MINISTERUL EDUCAȚIEI

Daniel Popa

INFORMATICĂ ȘI TIC

clasa a VI-a

intuitext
grup SOFTWIN

CUPRINS

1 Ne amintim, ne informăm 6
- Recapitulare 6
- Evaluare 8

2 Internet 9
- Protecția datelor personale pe Internet 10
- Măsuri de siguranță în utilizarea Internetului. Utilizarea soluțiilor de securitate 14
- Poșta electronică (e-mail) – conturi, structura unui mesaj 17
- Operații cu mesaje electronice 20
- Reguli de comunicare pe Internet 27
- Recapitulare 31

3 Prezentări 33
- Reguli elementare de susținere a unei prezentări 34
- Elemente de interfață ale unor aplicații de realizare a prezentărilor 36
- Operații de gestionare a prezentărilor 40
- Operații de editare a unei prezentări 42
- Reguli elementare de estetică și ergonomie utilizate în realizarea unei prezentări 43
- Structura unei prezentări: diapozitive, obiecte utilizate în prezentări. Formatarea acestora 44
- Animații și efecte de tranziție 49
- Recapitulare 53
- Evaluare 54

4 Animații grafice și modele 3D 55
- Scenariul unei animații 56
- Elemente de interfață ale unor aplicații de animație grafică 58
- Operații specifice de realizare a unei animații 64
- Operații de gestionare a animațiilor 71
- Realizarea desenelor 3D 74
- Operații de editare a proprietăților unui obiect 78
- Realitatea virtuală 82
- Recapitulare 87
- Evaluare 88

5 Algoritmi 89
- Ce este un algoritm? (recapitulare) 90
- Elemente de interfață ale unor aplicații de exersare a algoritmilor 91
- Instrumente de bază utilizate în exersarea algoritmilor 93
- Etapele unui exercițiu algoritmic 96
- Structura repetitivă cu contor 101
- Structura repetitivă condiționată anterior 103
- Structura repetitivă condiționată posterior 106
- Recapitulare 109
- Evaluare 110

6 Pași spre vacanță 111
- Recapitulare finală 112
- Evaluare finală 116
- Soluții 117

Competenţe generale

1. Utilizarea responsabilă și eficientă a tehnologiei informației și comunicațiilor
2. Rezolvarea unor probleme elementare prin metode intuitive de prelucrare a informației
3. Elaborarea creativă de mini proiecte care vizează aspecte sociale, culturale și personale, respectând creditarea informației și drepturile de autor

Competențe specifice

1.1. Utilizarea eficientă a instrumentelor specializate în scopul realizării unei prezentări

1.2. Utilizarea eficientă a instrumentelor specializate în scopul realizării unei animații grafice

1.3. Aplicarea operațiilor specifice pentru comunicarea prin Internet

2.1. Utilizarea unui mediu grafic-interactiv pentru exersarea algoritmilor

2.2. Aplicarea etapelor de rezolvare pentru cerințe simple, corespunzătoare unor situații familiare

2.3. Reprezentarea algoritmilor de prelucrare a informației pentru rezolvarea unor situații problemă

3.1. Elaborarea de prezentări folosind operații specifice, pentru a ilustra diverse teme

3.2. Elaborarea de animații grafice și modele 3D folosind operații specifice pentru a ilustra dinamic diverse teme

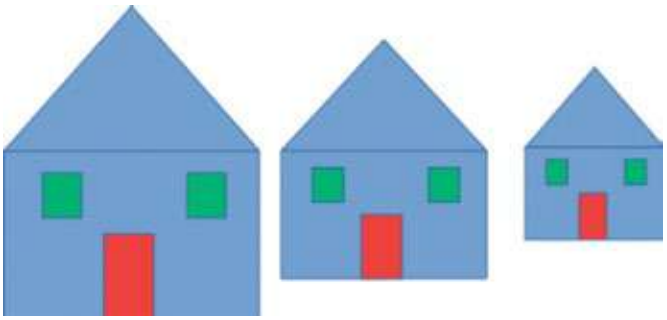
3.3. Utilizarea unor instrumente specializate pentru obținerea unor materiale digitale

1 NE AMINTIM, NE INFORMĂM

Recapitulare

Amintește-ți!

1 Deschide editorul grafic preferat și realizează un desen asemănător cu cel de mai jos. Cum ai procedat pentru a realiza desenul cât mai rapid?

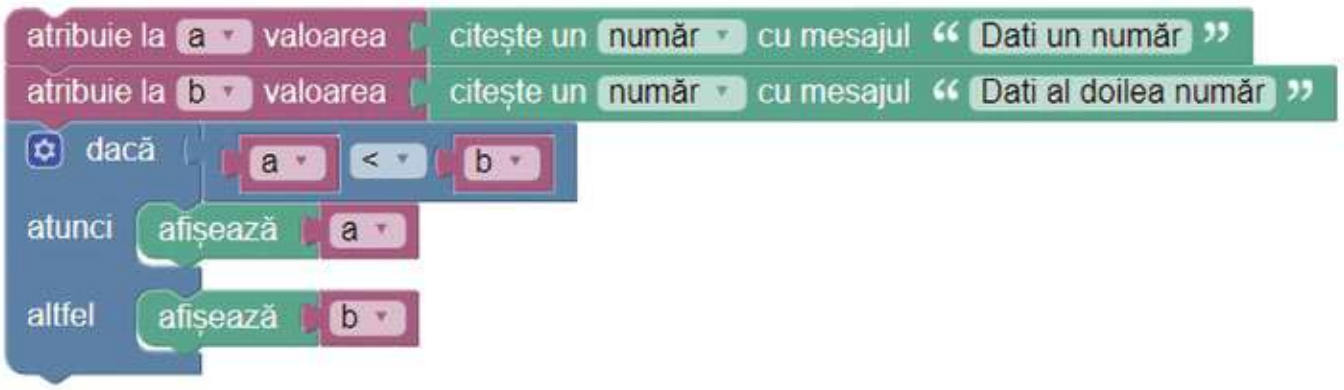


Joc – *Cine știe, câștigă!*

2 Împărțiți-vă în două echipe. Fiecare echipă observă laboratorul de informatică și creează un set de bilețele cu numele unor componente de computer (tastatură, placă de rețea, imprimantă etc.) care se găsesc sau nu în laboratorul vostru. Echipele pun bilețele într-un recipient diferit, apoi extrag, rând pe rând, câte unul din recipientul echipei adverse. Fiecare echipă va identifica dacă respectiva componentă se află sau nu în laborator și va preciza două informații despre aceasta.

3 Intră pe Internet, pe site-ul https://scratch.mit.edu/ și realizează un joc ca cel de la adresa: https://scratch.mit.edu/projects/200539078/.

4 Determină ce se afișează în urma executării algoritmului prezentat mai jos, dacă primul număr este 7, iar al doilea număr este 9.



5 Evaluează următoarele expresii matematice:

a) 15/4+2/3;

b) (4*3/8+5/2*2) *2-3/2;

c) 7/2 – 7%2*2.

6 Ce elemente poți găsi pe bara de aplicații (taskbar)?

a) ceas;

b) aplicații care rulează;

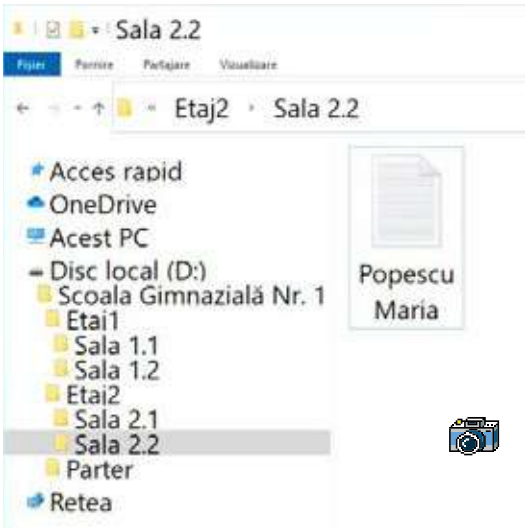
c) numele utilizatorului.

7 Caută pe Internet, textul „Extensie de fișier”. Informează-te și află mai multe din pagina *Wikipedia* ce este o extensie de fișier, apoi citește extensiile de fișiere explicate. Unde le-ai mai întâlnit?

8 Privește imaginea și completează un tabel asemănător celui de mai jos.

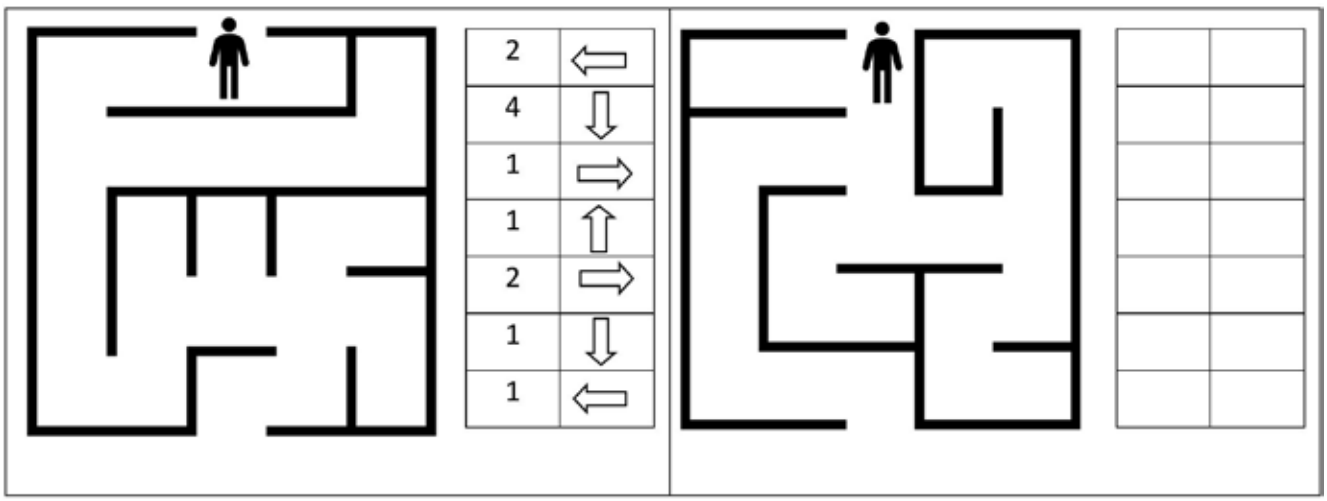
Tip dispozitiv	Nume	Caracteristici
Intrare		
Ieșire		
Stocare		

9 Imaginează-ți școala ta ca pe o ierarhie de directoare. Clădirea principală este un director, fiecare etaj este un director aflat în directorul clădirii principale, fiecare sală de clasă este un director aflat în directorul asociat etajului. Creează această ierarhie de directoare și în fiecare clasă (director corespunzător clasei) creează un fișier a cărui denumire să fie numele profesorului care predă în sala de clasă respectivă, ca în exemplul alăturat.



10 Ai realizat pe calculatorul tău o colecție de poze cu o dimensiune totală de 60 GB și vrei să le salvezi pe un suport extern. Ce alegi să folosești: DVD-uri sau memory stick ? Justifică răspunsul.

11 Dispui de un robot căruia poți să-i dai comenzi de forma *număr-direcție* și care se deplasează un număr specificat de pași în direcția indicată. Urmărește indicațiile date robotului din partea stângă, apoi scrie pentru robotul din dreapta o serie de comenzi care să-l ducă la ieșirea aflată în partea de jos a labirintului.



Evaluare

Din oficiu (10 p)

1 În imaginea de mai jos sunt patru etichete (A, B, C, D) care indică spre anumite elemente de interfață. Descrie rolul fiecărui element de interfață indicat. (10 p)

2 Descrie un dispozitiv de intrare și unul de ieșire, la alegere. (20 p)

3 Asociază fiecărei extensii de pe coloana din stânga tipul de fișier potrivit. (20 p)

Extensie
jpg
mp3
doc
avi

Tip fișier
film
document
imagine
muzică
fișier executabil

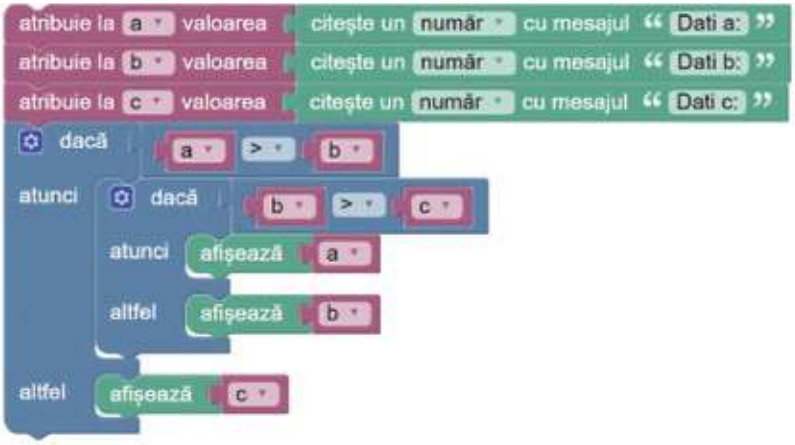
4 George are un pahar cu suc și o cană care conține apă. Descrie pașii pe care-i face George pentru a muta apa în pahar și sucul în cană. (10 p)

5 Evaluează expresia matematică: (9/4+9%4) *4+53/7. (10 p)

6 Determină ce afișează secvența de mai jos pentru: (20 p)

a) a = 9, b = 7, c = 8;

b) a = 2, b = 2, c = 6.



INTERNET

2

1.3.

Protecția datelor personale pe Internet

Amintește-ți!

1 **Lucrați în pereche.** 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 „siguranța online pentru copii”. Citește 2-3 dintre articolele găsite pe prima pagină în motorul de căutare și scrie ideile comune.

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.

Datele sau informațiile cu ajutorul cărora o persoană poate fi identificată direct sau indirect se numesc **date personale**. Datele personale conțin informații valoroase și pot fi utilizate în moduri negative, cum ar fi furtul de identitate, fraudă sau hărțuire online (cyberbullying).

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 etc.

Exemplu: Afirmația „Un elev din orașul București...” conține 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 ca fiind reprezentarea sa în spațiul virtual (suma caracteristicilor, comportamentelor, acțiunilor pe care o persoană le afișează în lumea digitală etc.). De obicei este **un cont protejat de o parolă** pe o rețea de socializare, joc video, mijloc de comunicare pe Internet.

Dacă ne gândim la rețelele sociale, *identitatea virtuală* are rolul unei măști, fiecare utilizator putând proiecta o imagine idealizată a sa.

Identitatea virtuală se poate referi, de asemenea, la urma sau amprenta digitală pe care o lasă o persoană prin activitățile sale online. **Exemplu:** căutările, postările din social media etc.

Pentru a-ți proteja prezența online, este nevoie să folosești parole puternice. Iată câteva sfaturi de urmat:

- **Creează parole lungi**, deoarece parolele lungi sunt mai greu de ghicit.

- **Evită cuvintele ușor de ghicit**, cum ar fi numele tău, data nașterii sau cuvinte comune precum „parolă”. Poți folosi o combinație de litere majuscule și minuscule, numere și simboluri.
- **Creează parole după o propoziție sau frază**. De exemplu: Din propoziția: „Ana are 5 mere si 7 pere.” se poate obține parola Aa_5 ms_7 p, 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.
- **Nu folosi aceeași parolă pentru mai multe conturi.** Este indicat să ai o parolă unică pentru fiecare dintre conturile tale.
- Schimbă periodic parola conturilor importante.

Exersează!

3. 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? Ce poți spune despre identitatea virtuală a celebrității respective? Dar a ta?

4. Realizează următoarele căutări pe Internet: „deep fake”, „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? Ce ar trebui să faci, dacă ai găsi pe Internet o imagine cu tine modificată?

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

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

Portofoliu

7. Creează o parolă puternică ținând cont de regulile învățate, apoi:
- Scrie strategia pe care ai folosit-o pentru crearea parolei tale.
- Explică în scris, în 2-3 propoziții, de ce este important să ai o parolă puternică.
- Caută pe Internet imagini, postere prin care să arăți riscurile asociate cu parolele slabe sau ușor de ghicit.

Autoevaluare

Verifică dacă:
- Ai scris caracteristicile unei parole puternice.
- Ai scris clar și complet strategia folosită pentru crearea parolei tale.
- Ai explicat în scris, în 2-3 propoziții, de ce este important să ai o parolă puternică.
- Ai găsit pe Internet imagini sau postere prin care să arăți riscurile asociate cu parolele slabe sau ușor de ghicit.

Organizarea portofoliului

Accesează manualul digital pentru a afla cum să îți organizezi portofoliul.

Amintește-ți!

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

Descoperă!

9 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, 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 minimul 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, efectuează pașii:

a) repornește calculatorul respectiv;

b) pornește browser-ul în *modul incognito* (apeși Ctrl+Shift+N în Chrome sau Edge);

c) utilizează browser-ul pentru scopul propus;

d) la final, repornește calculatorul.

- Nu folosi rețele Wi-Fi publice pentru a accesa informații sensibile de identificare personală (**Exemplu:** date bancare).

Raportează orice activitate suspectă sau încercare de furt de identitate către administratorii site-urilor accesate și adulților în care ai încredere.

Exersează!

10 Caută pe Internet și află „de ce este importantă securitatea cibernetică”.

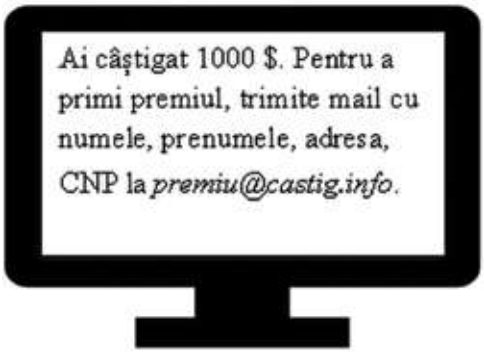
11 Caută pe Internet informații despre cât valorează datele tale cu caracter personal. O căutare în limba engleză ar aduce mai multe informații față de o căutare în limba română. (**Exemplu** de căutare: “The Value of Your Data”).

12 **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.

13 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?



Informează-te!

General **D**ata **P**rotection **R**egulation (GDPR) reprezintă Regulamentul privind Protecția Datelor Personale adoptat de Parlamentul European. GDPR este un pas important în domeniul protecției vieții private a cetățenilor europeni împotriva prelucrării abuzive a datelor personale ale acestora.

◉ O persoană are dreptul:

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

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 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.

Pentru persoanele sub 16 ani este necesar acordul părinților/tutorilor pentru prelucrarea datelor personale ale acestora.

Măsuri de siguranță în utilizarea Internetului. Utilizarea soluțiilor de securitate

Amintește-ți!

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

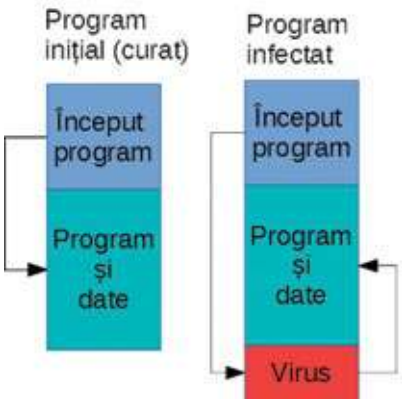
Descoperă!

2 **Lucrați în echipe.** Împreună cu 4 colegi, construiește o listă cu tipuri de programe care pot cauza probleme calculatorului. Scrieți în dreptul fiecărui tip de program ce știți despre el și cum funcționează.

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.

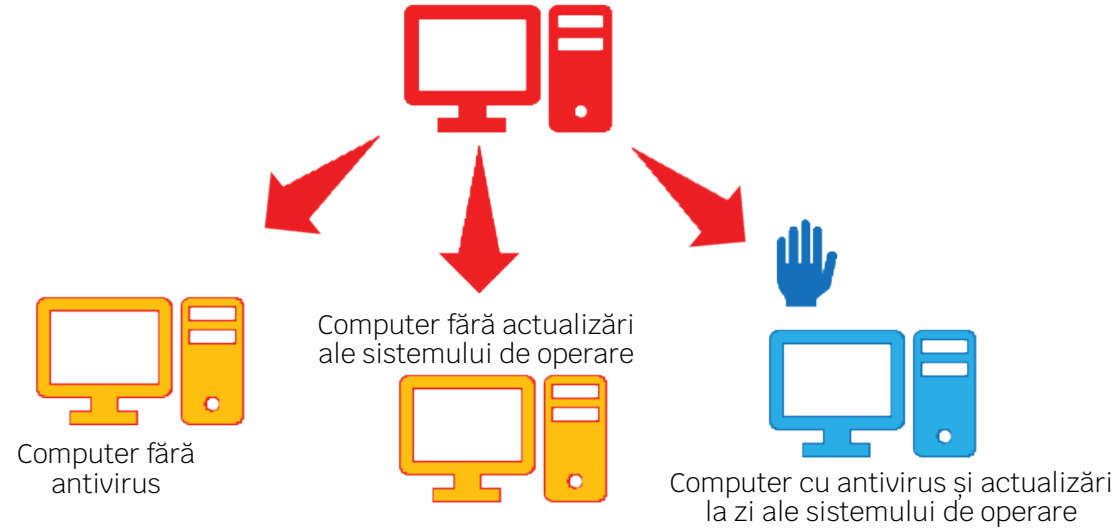


Exemple de programe malware: viruși, viermi, cai troieni, spyware, adware și alte programe rău intenționate.

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, 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, hard disk-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.

e) **Adware** este o aplicație care adaugă/aduce reclame pe computerul tău.

f) **Ransomware** este un tip de malware care blochează accesul *victimei* 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, oferă 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.

5 Asociază fiecărui program descris în coloana din stânga un tip de malware aflat pe coloana din dreapta.

Descriere	Tip malware
criptează pozele de pe computer și cere bani pentru a le decripta	virus
se transmite prin rețea	vierme
raportează undeva ce faci pe calculator	cal troian
îți aduce reclame pe calculator	spyware
promite că „sparge” un joc să-l folosești gratis, dar de fapt instalează un virus	adware
	ransomware

Descoperă!

6 **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?

7 Caută pe Internet „inginerie socială”. La ce se referă? Din ce ai învățat până acum unde se aplică ingineria socială?

IMPORTANT

Un program antivirus are rolul de a „vâna” 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.

O soluție de securitate completă ar trebui să ofere:

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

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

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 comportament asemănător cu cel al programelor malware.

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

Exersează!

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

Portofoliu

9 **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. **Exemplu de căutare: “best security software”**

10 **Lucrați în pereche.** 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?

11 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 (cyberweapon). Stuxnet este numele unui malware despre care se crede că a fost creat pentru a afecta programul nuclear al unei țări. 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.