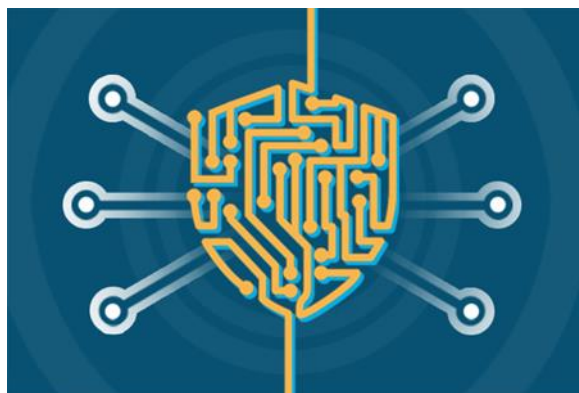


Securitatea cibernetica



Au elaborat:
Gorgan Bogdan
Bondari Sofia

Chişinău 2018

Securitatea cibernetică

(În toate slide-urile vom face referire la anexe, la fel vom improviza și vom asculta/comenta opiniile copiilor)

Prezentarea

Bogdan

În fiecare zi, suntem expuși, atât acasă cât și la locul de muncă, la amenințări ce își au originea în spațiul virtual. În majoritatea cazurilor nici măcar nu suntem conștienți de acest lucru, sau dacă-l realizăm, nu reacționăm la aceste amenințări într-o manieră adecvată. În media apar zilnic articole referitoare la incidente de securitate și la impactul pe care acestea îl au asupra noastră, ca indivizi sau organizații deopotrivă.

Aceste incidente relatate sunt de fapt doar vârful iceberg-ului, în realitate fiind cu mult mai expuși decât credem noi că suntem având în vedere că, din nefericire, riscurile asociate mediului virtual sunt în continuă creștere.

Sofia

Spatiul virtual se bazează pe internet, nu copii? Cine cunoaște definiția internetului?

Slide 1 Bogdan dirijează

Prin Internet se înțelege o rețea globală, compusă din sisteme de calculatoare interconectate și servicii computerizate, care permite utilizatorului, indiferent de locația sa geografică, să acceseze informația aflată oriunde în rețea.

Cu definiția neam clarificat, însă scopul nostru de astăzi este de a face navigarea pe internet mai sigură, de aceea

Slide 4 dirijează Sofia

- utilizează ultima versiune de browser;
- având în vedere că cele mai multe aplicații malițioase afectează Microsoft Internet Explorer (utilizat de peste 50% dintre utilizatori), orientează-te și spre alte tipuri de browser (ex. Google Chrome, Opera, Firefox, Safari etc.), mai ales când accesezi pagini web posibil nesigure;
- verifică secțiunea de contact a site-urilor web (adresă, număr de telefon, e-mail);
- atenție la ce plugin-uri instalezi, de multe ori acestea vin însoțite de un software malițios;
- nu apăsa pe link-urile din cadrul ferestrelor de tip pop-up;
- verifică existența „https://” în partea de început a adresei web, înainte de a introduce informații personale.

Mai cunoaște cineva alte reguli de navigare pe internet?

Bogdan

Internetul, cu totii avem acces la el, datorita dispozitivelor mobile, calculatoarelor, insa in urma unei utilizari excesive, sistemul de operare, soft-ul isi reduce din viteza de aceea:

Slide 6 dirijeaza Bogdan

Daca nu mai ai nevoie de un anumit soft, dezinstalează-l! Astfel, vor fi mai ușor de urmărit aplicațiile care necesită a fi actualizate, iar de multe ori acest lucru va permite o executare rapidă a sarcinilor de către calculator (sunt frecvente aplicațiile de mici dimensiuni și add-on-urile care se instalează împreună cu diverse softuri și care pornesc odată cu computerul, ocupând memoria acestuia și afectându-i performanțele).

Sofia

Pe langa aplicatiile care ne stopeaza din performanta dispozitivelor, se mai regasesc si programe malware, care la fel ne pot afecta dispozitivele, pentru a ne proteja de ele, este necesar un antivirus. Cum credeti, ce este antivirusul?

Slide 7 dirijeaza Sofia

Un element important în configurația de securitate cibernetică este **antivirusul**. Acesta este un program informatic conceput să detecteze, să prevină și să elimine instalarea oricăror forme de malware (virusi, troieni, adware, spyware etc.) pe sistemele de calcul. Actualizarea acestuia este deosebit de importantă pentru a putea face față celor mai noi (versiuni ale unor) programe malițioase.

Bogdan

Virusi, troieni, cine cunoaste care este diferenta?

Slide 8/9 dirijeaza Bogdan

*Un exemplu de malware este **troianul** (trojan horse), a cărui denumire provine din mitologia greacă. Acest tip de program pare a avea o funcție utilă, legitimă, dar deține și una ascunsă, potențial malițioasă, care scapă mecanismelor de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată rulat, programul poate iniția activități malițioase, precum sustragerea de informații, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanță la sistemul infectat.*

- *virusul informatic: program care se poate autoreplica în cadrul unui sistem și propaga în alte calculatoare din rețea fără știința utilizatorului. Acesta poate afecta negativ funcționalitatea, integritatea, disponibilitatea sistemului sau a datelor conținute de acesta;*
- *viermele informatic: un malware ce dispune de capacitatea de a se autoreplica și propaga într-o rețea de calculatoare și dincolo de aceasta (alte sisteme sau rețele), folosind resursele rețelei, fără a se atașa unui alt program sau proces.*

Sofia

Multi dintre voi petrec ceva timp în fața calculatorului, cine a încercat să comande ceva de pe un web-shop?

Pentru viitor și părinți, vă recomandăm un set de reguli:

Slide 11 dirijează Sofia

- cumpărăturile să se realizeze doar de pe site-uri web recunoscute și securizate;
- *contravaloarea unui produs achiziționat nu trebuie transmisă înainte de verificarea existenței și funcționalității acestuia, prin folosirea unui serviciu de escrow recunoscut;*
- *nu se folosesc servicii financiare de transfer rapid WesternUnion sau MoneyGram înainte de recepționarea produsului achiziționat, mai ales când această operațiune este solicitată de vânzător;*
- *verificarea site-ului web (există magazine online fictive care au ca scop atragerea de clienți și reținerea datelor bancare ale acestora).*
- *respectarea unei simple metode de verificare, respectiv compararea link-urilor receptate prin mesaje de tip „spam” cu cele legitime ale instituțiilor bancare.*

Bogdan

Multi dintre voi au deja propriile telefoane mobile, ce reguli, restricții cunoașteți?

Slide 13 dirijează Bogdan

- nu instalează decât aplicații necesare și verifică la ce date are acces înainte de a le descărca (poziționare geografică, contacte, apeluri telefonice etc);
- în plus față de codul PIN care protejează cartela SIM, folosește o parolă sau un cod pentru a securiza accesul la telefon;
- instalează software-uri de securitate special concepute pentru dispozitive mobile; acestea pot detecta și elimina virusii, bloca mesajele spam multimedia sau alte amenințări cibernetice;
- criptează memoria internă a telefonului sau tabletei dacă acestea conțin informații sensibile; dacă dispozitivul mobil este pierdut, persoana care intră în posesia acestuia nu va putea accesa datele respective;
- realizează salvări periodice ale datelor pe un suport extern pentru a le putea restaura;
- nu permite salvarea parolelor, în special pentru aplicațiile bancare sau cele puse la dispoziție de furnizorii de servicii pentru gestionarea consumului și plata facturilor;
- aplică, periodic, actualizările de securitate furnizate de producătorii software-urilor instalate pe dispozitivele mobile.

Sofia

Pe smartphone, cel mai probabil fie navigate pe rețele de socializare, fie va jucați în ceva jocuri, ce jocuri preferați (Bogdan va sculta ce jocuri iubesc copiii, le va acorda ceva sfaturi) dar Facebook totuși au? Sau Odnoklasniki?? Eu cred că preferați Instagramul... Toate sunt bune, dar vă protejați datele personale? Este destul de important, deci, uitați câteva sfaturi:

Slide 15 dirijează Sofia

- evitarea publicării informațiilor personale, precum ziua de naștere, adresa de e-mail sau adresa fizică;
- atunci când postezi fotografii, asigură-te că o faci doar cu persoanele cunoscute, iar acestea nu surprind locații exacte (ex.: adrese de domiciliu);
- nu dezvălui niciodată informații referitoare la perioadele în care părăsiți locuința;
- în cazul în care ai copii care au voie să folosească calculatorul familiei, nu le oferi privilegii de administrator asupra respectivului computer;
- instalează o soluție antivirus cu control parental, filtru de conținut și filtru pentru rețelele sociale. Dată fiind ponderea conținutului pornografic și a violenței online, este de datoria părinților să își păstreze copilul în siguranță;
- informează-te despre cyber-bullying și poartă discuții cu copilul tău.

Slide 16 dirijează Bogdan

Utilizatorul reprezintă primul zid de apărare împotriva amenințărilor din spatele monitorului, primul și uneori ultimul în identificarea pericolelor și, în funcție de caz, semnalarea acestora unui matur. Utilizatorul este, totodată, cel care poate preveni crearea unor daune atât pentru sine, cât și pentru mediul inconjurător.

Pentru a evita o scurgere de date, copii, vă țineți minte parolele, la cine e numărul de telefon? Data luna anul nașterii? Când ajungeți acasă le schimbați imediat, sunt destul de simple, nu sunteți în siguranță, de aceea :

Slide 17 dirijează Bogdan

- utilizează ID-uri și parole unice și nu le comunica altor utilizatori;
- lungimea parolei și complexitatea acesteia trebuie alese astfel încât să fie dificil de ghicit dar ușor de ținut minte;
- schimbarea periodică a parolelor (la un interval de 1-3 luni); 3 utilizarea unor parole diferite, pentru aplicații diferite;
- utilizarea unor metode multiple de autentificare (PIN, amprentă, mesaje alertă, etc);
- evitarea utilizării unor parole similare acasă și la locul de muncă.

Sofia Concluzie

Intrun final doresc sa va spun ca aceasta prezentare nu este un ghid sigur pentru a fi atotstiutori despre navigarea voastra pe internet, dar sper ca a contribuit la dezvoltarea cunostintelor despre acest domeniu, si va schimbat unele viziuni asupra navigarii pe internet, sunteti de acord? Cine are ceva intrebari?