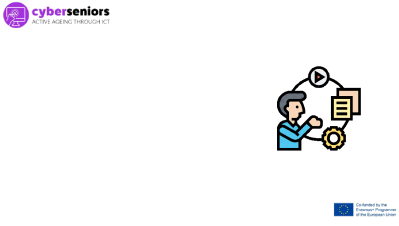
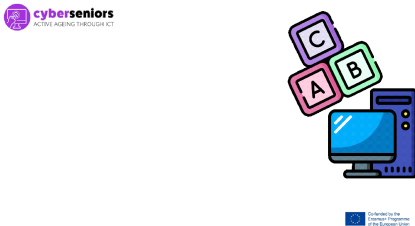
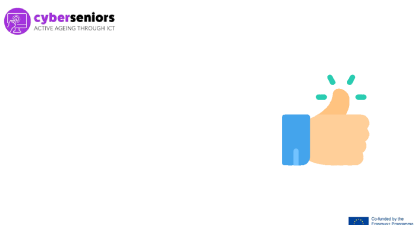
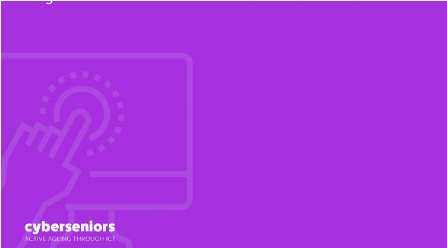


Modulul 2/ Utilizarea responsabilă și în siguranță a dispozitivelor ICT

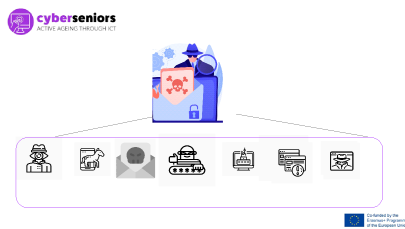
- Pregătește toate materialele necesare (calculator, prezentare, stick USB, etc ...)
- Pregătește prezentarea
- Asigură-te că ai o atitudine pozitivă și motivantă
- Fii punctual/ă

Slide 1 2 min 	Înainte de a începe sesiunea de instructaj: • Pregătește toate materialele necesare (calculator, prezentare, stick USB, etc ...) • Pregătește prezentarea • Asigură-te că ai o atitudine pozitivă și motivantă • Fii punctual/ă În timpul sesiuni de instructaj: • Ureeză-le bun venit participanților și prezintă-te pentru a crea o atmosferă plăcută. • Ține cont de durata fiecărei părți din prezentare pentru a avea timp să acoperim tot materialul. • Păstează timp la sfârșit pentru întrebări. • Acționează cu empatie și răbdare. • Asigură-te din când în când că audiența ta este atentă la explicațiile tale.
---	--

3 min		Vom prezenta faptul ca Cyberseniors este un proiect cofinantat de Comisia Europeana prin programul Erasmus +, avand ca obiectiv principal crearea unor resurse de instruire a persoanelor cu varsta de peste 55 ani,cum sa gestionam un smartphone si aplicatii uztile pentru a asigura o imbatranire activa si o mai mare autonomie.Amintim faptul ca toate informatiile si resursele pot fi accesate pe: www.cyberseniors.org Explică în mare ce se va discuta în sesiunea de astăzi. 1. Introducere in utilizarea smartphonului/tabletei 2. Utilizarea responsabila si in siguranta a Tehnologiei Informatiei si Comunicarii(TIC) 3. Aplicatii TIC pentru telefonul mobil si tableta(operatii bancare, nevoi zilnice, administratie publica)
10 min		Evoluția tehnologiei digitale a transformat modul în care interacționăm cu alți oameni și modul în care ne desfășurăm activitățile zilnice. ... este o abilitate fundamentală pentru noi toți, pentru a învăța cum să navigăm în lumea contemporană digitalizată și să ne adaptăm la nevoile în schimbare.
		● Nevoile cotidiene contemporane ● E-mail ● Comunicare virtuală ● Tranzacții digitale

		Abilitatea de a utiliza instrumentele digitale se referă la: ● Abilitățile necesare pentru a obține competențe digitale; ● Utilizarea sigură și critică a tehnologiilor informației și comunicațiilor (TIC) pentru muncă, timp liber, învățare și comunicare (Glosarul Eurostat, 2019); ● Familiarizarea cu elementele de bază ale securității digitale și utilizarea conținutului autorizat.
		Abilitatea de a utiliza instrumentele digitale are următoarele beneficii: ● Deschide o lume de oportunități; ● Unește oamenii; ● Ne permite să facem lucruri de la distanță (foarte important în contextul pandemiei) ● Ne îmbunătățește abilitățile și permite învățarea pe tot parcursul vieții; ● Promovează independența;
		

15 min



Acestea sunt unele dintre cele mai comune tipuri de amenințări.

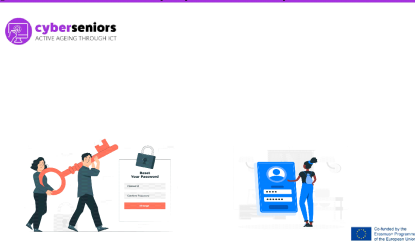
Este destinat pentru **impersonarea** altei persoane pentru a fura date sau a modifica datele unui server. Tehnicile de phishing folosesc, de asemenea, fraudă de identitate pentru a ne face să credem că trimitem datele noastre către un site web de încredere atunci când, de fapt, hackerul le primește, de ex. uzurparea identității prin Facebook pentru a ne fura parola.

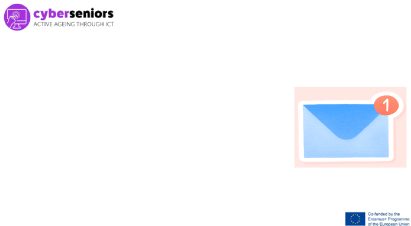
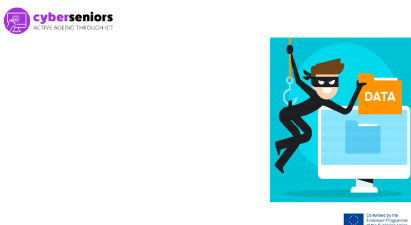
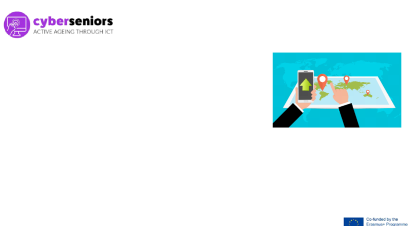
Troianul este un software mascat ca benefic și pretinde că îl instalăm pentru a obține acces la datele noastre sau pentru a ne transforma computerul într-un membru al unei rețele bot. Poate fi deghizat în orice, suite de birou, antivirus, software bancar etc. Din acest motiv, este esențial să nu avem încredere în orice software pe care îl instalăm. Ar trebui să instalăm software-uri numai din surse de încredere (magazine de aplicații) și ar trebui să verificăm fiecare software pe care îl instalăm cu un antivirus.

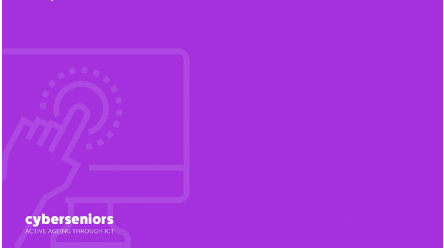
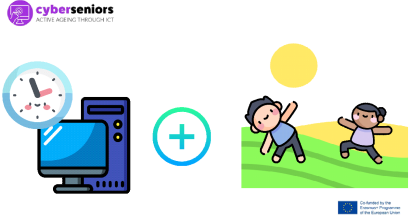
SPAM: conceptul de spam este foarte larg și acoperă toate comunicările nedorite cu cineva care pot deveni inexistente și pot fi repetate sau nu. Ca regulă generală, este produs prin email, dar poate fi produs prin orice alte mijloace, whatsapp, sms, apel telefonic etc. Scopul poate fi obținerea de informații pe site, furtul de date, instalarea de software rău intenționat etc.

Ingineria socială exploatează slăbiciunea noastră ca oameni pentru a avea încredere în ceilalți și pentru a obține astfel informațiile necesare pentru un atac. De exemplu... un apel de „asistență” care ne solicită o parolă de serviciu pentru a rezolva o problemă. Ingineria socială este, de asemenea, considerată a fi studiul informațiilor publice ale unui utilizator (rețele sociale, site-uri web personale etc.) pentru a obține informații relevante pentru un atac... de ex. Publicăm numele animalului nostru de companie pe Facebook cu vizibilitate universală. Un presupus atacator va adăuga aceste informații la lista de parole pe care va încerca să le introducă în conturi.

Phishing: Phishing-ul este o tehnică care duce la instalarea de malware, furtul de date sau de bani prin mesaje de e-mail, site-uri web, apeluri telefonice (vishing) sau SMS (smishing) care par legitime ca aspect și context, dar care ne-ar putea aduce la un site-ul web de unde vor fura date, vor facilita instalarea de programe malware sau vor fura bani de pe cardurile noastre de credit, printre alte acțiuni.

		Adware: este un software care ne afișează reclame în aplicațiile sau paginile web pe care le vizităm pentru a genera profit pentru creatorul de malware prin clicurile noastre pe anunțuri. Spyware: este un software care spionează acțiunile noastre pe dispozitivul nostru. Dacă dispozitivul nostru are funcții multimedia sau senzori de locație, acesta poate spiona acele informații, poate activa camere sau microfoane sau poate accesa locația noastră de pe mobil etc.
		Jumătate dintre vârstnici nu folosesc funcția de parolă pe cel puțin unul dintre dispozitivele lor cu acces la internet, creând posibilitatea ca aceasta să poată fi preluată de oricine. Blocați toate dispozitivele, inclusiv computerul, tableta și smartphone-ul cu parole puternice. Acest lucru va ține privirile indiscrete și va fi o apărare în cazul în care dispozitivele dumneavoastră sunt pierdute sau furate. Cât de des trebuie să schimbați parolele? Cu excepția cazului în care deveniți conștienți de o încălcare a parolei, nu este nevoie să vă schimbați frecvent parolele dacă fiecare este o parolă puternică și unică. Cu toate acestea, dacă credeți că unul dintre conturile dvs. a fost piratat, vă rugăm să vă schimbați imediat parola.
		Când creați postări pe rețelele sociale, puteți alege setările de confidențialitate pentru a selecta publicul care va vedea postarea dvs. Ar putea fi doar prietenii pe care i-ai adăugat pe rețeaua de socializare, ar putea fi o postare publică pentru oricine sau poate fi o postare privată doar pentru tine. De asemenea, puteți specifica sau nu locația dvs. Asigurați-vă că informațiile dvs. private nu sunt partajate (parole, număr de telefon, e-mail etc.) *Vom pune videoclipul următorului slide pentru a întări pericolul accesului liber la informațiile noastre pe rețelele sociale, de exemplu.

		În timpul comunicării prin rețelele sociale, mesagerie și e-mail, ar trebui să aveți grijă să nu faceți clic pe link-urile trimise de o persoană necunoscută. Infractorii cibernetici se pot uzurpa, de exemplu, angajații Facebook sau serviciul de securitate al Instagram. Nu ai încredere în acele mesaje, dacă le primești printr-un chat normal, o postare sau dintr-o pagină normală de Facebook. Mesajele de siguranță vă vor fi trimise prin notificări sau vor fi disponibile în setări. Angajații rețelelor sociale nu vă vor cere niciodată parola sau informațiile private.
		Dacă prietenii sau familia vă cer să îi ajutați într-o situație de urgență, sunați întotdeauna pentru a vorbi cu ei personal și pentru a confirma dacă au trimis într-adevăr mesajul. În caz contrar, aceste mesaje pot proveni de la criminali cibernetici. Aceștia pot crea un profil care va fi identic cu profilul prietenului tău sau al membrului familiei și să încerce să obțină bani de la tine.
		Puteți utiliza instrumentul „Găsiți telefonul meu” de la Google, dacă sunteți conectat la contul dvs. Google (gmail) de pe telefon. În primul rând, trebuie să permiteți Google să vă folosească datele despre locație, informațiile despre dispozitiv și evenimentele de conectare pentru a vă localiza dispozitivele și accesoriile. Este posibil ca locația dispozitivului dvs. să nu fie întotdeauna exactă, dar veți vedea o hartă a locației curente a telefonului dvs. Vor fi disponibile și date referitoare la nivelul de încărcare și conexiunea la rețeaua mobilă. Veți avea mai multe opțiuni: Setați alarma pe telefonul dvs. Dispozitivul va suna timp de cinci minute chiar dacă telefonul este în modul silențios. Blocați-vă telefonul și deconectați-vă de la contul dvs. Google. De asemenea, puteți afișa un mesaj text pe ecranul telefonului. Ștergeți datele dispozitivului prin resetarea la setările din fabrică. După aceea, nu veți mai putea să vă monitorizați dispozitivul.

	 cyberseniors ACTIVE AGEING THROUGH ICT	
		
5 min		● Este necesar să se mențină un echilibru mental și fizic. ● Gestionați-vă interacțiunile cu instrumentele digitale Bunăstarea digitală ne influențează bunăstarea generală și invers. Cea mai bună sugestie este să găsim un echilibru între ambele „lumi” pentru a obține cea mai bună îmbogățire și beneficii pozitive în fiecare domeniu, reducând riscurile unei utilizări excesive a instrumentelor digitale care, după cum am văzut, ne-ar putea afecta în moduri diferite. . Utilizați tehnologia pentru a interacționa cu lumea fizică și cu alți oameni într-un mod activ.

	  	Acestea sunt câteva consecințe ale abuzului de tehnologie
	  	● Înțelegeți și controlați-vă obiceiurile tehnologice ● Stabiliți limite ● Gestionați-vă mai bine conexiunile ● Luați pauze în mod regulat ● Dormiți și odihniți-vă bine, evitați să utilizați tehnologia înainte de a merge la culcare
5 min	     	CONCLUZII Vom lăsa ceva timp până la sfârșitul sesiunii pentru a rezolva îndoielile sau preocupările legate de cele explicate, le vom mulțumi pentru participare și îi vom încuraja să exerseze acasă pentru a nu uita ce au învățat astăzi. MULTUMIM FRUMOS!