispozitiv să se rotească cu viteză foarte mare, distrugând centrifuga.