**Slide 2**

In cadrul prezentarii de azi, vom vorbi despre:

Avantajele și dezavantajele/riscurile navigării pe internet, ce este securitatea cibernetică, tipurile acesteia, tipurile de amenințări, de unde provin si despre importanța securității cibernetice.

**Slide 3**

**Internetul**oferă omului modern o mulţime de avantaje, care îi uşurează sau îi îmbunătăţesc viaţa, fie îl ajută să economisească timp, bani, fie îi oferă modalităţi de a-şi petrece timpul simţindu-se mai bine (cel puţin pe moment) etc. Din păcate, însă, utilizarea internetului prezintă şi anumite probleme, pericole, pe care este foarte bine ca oricine care accesează internetul să le cunoască, să le conştientizeze, şi să se ferească de ele.

**AVANTAJELE INTERNETULUI**

**Acces foarte rapid şi facil** (de regulă) la toate avantajele internetului.Internetul oferă informaţii din toate domeniile (politică, administraţie, sport, agricultură, vreme, informaţii juridice – legi, hotărâri etc.) prezentate sub tot felul de forme: ştiri, articole, imagini, videoclipuri etc.

**Comunicare** cu instituţiile publice şi companii private (găsirea numerelor de telefon şi fax, posibilitate de comunicare prin mail – poştă electronică etc); **socializare** prin: mail, siteuri de socializare, messenger, skype etc; există posibilitatea de a vorbi ca la telefon, gratuit;  comunicare cu rude şi prieteni, comunicare cu colegi de şcoală/facultate/serviciu, comunicare cu profesori etc.

**Instruire.**Acces la cursuri online(unele gratuite), şi alte informaţii/documente utile în pregătirea profesională şi carieră (valabil în perioada şcolii, liceului, facultăţii, serviciului şi tot restul vieţii). Posibilitatea de a învăţa limbi străine gratuit

**Comerţ electronic.** Posibilitatea de a găsi şi cumpăra produse de care ai nevoie, la cel mai mic preţ de pe piaţă. Posibilitatea de a vinde diferite produse.

**Publicitate.**Posibilitatea de a da, gratuit, anunţuri referitoare la orice: cumpărări-vânzări, matrimoniale, evenimente, proteste etc.

**8. Economie de timp**.Internetul îţi poate asigura o foarte mare economie de timp. În loc să pierzi timpul (în diferite moduri), pentru a obţine ceva/a rezolva ceva, prin intermediul internetului foarte multe probleme se rezolvă mult mai rapid.

**Slide 4**

**DEZAVANTAJELE  INTERNETULUI** 

**Accesul la internet este permis oricui,** indiferent de vârstă, indiferent de pricepere şi experienţă în domeniul informatic. Astfel, oricine poate intra pe internet, însă şi oricine poate dăuna internetului, în diferite moduri. Internetul este de cele mai multe ori ”poluat” de următoarele categorii de persoane: copii/tineri  incompetenţi care publică informaţii false; persoane de rea-credinţă care încearcă să manipuleze, prin publicarea de informaţii false.

**Calitatea şi veridicitatea** informaţiilor de pe internet **este nesigură**. Pentru că oricine are acces la internet, oricine poate posta informaţii pe internet, oricine poate spune neadevăruri, poate dezinforma, sau poate minţi.

**Informaţiile personale nu sunt în siguranţă** când folosim internetul. Această securitate a datelor personale pe care o promovează site-urile ce oferă, de exemplu, căsuţă de mail, este falsă. Adică, tot ce este în calculator este expus în momentul în care este conectat la internet.

**Infracţiunile / ilegalităţile / fraudele** / înșelătoriile care pot avea loc, şi care  pot afecta, legate de: tranzacţii bancare online, insalaciuni in domeniul economic, comertului electronic, al afacerilor etc.  Pe internet nu există siguranţă 100% legat de contul bancar sau de orice alte conturi online deţinute! Lipsa unei identităţi reale a colaboratorilor/partenerilor pe internet, creşte riscul de a fi minţit. . Internetul permite de asemenea ÎNCĂLCAREA DREPTURILOR DE AUTOR, COMERCIALIZAREA PRODUSELOR CONTRAFĂCUTE etc.

Problemele semnalate cel mai des vizează hărţuirea şi abuzul pe Internet sub toate formele sale – agresiunea verbală, calomnierea, furtul de date personale, infectarea calculatorului cu viruşi, dependenţa de calculatoretc.

**Slide 5**

Termenul Cybersecurity se referă la tehnologiile menite sa apere sistemele informatice și rețelele de acces neautorizat ,de hackeri si chiar de grupari teroriste. Internetul nu este doar sursa principală de informații, ci este și un mijloc prin care oamenii fac afaceri. Din această cauză, hackerii și infractorii cibernetici folosesc internetul ca instrument de răspândire a programelor malware și de atacuri cibernetice.

Cybersecurity își propune să protejeze computerele, rețelele și programele software de astfel de atacuri cibernetice.

**Slide 6**

Securitatea cibernetica se clasifică în mai multe tipuri:

**Slide 7**

# Securitatea informațiilor

Siguranța informațiilor vizează protejarea informațiilor personale ale utilizatorilor de accesul neautorizat, furtul de identitate. Aceasta protejează confidențialitatea datelor și a hardware-ului care manipulează, stochează și transmite aceste date/informatii. Exemple de securitate a informațiilor includ autentificarea utilizatorilor și criptografia.

**Slide 8**

#Securitatea retelei

Securitatea rețelei are scopul de a proteja gradul de utilizare, integritatea și securitatea unei rețele, componente asociate și informatii partajate în rețea. Atunci când o rețea este asigurată, amenințările potențiale sunt blocate de la introducerea sau răspândirea în acea rețea. Exemple de securitate în rețea includ programe antivirus și antispyware, firewall care blochează accesul neautorizat la o rețea și VPN-uri (rețele private virtuale) utilizate pentru acces securizat la distanță.

**Slide 9**

# Securitatea aplicatiilor

Soluția de securitate a aplicațiilor vizează protejarea aplicațiilor software de vulnerabilitățile care apar din cauza unor deficiențe în fazele de proiectare, dezvoltare, instalare, upgrade sau întreținere a aplicațiilor.

Diferitele tipuri de securitate a aplicațiilor, cum ar fi firewall-urile, programele antivirus, programele de criptare și alte dispozitive, pot ajuta la prevenirea accesului neautorizat

**Slide 10**

Există multe tipuri diferite de amenințări la adresa securității informatice.Voi vorbi despre cateva dintre ele.

**Slide 11**

Virusii sunt un tip de programe Malware special concepute pentru a provoca daune computerului victimelor.Virusul are capacitatea de a corupe fisierele si a fura informatii private cum ar fi detaliile cartii de credit ale utilizatorului si de a le trimite inapoi la hacker.

Furtul de identitate este un tip de amenințare la adresa securității cibernetice, care implică furtul informațiilor personale ale victimelor de pe site-urile de social media, cum ar fi Facebook sau Instagram.

Atacul de parola este un tip de amenințare împotriva securității cibernetice care implică încercarea hackerilor de a sparge parolele utilizatorului.

Spyware-ul, care este si el un tip de programa Malware, poate spiona comportamentul victimelor. Unele programe malware, cum ar fi keyloggerul, pot înregistra înregistrările de taste ale victimelor, inclusiv parolele, numerele PIN și detaliile cărților de credit.

Adware este un grup de malware care generează ferestre pop-up. Dacă un utilizator observă pe ecranul computerului mesaje ciudate de tip pop-up, este cel mai probabil supus unui atac adware. Principala intenție a adware-ului este să obțină permisiuni care le vor permite hackerilor să instaleze virusi in calculator.

Troienii(Trojans) sunt un tip de programe malware care se ascund ca programe inofensive si utile. Troienii pot provoca o varietate de activități rău intenționate pe computerul victimelor, inclusiv descărcarea de programe rău intenționate, ștergerea sau furtul de fișiere și furnizarea accesului neautorizat al hackerilor la computerul victimelor.

Ransomware este un grup de programe malware care blochează sau criptează computerul victimei și solicită plata pentru decriptarea calculatorului.Trebuie

de mentionat faptul ca hackerii solicita plata in valute virtuale cum ar fi BitCoin pentru a evita represiunea autoritatilor.

Unele programe rău intenționate, cum ar fi Browser Hijacker, redirecționează browserul victimelor către anumite site-uri web alese de hacker sau către un site care plătește hacker-ul pe baza numărului de accesări pe care le primește.

Adresele de e-mail de tip phishing sunt destinate să fure informații privitoare la utilizatori, cum ar fi datele de conectare ale utilizatorilor și numerele cărților de credit.Intrucat atacurile de tip phishing folosesc emailuri sau programe aparent inofensive, este dificil pentru utilizatori sa le depisteze.

**Slide 12**

Există numeroase moduri prin care aceste amenintari cibernetice infectează computerul nostru, printre cele mai frecvent utilizate sunt

**Slide 13**

# Site-urile suspecte

Hackerii folosesc software și site-uri aparent legitime pentru a atrage utilizatorii în descărcarea de programe malware. Momeala de bani sau jocuri gratis atrage unii utilizatori. Chiar și oamenii care nu vizitează aceste site-uri suspecte sunt predispuși la faptul ca aceste site-uri/link-uri ispititoare sa fie ascunse in calculatorul lor.

Malware-ul care provine de pe aceste site-uri poate călători prin internet ajungand in calculatorul unui utilizator nevinovat redirectionand experiența lor de navigare pe aceste site-uri.

**Slide 14**

# Partajarea/distribuirea fisierelor prin reteaua peer to peer

Rețeaua Peer-to-peer permite [calculatoarelor](https://ro.wikipedia.org/wiki/Calculator" \o "Calculator) să se conecteze în mod direct unul la celălalt, pentru schimb de [fișiere](https://ro.wikipedia.org/wiki/Fi%C8%99ier" \o "Fișier) ([partajare de fișiere](https://ro.wikipedia.org/wiki/Partajare_de_fi%C8%99iere" \o "Partajare de fișiere)) în comun. Nu există o limită teoretică pentru dimensiunea unei rețele peer-to-peer, acestea pot fi constituite din două, dar și din sute de calculatoare. Utlizarea principală a aplicațiilor P2P este aceea de a oferi și descărca fișiere, dar este de asemenea si o metodă foarte frecvent utilizată pentru distribuirea programelor malware și efectuarea altor fapte dăunătoare.

Exemple de rețele P2P: [BitTorrent](https://ro.wikipedia.org/wiki/BitTorrent), [eDonkey](https://ro.wikipedia.org/w/index.php?title=EDonkey&action=edit&redlink=1), [Gnutella](https://ro.wikipedia.org/w/index.php?title=Gnutella&action=edit&redlink=1), [FastTrack](https://ro.wikipedia.org/w/index.php?title=FastTrack&action=edit&redlink=1), [ANts](https://ro.wikipedia.org/w/index.php?title=ANts&action=edit&redlink=1), [Kazaa](https://ro.wikipedia.org/w/index.php?title=Kazaa&action=edit&redlink=1), [BearShare](https://ro.wikipedia.org/w/index.php?title=BearShare&action=edit&redlink=1), [Direct Connect](https://ro.wikipedia.org/w/index.php?title=Direct_Connect&action=edit&redlink=1) sau [Limewire](https://ro.wikipedia.org/w/index.php?title=Limewire&action=edit&redlink=1).

**Slide 15**

# Descărcările torrent

Încercați să găsiți un anumit film care nu este online inca? Sau poate doriți o copie gratuită a celui mai recent joc PC. Site-urile torrent sunt folosite de utilizatorii de computer foarte priceputi care folosesc virusii si programele malware practic in fiecare zi.

În majoritatea cazurilor, fișierul pe care îl descărcați ar putea fi un program de instalare malware scris de un programator iscusit.

**Slide 16**

#Phishing-ul

Imaginati-va o situatie, e dimineață și apa din ibric încă nu a început să clocotească. Va așezati pe scaunul din bucătărie și începeti să va butonati telefonul, la fel cum faceti în fiecare zi. Deschideti căsuța de mail, ca să vedeti ce sarcini aveti de rezolvat la serviciu, dar un mesaj va atrage atenția. Apa începe să fiarbă și pulsul va crește. ”Ajută-mă și primești o sută de mii de dolari”, scrie în subiect. Parcă nici cafea nu va mai trebuie.

Un domn din Africa va propune un târg care v-ar transforma în milionar peste noapte. Dumneavoastra îi trimiteti câteva informații prin e-mail sau le introduceti pe site-ul unei bănci și el va dă o parte din averea lui enormă care, momentan, e blocată de autoritățile nigeriene. Faceti o faptă bună și va și îmbogățiti. Sună ca un vis devenit realitate, nu? E, mai degrabă, un coșmar.

**Ce este phishingul?**

Phishingul este o metodă de înșelătorie aproape la fel de veche ca și Internetul. Infractorii se folosesc de inginerii sociale pentru a păcăli utilizatorii, infectându-le computerele, furându-le banii sau chiar identitatea. Tentativele de phishing se bazează pe emailuri, mesaje instant sau chiar și apeluri telefonice, și încercă să îi convingă pe utilizatori să acceseze anumite site-uri sau să îți dea anumite date personale. Site-urile respective sunt fie copii perfecte ale unor site-uri cunoscute (Facebook, site-uri ale unor bănci, PayPal), sunt fie infectate cu viruși.

## Cum să recunoști tentativele de phishing și care sunt riscurile

Din fericire, există câteva metode simple de a-ți da seama dacă cineva încearcă să te păcălească sau chiar vrea să te transforme în milionar (un prim indiciu: nu îți va da nimeni bani gratis niciodată).

În primul rând, când vine vorba de mesajele scrise, infractorii lasă mereu indicii care îi dau de gol. Trebuie doar să fii atent la unele semnale.

Majoritatea mesajelor de tip phishing care se propagă fie prin email, fie prin platformele de mesagerie instant (inclusiv Facebook), sunt înțesate de erori gramaticale și pornesc de la o premiză oarecum absurdă (cum ar fi o serie de schimbări drastice aduse unei platforme). În plus, există mereu un link care, la prima vedere pare legitim, urmat de o amenințare de genul ”contul îți va fi șters automat dacă nu îți introduci datele în decurs de cinci zile”.

Dacă observi oricare dintre aceste semne, este bine să marchezi emailul sau mesajul drept spam, pentru a alerta serviciile pe care le folosești că acest timp de mesaje se propagă prin platformele lor. Mailurile și mesajele nu vin tot timpul de la persoane necunoscute, ci este posibil ca un prieten infectat cu un malware să îți trimită un link capcană fără voia lui.

## Alte sfaturi pentru a te feri de phishing

* *Ai grijă la mesajele în care ți se cer informațiile confidențiale* – În special când vine vorba despre informații de natură financiară. Organizațiile nu îți vor cere niciodată detalii cu caracter sensibil prin email, de exemplu.
* *Nu te lăsa presat –*Infractorii vor încerca mereu să te sperie prin diverse metode pentru a te convinge să le pui la dispoziție datele de care au nevoie pentru a te fura. În cazul în care un site de la care ai făcut o comandă recent îți cere să reintroduci datele cardului pentru a nu-ți întârzia livrarea, pune mâna pe telefon și interesează-te direct la sursă.
* Fii atent la mesajele generice – Mesajele frauduloase nu sunt, de multe ori, personalizate și sunt presărate de greșeli.
* *Nu accesa direct link-urile dintr-un mesaj care pare suspect –*Dacă ai un link care pare să ducă către un site cunoscut, mai bine deschizi o filă nouă și tastezi manual adresa. În cazul în care ai dat click pe link-ul din mesaj, sunt șanse mari ca site-ul pe care l-ai accesat să fie o copie aproape identică a unuia legitim, dar vor exista mereu diferențe (de culoare, de aranjare în pagină, greșeli gramaticale sau link-uri URL ciudate după accesare).
* *Ascultă-ți instinctul –*Dacă o oferă pare prea bună să fie adevărată, probabil că este o țeapă. Dacă măsura anunțată de o companie pare absurdă, cineva încearcă să te păcălească. Încearcă mereu să te documentezi înainte să-ți dai datele personale.
* *Folosește o soluție de securitate cu filtru anti-phishing –*Ai la dispoziție soluții de securitate avansate care te apără de astfel de atacuri. Dacă folosești serviciile Microsoft, trebuie să știi că browserul Internet Explorer preinstalat pe sistemele cu Windows vine cu un filtru anti-phishing și serviciile de email precum Outlook folosesc tehnologii anti-spam și anti-phishing.

**Slide 17**

**Importanta securitatii cibernetice (concluzie)**

Pe parcursul istoriei au avut loc numeroase atacuri cibernetice (GoldenEye, WannaCry), care au dus la falimentarea si ruinarea mai multor companii si organizatii de importanta nationala si internationala.

Odata cu trecerea anilor amenintarile cibernetice evolueaza, devenind din ce in ce mai periculoase si greu de controlat, de aceea este extrem de important sa cunoastem potentialele pericole si cum sa ne aparam de ele, inainte ca acestea sa devina o adevarata problema, acesta fiind si scopul prezentarii noastre de azi caci o persoana informata este o persoana protejata.