PROIECT

La informatică

“SECURITATEA CIBERNETICĂ”

CLASA a XI-a “C”

Au realizat:
Apostol Cristina
Cazacu Felicia

SLIDE 1: Securitatea cibernetica

SLIDE 2: Scopul acestui proiect este de a ajuta elevii să conştientizeze riscurile navigării pe internet si metodele de precauție.

SLIDE 3: OBIECTIVE

1. Cunoaşterea regulilor de navigare pe internet.

2. Cunoşterea noțiunii de securitate cibernetică.

3. Cunoaşterea metodelor de evitarea a harțuirii pe internet.

4. Dezvoltarea aptitudinii de a recunoaste un calculator virusat.

5. Cunoasterea metodelor de securitate a informatiilor si aplicatiilor.

6. Cunoasterea metodeor de evitare a spam-urilo, phising-ului, spyware si keyloggers.

Filmulet

SLIDE 4: CE ESTE SECURITATEA CIBERNETICĂ?

Securitatea cibernetică poate fi definită ca un sistem eficient de protecţie a siguranţei personale într-un spaţiu informaţional de tehnologii înalte, spaţiul virtual.

SLIDE 5: Cum să ne păstram identitatea, să ne asigurăm respectarea drepturilor si libertaţilor fundamentale?

SLIDE 6-16: 10 reguli pentru o navigare sigură şi placută pe Internet!

1.Stabileste împreuna cu parintii tai regulile de folosire a calculatorului si a Internetului.

2.Nu da nici unei persoane întalnite pe Internet informatii personale despre tine sau familia ta.

3.Parolele sunt secrete si îti apartin.

4.Daca vrei sa te întalnesti fata în fata cu persoanele cunoscute pe Internet sau de la care ai primit mesaje pe telefonul mobil, anunta-ti parintii pentru a te însoti, preferabil într-un loc public.

5.Posteaza cu mare grija fotografii cu tine sau cu familia ta!

6.Nu tot ceea ce citesti sau vezi pe Internet este adevarat.

7.Nu raspunde la mesajele care te supara sau care contin cuvinte sau imagini nepotrivite!

8.Da dovada de respect, chiar daca nu-i cunosti pe cei cu care comunici.

9.Cumpararea produselor pe Internet este permisa doar parintilor.

10.Poti oricand sa te opresti din navigarea pe Internet sau sa refuzi sa continui discutiile pe chat, daca s-a întamplat ceva care nu ti-a placut, te-a speriat sau, pur si simplu, nu ai înteles.

SLIDE 17: Nerespectarea regulilor -> Hartuirea in mediul online

SLIDE 18: Cyber Bullying - este un termen englezesc ce nu poate fi tradus în mod direct în limba română, însă acesta s-ar asocia cu termenii de intimidare, terorizare, brutalizare şi hărţuire în mediul on-line.

În cazul în care prin **hărţuirea online** se recurge la acţiuni de şantaj, ameninţări sau încălcarea inviolabilităţii vieţii personale, **victima ar trebui să depună o plângere penală.**

SLIDE 19: Înainte de a apela la instrumentele legale, ar fi bine să distingem acele acţiuni şi manifestări care cad sub incidenţa acestui fenomen, şi anume:

bârfa: emiterea în mediul online a unor declaraţii speculative ce denigrează o persoană sau instigă un grup de persoane în a adopta un comportament restrictiv;

urmărirea online: hărţuirea intimidantă cu scopul de a aduce conflictul şi în viaţa reală. De exemplu, de a solicita întrevederi în viaţa reală prin a ameninţa cu răfuială fizică;

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 protecţia anonimatului, agresorii îşi ameninţă victimele sau, aleatoriu, folosesc identitatea victimei în raport cu alte persoane;

Aceste acţiuni constituie nişte abuzuri în adresa persoanei. Dacă hărţuirea se realizează pe o **reţea de socializare** (*facebook, odnoklassniki, instagram, twitter* etc.), trebuie să cunoaşteţi că aceste platforme au opţiuni de a raporta comentariile abuzive, hărţuirea sau aşa numitul spam. A nu se ignora această opţiune ce vi se pune la dispoziţie, ea poate duce la închiderea contului de pe care sunteţi molestat.

SLIDE 20: Comunicarea pe reţelele de socializare

Rețelele de socializare pot reprezenta cel mai bun prieten sau cel mai groaznic inamic.

Efectele negative ale reţelelor de socializare:

Poate exista pericolul ca oamenii să fie tentaţi să petreacă din ce în ce mai mult timp în faţa calculatorului şi din ce în ce mai puţin făcând mişcare sau întâlnindu-se cu prietenii.

SLIDE 21: Facebook şi Odnoklassniki rămân în continuare cele mai populare reţele de socializare din Republica Moldova, cea din urmă înregistrând însă o micşorare dramatică.

SLIDE 22: Facebook este un site web de tip rețea de socializare din Internet, creat de către Mark Zuckerberg în anul 2004 pentru a oferi posibilitatea de a contacta persoane apropiate, dar şi persoane încă necunoscute.

Creat inițial la Harvard, SUA, facebook era la origine o rețea socială cu circuit inchis pentru studenții acestei universități; ulterior ea s-a deschis şi altor universități americane. La început verificarea apartenenței la universitate se făcea prin adresa de poştă electronică (e-mail) a studentului, dar începând din septembrie 2006 rețeaua este deschisă tuturor. Imediat rețeaua facebook a devenit foarte populară dar şi controversată, fiind interzisă în câteva țări din Orientul Mijlociu. De asemenea, prin intermediul acestei rețele au fost provocate şi coordonate unele manifestații protestatare din Republica Moldova şi Iran.

SLIDEUL 23: Reputaţia Online

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.

Copiii si adolescentii care utilizeaza site-urile de socializare nu sunt constienti de faptul ca o fotografie "share"-uita pe un site de socializare ramane in baza de date, chiar daca a fost stearsa. Acelasi lucru se intampla si in cazul informatiilor de natura personala. O poza postata in adolescenta pe un site de socializare poate sa-i distruga cariera la maturitate, daca este gasita de un angajator.

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.

SLIDE 24-31: Cum recunoaştem un calculator virusat?

7 semne:

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.
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. 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. *“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.
7. *“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.

SLIDE 32: Cum să te fereşti de viruşi, viermi şi troieni?

Cele mai întâlnite tipuri de ameninţări informatice

•Viruşi: viruşii informatici sunt programe care se autocopiază pe sistemul compromis, fără ştirea utilizatorului. Virusul va infecta astfel componente ale sistemului de operare sau alte programe informatice.
•Viermi: programe care se pot auto-replica. Acestea folosesc reţeaua de calculatoare pentru a-şi trimite propriile copii în alte noduri (calculatoare din reţea), reuşind să facă acest lucru fără intervenţia vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie ataşat la un program existent.
Viermii provoacă daune reţelei, chiar şi prin simplul fapt că ocupă bandă, în timp ce viruşii corup sau modifică aproape întotdeauna fişiere de pe computerul ţintă.
•Troieni: aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidenţiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat.

Pentru a asigura integritatea calculatorului şi a datelor personale, vă recomandăm respectarea următoarelor reguli:
•Instalaţi o soluţie de securitate ce oferă cel puţin protecţie
•Aveţi în vedere ca soluţia de securitate instalată să fie permanent actualizată
•Nu deschideţi ataşamente şi nu accesaţi link-urile ce vin din partea unor expeditori necunoscuţi. Dacă este absolut necesară deschiderea unui ataşament, se recomandă ca acestasă fie descărcat şi scanat cu soluţia antivirus instalată pe calculator
•Nu deschideţi ataşamentele şi nu daţi click pe link-urile din mesajele spam
•Nu folosiţi niciodată calculatoare publice pentru a efectua tranzacţii bancare, sau pentru alte tipuri deachiziţii online. Aceste calculatoare ar putea conţine programe care înregistrează datele personale, precum troienii bancari
•Evitaţi să faceţi shopping online atunci când sunteţi conectaţi la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenelesau mall-uri. De obicei, informaţiile

schimbate între dumneavoastră şi magazinul online, nu sunt criptate, şi pot fi interceptate uşor de către un atacator
•În cazul în care vă conectaţi la hotspot-uri publice nesecurizate, utilizaţi o aplicaţie firewall care să filtreze accesul din exterior
Nu trimiteţi niciodată parolele dumneavoastră de cont prin e-mail sau prin ataşamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informaţii, având în vedere că ar trebui să le aibă deja.

SLIDE 33: Protecţie antivirus

Cel mai bun antivirus gratuit în 2018
Piaţa este plină de soluţii antivirus care îţi pot oferi tot ce ai nevoie pentru a păstra un sistem Windows curat şi fără infecţii dăunătoare. Ai de ales între mai multe soluţii comerciale pentru care va trebui să achiziţionezi o licenţă sau poţi alege o soluţie antivirus gratuită. Toate soluțiile de securitate gratuite pot oferi unui utilizator casnic protecţia necesară sistemului prevenind infiltrarea fişierelor dăunătoare.

SLIDE 34: Cel mai bun antivirus gratuit în 2018

Avira Free Security Suite
Una dintre celebrităţile de pe piaţa produselor de securitate gratuite, Avira rămâne unul dintre produsele cu detecţie foarte bună şi un pachet suficient de bogat de opţiuni.
Avast Free Antivirus
Una dintre cele mai populare opţiuni de foarte mulţi ani, Avast este apreciat pentru rata bună de detecţie şi pentru opţiunile foarte bogate pentru un produs gratuit. Pe lângă opţiunile standard de scanare bazată pe semnături, Avast mai oferă un modul care afişează în browser note de încredere pentru site-uri, un sistem de blocare a tentativele de phising prin scanarea mesajelor de email şi un scanner pentru vulnerabilităţile locale ale sistemului de operare şi alte unor aplicaţii.

SLIDE 35: Securitatea informaţiilor

Alegeţi o parolă pentru contul dumneavoastră care să nu fie uşor de ghicit de către un alt utilizator sau program. În acest sens, evitaţi parolele generice, precum ”123456789” sau ”parola” sau o parolă identică cu numele de utilizator;
Asiguraţi-vă că ştiţi pe cine urmăriţi şi pe cine adăugaţi drept prieten
Evitaţi să accesaţi link-urile împărtăşite de către alţi utilizatori;
Evitaţi să faceţi publice informaţii personale, precum ziua de naştere,adresa de

email sau adresa fizică;
Atunci când împărtăşiţi poze, asiguraţi-vă că o faceţi doar cu persoanele cunoscute
Nu dezvăluiţi niciodată informaţii referitoare la perioadele în care părăsiţi locuinţa (mesaje precum: ”plec la mare tot weekend-ul; ”sunt singur acasă” trebuie evitate)
Utilizaţi o soluţie de securitate specializată, care să scaneze mesajele şi comentariile, şi care să verifice nivelul de securitate al informaţiilor confidenţiale;

SLIDE 36: Securitatea aplicaţiilor (software)

Soluţiile software de securitate a sistemelor sunt instrumente cu rol în detectarea şi eliminarea viruşilor, lucrând activ la îmbunătăţirea principiilor de apărare a computerelor. Cele mai importante module ale sistemelor de securitate sunt cele de scanare, diagnosticare şi protejare împotriva programelor de tip spion, viruşi, cai troieni sau multe altele.

SLIDE 37: Securitatea in reţelele WI-FI

Tratează orice reţea necunoscută cu mare grijă Infractorii cibernetici pot să creeze propriile capcane: de exemplu, o reţea Wi-Fi publică, prin intermediul căreia să încerce să obţină datele utilizatorilor. Denumirea acesteia poate să fie similară cu a unui loc cunoscut care oferă Wi-Fi, tocmai pentru a-i atrage pe cei mai puţin atenţi la astfel de detalii.

Evită, pe cât posibil, reţelele care solicită acces la date personale pentru a putea naviga pe Internet – Unele hoteluri şi mai ales aeroporturile oferă utilizatorilor opţiunea de a se conecta la reţelele lor fără parolă, înregistrându-se în schimb cu o adresă de e-mail sau cu un cont de pe o reţea de socializare. Pentru a se conecta la Internet, utilizatorii sunt anunţaţi că le vor fi accesate profilul public şi contactele. Recomandarea mea este să eviţi astfel de conexiuni.

SLIDE 38: Ce sunt cookie-urile şi ce fac ele?

Atunci când navighezi pe internet, întâlneşti des termenul de *"cookie"*. Multe saituri web te informează în legătură cu utilizarea lor şi îţi cer permisiunea de a le folosi.
Chiar dacă ştii că aceste cookie-uri nu sunt nişte prăjituri, poate nu ştii ce sunt cu adevărat şi care este rolul lor pe internet.
Cookie-urile sunt fişiere care stochează informaţii despre tine, browser-ul tău web şi comportamentul tău pe internet. Ele sunt fişiere foarte mici păstrate pe PC-ul sau dispozitivul tău, ce pot fi folosite de saiturile sau de aplicaţiile web pentru a ajusta

experienţa ta online.

SLIDE 39: Spam-urile

SPAM – ul este un mesaj de posta electronica (e-mail) nesolicitat. In cele mai multe cazuri sunt mesaje comericiale (oferte, promotii, comentarii pe siteuri de stiri, forumuri etc.) si intenitia expeditorului este de a beneficia de publicitate la costuri foarte mici.

Momentan nu exista mijloace de a bloca definitiv spam-ul.

Mai grav, exista mesaje spam care pot aduce daune serioase destinatarilor:
– virusii continuti in mesajele electronice pot deteriora sistemul de calcul, inclusiv calculatoarele din reteaua locala;
– e-mail phishing, mai exact mesaje care par trimise de o organizatie legitima, cu scopul de a obtine in mod fraudulos informatii cu caracter personal, cum ar fi parole sau detalii ale cardului de credit;
– oferirea de produse sau afaceri fabuloase dar in realitate false, cu scopul a va atrage in diverse capcane sau pentru a vizita anumite site-uri;
– mesaje de amenintare, hartuire, blocarea comunicarii serverelor de e-mail ;
– mesaje sub forma de comentarii, de obicei in alta limba fata de cea in care este setata siteul ; mesaje fictive, care au in cadrul lor un link (o adresa web) .

SLIDE 40: Spyware=Programele spion

Spyware: o categorie de software, ataşate de obicei la programe gratuite (jocuri, programe de schimbat fişiere, programe de video chat 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, ş.a.m.d.) şi le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

SLIDE 41: Keyloggers

Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură şi salvează aceste date într-un fişier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanță, predeterminată. De asemenea, poate captura capturi de ecran şi utiliza alte tehnici pentru a urmări activitatea utilizatorului. Un keylogger poate cauza pierderea parolelor, date de autentificare, şi alte informații similare.

Un **keylogger** este capabil de inițierea următoarelor activități:

- Să înregistreze intrările de taste de pe tastatură.
- Să obțină capturi de ecran cu activitatea utilizatorului de pe internet la intervale de timp predeterminate.
- Să urmărească activitatea utilizatorului prin înregistrarea titlurilor ferestrelor, numele aplicațiilor lansate, şi alte informații specifice.

- Să monitorizeze activitatea online a utilizatorului înregistrând adresele website-urilor vizitate, cuvintele cheie introduse şi alte date similare.
- Să înregistreze nume de autentificare, detalii a unor diverse conturi, numerele cardurilor de credit şi parole.
- Să captureze conversațiile chat-urilor online de pe instant messengers.
- Să obțină copii neautorizate a emailurilor primite şi trimise.
- Să salveze toate datele colectate într-un fişier de pe hard disk, şi să trimită acest fişier unei adrese de email.
- Să îşi complice detectarea şi eliminarea.

Keyloggerii nu pot fi comparați cu viruşii normali. Ei nu se răspândesc ca aceste amenințări, şi în majoritatea cazurilor, trebuie instalați ca orice alt software.

SLIDE 42: Adresele de e-mail pentru 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 foloseşti deja. De exemplu, e posibil ca cineva care practică phishing să îți trimită un e-mail care arată ca şi cum a fost trimis de banca ta, astfel încât să îi transmiți informaţii despre contul tău bancar.

SLIDE 43: E-mailurile sau site-urile de tip phishing pot să îți ceară:

- nume de utilizator şi 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 naşterii.

Important: Google sau Gmail nu îți va solicita niciodată să transmiți aceste informaţii prin e-mail.

SLIDE 44: Evită atacurile de phishing;

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

1.nu da clic pe niciun link şi nu transmite niciun fel de informaţii personale până când confirmi că e-mailul este real.

2.dacă expeditorul are o adresă Gmail, raportează abuzul din Gmail la Google.

SLIDE 45: Concluzii si opinii