Proiect co-finanțat din Fondul Social European prin Programul Operațional Capital Uman 2014-2020
Axa prioritară: Educație și competențe; Obiectiv specific 6: Îmbunătățirea competențelor personalului didactic din învățământul pre-universitar în vederea promovării unor servicii educaționale de calitate orientate pe nevoile elevilor și a unei școli incluzive
Denumirea proiectului: *EduForm - EDUcație inclusivă de calitate prin FORMare profesională continuă* (POCU/73/6/5/106757)

AVIZAT
MANAGER PROIECT

GHID DE BUNE PRACTICI MANAGEMENT EDUCAȚIONAL

MAZERA Mihaela Adela

Expert relația cu comunitatea

CUPRINS

PLATFORME EDUCAȚIONALE ON-LINE

Resursele educaționale deschise reprezintă mulțimea materialelor educaționale disponibile on-line utilizate sau reutilizate în mod deschis și gratuit de către elevi și profesori deopotrivă.

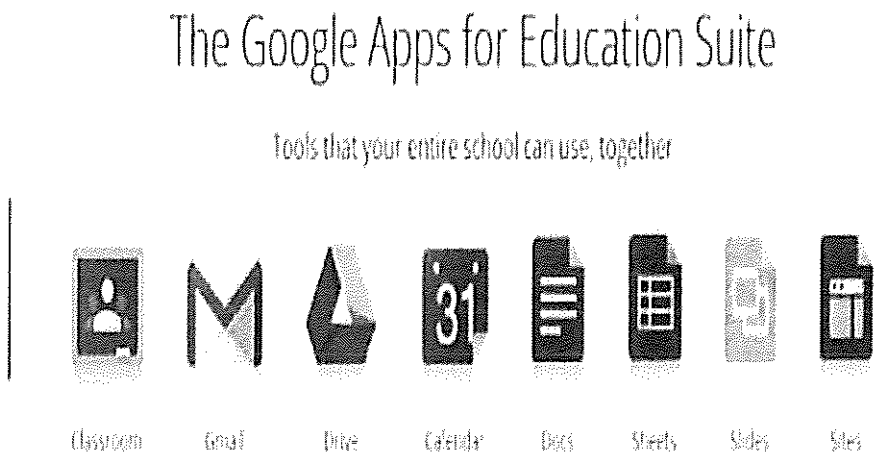
Tehnologia digitală este esențială în procesul de învățare și creeara platformelor educaționale on-line este metoda potrivită de a îmbina educația cu tehnologia.

Presupune învățarea activă folosind tehnologia. Elevi devin mai autonomi și responsabili față de propriul lor proces de învățare, încurajează învățarea colaborativă şi lucrul în echipă.

GoogleApps for Education

Google Apps for Education reprezintă un grup de aplicații creat de Google care include un grup de 8 aplicații: Classroom, Gmail, Drive, Calendar, Docs, Sheets, Slides și Sites concepute ca o soluție simplificată și gratuită a nevoilor educaționale. Cu acest pachet de aplicații este asigurată colaborarea în orice moment, oriunde. Clasele, profesorii și elevii își pot desfășura activitatea într-o deplină colaborare oriunde s-ar afla, pe orice fel de dispozitiv. În plus pot fi accesate informații de pe cărțile Chromebooks și noile aplicații Google cum este G Suite for Education.

Google prin aceste aplicații încearcă și reușește co-editarea documentelor, a spreadsheet-urilor și prezentărilor în timp real, gestionarea listelor, crearea și programarea agendelor. Pot fi create clase, distribuite teme și consultații, se pot trimite reacții și opinii. Un adiministrator (profesorul)își poate adăuga elevii, gestiona dispozitive, configura securitatea sau modul de comunicare prin email, chat sau videoconferință.



Platforma Edmodo

http://www.google.com/url?q=http%3A%2F%2Fwww.edmodo.com&sa=D&sntz=1&usg=AFQjCNGLEDCRMn81V7rC4z0s_FFQC1wcoA

Popularitatea rețelelor de socializare (mai ales a Facebook-ului) este într-o continuă creștere, numărul de utilizatori mărindu-se pe zi ce trece. Acest fapt se datorează în primul rând posibilității de comunicare pe care o oferă acest tip de rețele, iar în al doilea rând, ușurinței cu care pot fi ele folosite. Platforma de e-learning Edmodo întrunește ambele condiții, fiind extrem de „prietenoasă" cu orice utilizator și asigurând o comunicare eficientă între profesori, elevi și părinți. În timp ce rețelele obișnuite de socializare reprezintă un mediu liber, în care fiecare utilizator se poate exprima în orice fel și nu are nicio restricție în privința tipului de conținut afișat, platforma Edmodo este un mediu controlat în care profesorul poate vedea fiecare mesaj, fișier sau conținut distribuit de către membrii clasei lui. Toate aceste date sunt vizibile și pentru părinți, așadar orice fel de situație neplăcută care ar putea fi declanșată pe o rețea obișnuită de socializare (apariția unui tip de conținut nepotrivit, declanșarea unor discuții în contradictoriu ș.a.m.d.) este evitată întru totul.

Platforma Edmodo se remarcă prin uşurinţa cu care poate fi folosită. Asemănarea dintre aceasta şi populara reţea Facebook apropie mediul şcolar de generaţia mai tânără, desăvârşindu-se procesul de învățare prin mijloace extrem de moderne, pe placul elevilor, exact în mediul în care aceștia se simt cel mai bine.

Platformă pentru gestionarea clasei și a activităților de învățare, pentru comunicare și colaborare. Este adaptată pentru învățământul preuniversitar. Permite și înscrierea părinților.

Easyclass

https://www.google.com/url?q=https%3A%2F%2Fwww.easyclass.com%2F&sa=D&sntz=1&usg=AFQjCNEMBEOnfV3jAZuXawlAQzEVhl4IwA

Permite gestionarea activităților de învățare - clasele de elevi pot primi materiale, teste, sarcini de lucru variate. Produsele activității elevilor pot fi notate și pot primi feedback.

Școala pe net

https://www.google.com/url?q=https%3A%2F%2Fscoalapenet.ro%2F&sa=D&sntz=1&usg=AFQjCNHlRRj6rSMc3CoGb_xDomHzYSYBVA

Platformă cu resurse pentru toți profesorii interesați să-și dezvolte competențele digitale și să susțină activități de învățare cu ajutorul noilor tehnologii. În cele ce urmează ne vom ocupa de cele patru metode folosite de platforma **Școala pe net** pe care le vom utiliza în unitatea noastră școlară, și anume Google clasroom, Facebook live, WhatsaApp și Zoom, fiecare cu caracteristicile și limitările sale.

GOOGLE CLASSROOM
https://classroom.google.com/

Permite încărcarea de materiale, postarea de anunțuri, notarea materialelor încărcate de elevi. Necesită conturi google (pentru profesor și elevi) și activarea licenței google.

Google Classroom face parte din suita de aplicații G Suite for Education creată de Google împreună cu profesori, pentru a le permite acestora să faciliteze, în online, predarea, interacțiunea și colaborarea cu elevii atât în timpul orelor, cât și în afara lor.

Practic, Google Classroom vă ajută să creați clase virtuale pentru elevii voștri. Imaginați-vă o clasă, cu elementele ei nelipsite: elevi, profesori, sarcini de lucru, proiecte, feedback din partea profesorilor (și a elevilor), evaluare.

Este accesibilă atât de pe desktop, cât și de pe telefon și este folosită pentru toate nivelurile de învățământ.

Pași utilizare pentru profesori:

Autentificare cu adresa de email Google

Pentru a vă pregăti pentru organizarea unei clase virtuale Google Classroom aveți nevoie de o adresă de email care poate fi:

- adresa personală de gmail, de forma popescu@gmail.com

Pasul 1 – Accesul în Google Classroom prin email

Pentru a intra în spațiul în care creați clasa aveți două opțiuni:

1. Accesați în bara browserului de internet classroom.google.com și introduceți datele contului personal de email (user și parolă).
2. Al doilea mod de a accesa Classroom este direct din contul de gmail personal.Intrați în cont și în colțul din dreapta sus, lângă inițiala numelui, dați click pe simbolul Aplicații Google (Google Apps).

Apoi scroll până ajungeți la aplicația **Classroom** și dați click pe aceasta. Se va deschide pagina în care creați clasa.

Pasul 2 – Crearea clasei

Apăsați simbolul plus (+) din colțul din dreapta sus și apoi Creați un curs (**Create class**).

Acceptați mesajul care apare. Având în vedere situația actuală și interesul de a păstra comunicarea cu cât mai mulți elevi folosiți Classroom și pe adresa personală.

Introduceți numele clasei. Celelalte secțiuni sunt opționale, nu le completați.

Apăsați Creați (**Create**) și apoi **Got it** (dacă vă apare pe ecran mesajul în engleză cu noutăți).

Bun venit în prima clasă creată! În momentul în care ați creat clasa, a fost generat automat un cod al clasei, care rămâne permanent pe ecran sub numele clasei. Îl puteți folosi pentru a invita elevi în clasă. În cazul clasei create de noi codul este ydf5spq.

Puteți personaliza aspectul clasei accesând, în colțul din dreapta jos al imaginii de copertă, Selectați o temă din galerie sau Încărcați o fotografie proprie. Ca exemplu, noi am ales să schimbăm tema și am ales un fundal gri cu dispozitive tehnologice.

Important! Înainte de a invita alți colegi de cancelarie în clasa creată și înainte de a-i invita pe elevi, trebuie să cunoașteți principalele secțiuni ale clasei virtuale.

Butonul oferă acces la profilul contului, unde puteți vedea: clasele create cu acel cont de email, calendar, clasele din care faceți parte, activitate în curs (sarcini de lucru, teme ale elevilor de corectat), setări ale contului.

Numele clasei **Flux**

În această secțiune comunicați cu elevii, creați și programați anunțuri care vor ajunge ca într-un wall de Facebook la toți elevii. Aici aveți în vedere că există și opțiunea ca doar profesorii să posteze, se poate modifica din setările generale ale clasei.

Activitatea la curs – Aici creați teme, sarcini de lucru, chestionare, întrebări, încărcați materiale. Recomandăm ca înainte de a posta materiale să le aveți organizate într-un folder special creat în calculator, pentru a le accesa ușor. De asemenea, recomandăm să creați prima dată subiecte pentru sarcinile trimise sau chiar pentru unități de învățare.

Astfel, dacă veți crea subiectul Limba română, elevii pot accesa mai ușor toate sarcinile alocate acestei discipline.

Persoane – Aici invitați alți colegi de cancelarie care predau la clasă și bineînțeles elevii.

Apăsați simbolul pentru fiecare în parte. Puteți invita elevii prin adresele lor de email sau oferindu-le codul clasei despre care vorbeam mai sus.

Note – aici veți vedea notele pe care le-ați dat sarcinilor sau evaluărilor lucrate de elevi.

Setări clasă – aici puteți edita informațiile despre clasă, dar puteți seta și anumite aspecte legate de afisaj și dacă permiteți elevilor să posteze sau nu în Flux.

Aplicații Google – Toate aplicațiile la care aveți acces din contul de gmail.

Inițiala numelui / prenumelui din contul de gmail. Vă arată contul de gmail în care sunteți înregistat în acel moment.

Pași utilizare pentru elevi

Elevii au 2 opțiuni de a intra în clasa virtuală creată:

1. Primesc și acceptă invitația primită pe email
2. Intră în adresa lor personală de email Google, deschid emailul de invitație și dau Join în clasă.

Elevii vor vedea secțiunile clasei: Flux, Activitate la clasă, Persoane, cu excepția Notelor și a setărilor clasei.

Folosesc codul clasei
Intră pe classroom.google.com
Se conectează cu adresa personală
În loc să creeze o clasă, aleg ***Înscrie-te la un curs*** și introduc codul clasei primit de la profesor.

FACEBOOK LIVE
https://en-gb.facebook.com/login/

Instalare aplicație: Este suficientă crearea unui cont personal de Facebook.

Pași utilizare pentru profesori:

1. Crearea grupului. În contul personal, în dreapta sus, lângă Acasă (**Home**) apăsați butonul Creează (**Create**). Din opțiunile care apar, alegeți Grup (**Group**).
2. Setările grupului. Alegeți un nume pentru grup (**Name your group**), ca exemplu poate fi numele clasei voastre sau ceva care să vă reprezinte identitatea clasei. Adăugați persoane în grup (**Add some people**), introducând numele lor de Facebook sau adresele lor de email. Puteți face acest lucru și mai târziu.
Confidențialitatea grupului este o setare foarte importantă de avut în vedere. Recomandăm ca grupul să fie privat și ascuns pentru comunicarea cu elevii sau cel mult privat și vizibil. Acest lucru înseamnă că informațiile postate pot fi vizualizate doar de membrii grupului.
3. Creare grup. Apăsați butonul Creează (**Create**) și grupul a fost deja creat.
4. Personalizare. Opțional, puteți schimba fotografia de copertă (**Cover Photo**) la fel ca în profilul personal. Poate fi o imagine relevantă pentru clasă, o fotografie de grup care vă este dragă..
5. Invită membri în grup. Pentru a invita membri noi în grup introduceți numele lor în secțiunea din dreapta paginii, Invită membri (Invite members). Atenție: în cazul oricărui tip de grup, membrii grupului pot să invite în grup doar persoane cu care sunt prieteni.
6. Și acum să trecem la opțiunea care vă va ajuta pentru predarea la distanță. Pentru a susține o lecție live, în pagina principală a grupului, deasupra spațiului pentru postare, apăsați Clip video în direct (**Live video**). Se va deschide o nouă pagină, împărțită în două secțiuni.
În cea din stânga veți vedea imaginea de pe camera calculatorului personal, în timp ce, în cea din dreapta completați câteva informații despre lecție înainte de a intra în direct: text (**Spune ceva despre acest clip video în direct...**) care va însoți video-ul și puteți da un titlu transmisiei live.
7. Transmisie live. Înainte de a intra live, verificați că aveți pornite setările de microfon ale calculatorului. Apoi apăsați butonul albastru Intră în direct (**Go live**) . În 3 secunde veți intra live pe grupul vostru.
8. Invită prieteni. Dacă elevii nu s-au conectat încă la lecție, invitați-i apăsând butonul din stânga ecranului, jos, Invită prieteni (**Invite friends**) care va apărea după câteva secunde de la debutul transmisiei.
Recomandăm ca după ce intrați live, înainte de a începe comunicarea cu elevii, să verificați că aceștia vă aud și vă văd. Ei pot răspunde printr-un mesaj în Scrie un comentariu (ca la orice postare pe Facebook).
În timpul predării faceți pauze speciale pentru adresarea de întrebări, ca la clasă. Altfel, va fi provocator să urmăriți și cursul lecției și chat-ul în același timp.

9. Încheierea lecției. Pentru finalizarea întâlnirii online, este suficient să apăsați butonul roșu Închide transmisia (**End live video**). Apoi puteți opta pentru salvare și postare pe grup sau ștergere. Apăsați opțiunea Încheie (**End**) în fereastra care se deschide. Apoi apăsați opțiunea Gata (**Done**), pentru a alege salvarea video-ului în grup. Astfel, elevii care nu au reușit să intre live vor putea avea acces la video. Dacă nu vreți să se salveze, selectați Șterge clipul video (**Delete video**).

Pași utilizare pentru elevi:

1. Să dețină un cont personal de facebook
2. Să accepte invitația de a intra în grup
3. Să accepte invitația de a viziona live lecția

Platforma Facebook Messenger permite un număr maxim de 8 persoane în apel video. Persoana care inițiază apelul video trebuie să fie conectată la calculatorul persoanal pentru a selecta celelalte 7 persoane.

Pași instalare aplicație:

1. Pe calculatorul personal: Este suficientă crearea unui cont personal de Facebook, unde veți folosi chatul Messenger. Recomandabil ca profesorul să se conecteze de pe calculatorul personal, chiar dacă elevii pot folosi și telefonul
2. Pe telefon se va instala aplicația Messenger

Pași utilizare pentru profesori:

1. Crearea grupului. În contul personal de Facebook, apăsați iconița și selectați Grup nou (**New goup**). Apoi denumiți grupul (numele Grupei de grădiniță/Clasă) și invitați copiii/elevii. Persoana care care creează grupul (dirigintele/managerii de caz pt. sprijin) este administratorul grupului. Doar administratorii pot invita membri în grup.
2. Vizualizați conversația pe tot ecranul pe calculatorul personal pentru a vă fi mai ușor să o urmăriți. Dați click pe rotița albastră Setări din fereastra de chat și selectați Deschide în Messenger.
3. Începeți comunicarea și anunțați întâlnirea. Spațiul de chat poate fi ușor folosit pentru comunicare în scris, trimitere fotografii, documente și fișiere audio.
4. Pentru a porni conversația video (max. 8 persoane din grup, incluzând administratorul), dați clik pe simbolul (camera) din colțul din dreapta sus al ferestrei de chat. Se va deschide o fereastră cu lista participanților. Alegeți primii 7 participanți cu care aveți stabilită întâlnirea. Pentru a începe, apăsați Sună și conversația poate începe. Toți participanții din grup pot vedea că se desfășoară un apel, dar doar cei selectați pentru convorbire vori fi apelați direct.
5. Pentru finalizarea conversației închideți apelul video.

Pași utilizare pentru elevi:

1. Să dețină un cont de Facebook
2. Să instaleze aplicația Facebook Messenger, dacă aleg să participe la conversația video de pe telefon sau tabletă
3. Să accepte apelul video + audio din fereastra de chat doar atunci când sunt apelați direct.

IMPORTANT:

1. Înainte de a începe lecția live în grupul privat al clasei/grupei, asigurați-vă că elevi/preșcolarii vă aud și vă văd.
2. Comunicati-le elevilor/preșcolarilor să fie prezenți în fața ecranului cu 5 minute înainte de a începe, pentru a putea desfășura la timp lecția.

WHATSAPP

https://web.whatsapp.com/

1. Începeți crearea grupului. Intrați în aplicația WhatsApp pe telefon și apoi în Chats. În colțul din dreapta sus selectați New Group.
2. Invitați participanții în grup. Pentru a putea invita pe cineva în grup este nevoie să aveți numărul de telefon al persoanei salvat în agendă. Selectați persoanele pe care doriți să le invitați în grup și apăsați Pot fi doar elevi, sau elevi și profesori ai clasei.
3. Dați un nume grupului în fereastra care se deschide, poate fi numele simplu al clasei (ex. Clasa a III-a A sau Grupa Mijlocie B), care vă reprezintă și îl știți doar voi. Selectați o fotografie pentru grup, apăsând pe simbolul cameră foto. Astfel, va fi
mai ușor pentru membri să identifice grupul în chat-ul lor personal. Aveți 3 opțiuni: să faceți o fotografie (Take photo), să alegeți una din galeria telefonului (Choose photo) sau să căutați pe web (Search web).
4. Apăsați Create pentru a crea grupul și veți ajunge direct în fereastra de chat.
5. Adăugare participanți. Puteți adăuga participanți și după crearea grupului. În fereastra de chat, apăsați pe numele grupului. În pagina deschisă, Group Info, glisați în jos pe ecran până când ajungeți la + Add participants. Aici veți putea să invitați participanții pe care îi doriți în grup.
6. În această fereastră puteți inițiа deja conversații cu toți membrii grupului și puteți trimite mesaje text sau linkuri (anunțuri și informații rapide etc.), fotografii (fișe de lucru, fișe din caietul elevului pentru a fi corectate de profesor, proiecte etc.) și mesaje audio (uneori vocea vă poate ajuta să câștigați timp și să transmiteți mesaje mai lungi mai repede decât să le scrieți). Pentru a înregistra mesaje audio, țineți apăsat simbolul microfon cât timp vorbiți aproape de telefon și eliberați când ați
finalizat înregistrarea. Mesajul audio se va trimite automat.
Atenție! Dacă nu doriți să trimiteți mesajul audio, înainte de a elibera butonul microfon, glisați degetul spre stânga pentru a-l anula (slide to cancel).
7. Dacă aveți nevoie să le trimiteți elevilor documente, în fereastra de chat apăsați simbolul + din stânga jos și selectați opțiunea Document. Se va deschide o nouă fereastră, cu locul din telefon unde aveți salvate documentele pe care doriți să le trimiteți. Puteți trimite documente de până la 100 MB. Puteți trimite documente Word, PowerPoint, PDF etc.
8. Apeluri video + vocale și apeluri vocale. Atunci când vă vedeți și vă auziți sunteți mai conectați cu elevii și se apropie puțin mai bine cu interacțiunea de la școală. Porniți direct din fereastra de chat a grupului, apăsând simbolul + , din colțul dreapta sus al ecranului. Selectați maximum 3 persoane (persoana care inițiază apelul este a 4-a). Odată selectate persoanele, puteți optați pentru apel video + vocal sau doar apel vocal, în funcție de ceea ce aveți nevoie. 9. Încheierea conversației. Pentru finalizarea întâlnirii online, este suficient să apăsați butonul roșu cu simbol telefon.

Pași utilizare pentru elevi:
1. Să instaleze aplicația WhatsApp din Magazinul Play (Google Play) sau App Store
2. Să seteze contul, folosind un număr de telefon valid.
3. Odată adăugat în grup să verifice mesajele care apar și să răspundă apelurilor profesorilor, la orele agreate.

Conversațiile de grup continuă și pe web / desktop
Instalare aplicație: Conversațiile de pe telefon sau tabletă pot fi cu ușurință sincronizate pe computer. Pentru comunicarea cu elevii, vă poate fi mai ușor să folosiți calculatorul, unde aveți la îndemână materiale utile pentru lecții și unde puteți tasta și mai repede decât pe telefon. Iată cum puteți face sincronizarea:

Pași pentru profesor și pentru elevi:

Calculator: În browser-ul de internet intrați pe web.whatsapp.com și urmați instrucțiunile care apar:

Telefon:
1. Deschideți WhatsApp pe telefon
2. În bara de meniu de jos selectați Settings și apoi WhatsApp Web

Telefon și calculator:
1. Îndreptați telefonul către ecranul calculatorului pentru a scana codul QR și astfel se va sincroniza conținutul de WhatsApp de pe telefon, cu calculatorul.

IMPORTANT:
1. Comunicați părinților / aparținătorilor preșcolarilor/elevilor un orar agreat de întâlnire prin WhatsApp, pentru a vă asigura că elevii /preșcolarii vor avea acces la un telefon cu date mobile suficiente sau cu posibilitate de a se conecta prin WiFi.
2. Recomandați elevilor/părinților să salveze numerele de telefon ale colegilor în agenda telefonului pentru a se putea identifica între ei. E mult mai personal să știi cui te adresezi. Faptul că profesorul vede numele în chat-ul personal, nu înseamnă că și elevii văd numele persoanelor care scriu.
3. Uneori se mai întâmplă să și greșim anumite mesaje. Aveți opțiunea de a șterge mesajele trimise din greșeală, atât timp cât destinatarii nu au văzut mesajul. Odată văzut de destinatar, mesajul nu mai poate fi șters.

4. Dacă WhatsApp este singura modalitate de comunicare cu elevii, stabiliți un program clar al întâlnirilor și respectați-l cu toții pe cât posibil, pentru a intra în scurt timp în rutină.
5. Un grup de WhatsApp poate avea până la 256 de membri. Pentru apelurii video în timp real, aplicația permite grupuri de maximum 4 persoane.
2. Puteți trimite fișiere în limita a 100 MB.
3. Aplicația WhatsApp folosește datele mobile alocate numărului de telefon sau o conexiune WiFi. Dacă nu folosiți o rețea WiFi - se pot percepe taxe pentru datele mobile. Contactați-vă operatorul de telefonie pentru mai multe detalii.

ZOOM MEETING
https://zoom.us/meetings

Pași utilizare pentru profesori:
Asigură-te că ai:
- computer personal / telefon / tabletă (Android, iOS)
- adresă e-mail

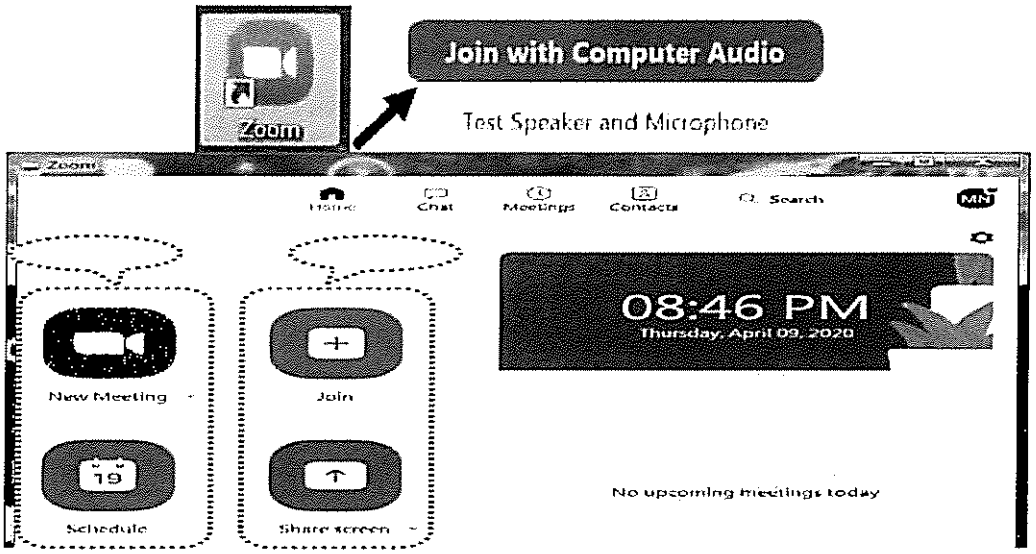
Pași utilizare pentru elevi:
Asigură-te că au:
- computer personal / telefon / tabletă (Android, iOS)

Nu este nevoie de o adresă de e-mail pentru conectarea elevilor la Zoom.

Tip interacțiune:
- 1 la grup
- 1 la 1

Programul Zoom Meeting este o aplicație software simplă și versatilă care permite derularea conferințelor audio-video online prin intermediul conexiunii internet. Datorită facilităților ei este folosită la nivel mondial atât în activitatea didactică la distanță cât și pentru organizarea unor ședințe având caracter administrativ.
- durata pentru o transmisiune online este nelimitată pe perioada pandemiei;
- maxim 100 de participanți la o conferință ;
- număr nelimitat de transmisiuni online;
- chat public și privat;
- transfer de fișiere de maxim 512 MB;
- partajare ecran sau aplicații software;
- înregistrarea activității online pe computerul local.

Aplicația poate fi instalată gratuit și pe telefonul mobil cu Android folosind aplicația "Magazin Play ". Aplicația Zoom poate fi lansată și din browserul Internet fără a instala niciun software, de la adresa web: zoom.us. Această versiune online are însă anumite limitări. Se recomandă instalarea aplicației pe calculatorul personal. Aici detaliem utilizarea variantei gratuite a aplicației Zoom instalată.



UTILIZAREA APLICAȚIEI ZOOM MEETING -în cazul instalării variantei gratuite a aplicației Zoom pe calculator

1. **Meniul principal.** După instalarea aplicației Zoom, iconița aplicației devine vizibilă pe desktop, permițând lansarea aplicației și afișarea fereastrei principale Zoom, care cuprinde opțiunile principale atât pentru profesori cât si pentru elevi:
2. **Inițierea activității online** este realizată de profesor prin selectarea uneia din cele două opțiuni:

A ."New Meeting " - pentru a activa direct transmisiunea online cu puțin timp înaintea orei de inceput a activității didactice. În acest caz se selecteaz ă în fereastra care apare, opțiunea **"Join with Computer Audio"** pentru a activa difuzorul calculatorului. Opțional se poate selecta opțiunea **"Test Speaker and Microphone"** pentru a testa difuzorul și microfonul calculatorului urmărind indica țiile afișate de program.

În acest moment este activa transmisiunea online (cu opțiunile implicite), fiind active atât camera video a calculatorului, cât și microfonul încorporat. Durata transmisiunii nu este limitată.

B."Schedule" – pentru a planifica una sau mai multe transmisiuni online viitoare la anumite ore și date. În acest caz programul afiș ează o fereastra care permite setarea mai multor parametrii ai activităț ilor online planificate care implică ș i controlul modului de intrare al studenților in activitatea online (cu video on/off cu audio on/off etc.).

Parametrii care pot fi setați in fereastra **"Schedule meeting"** sunt:

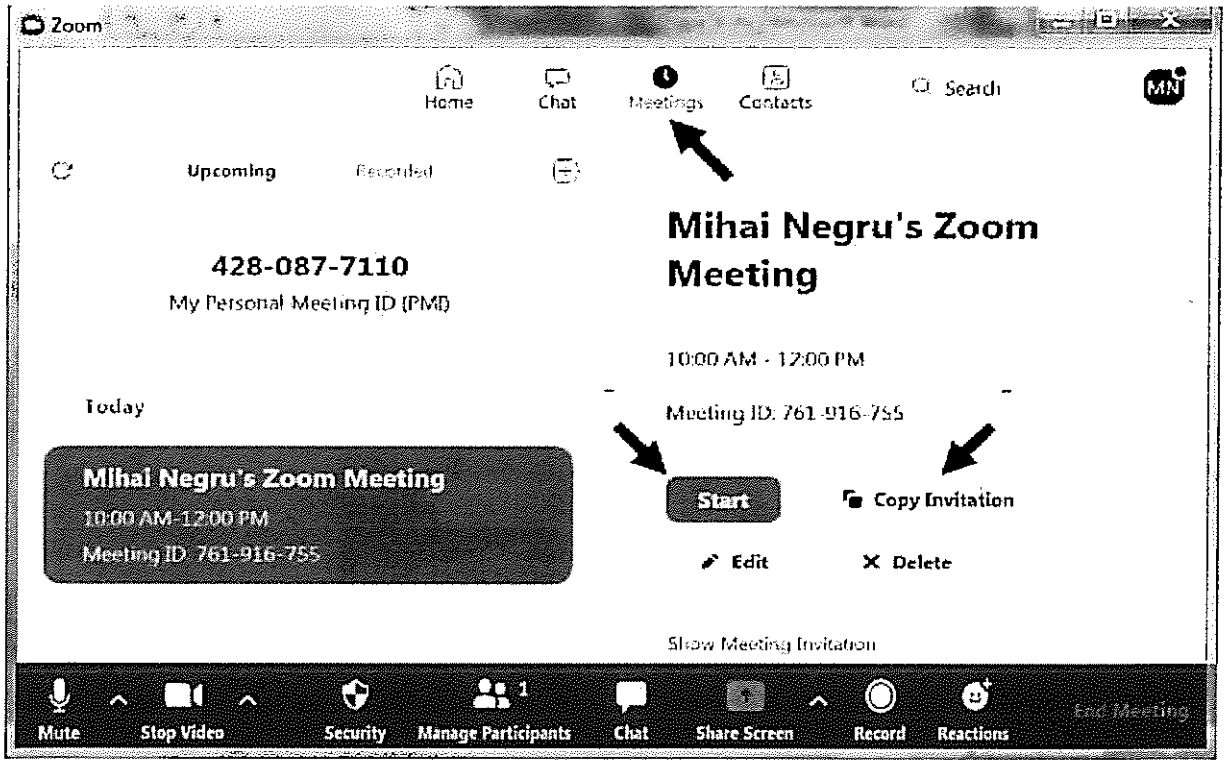
Titlul activității online – se poate modifica
Data cursului - Inactiv pt versiunea free
Ora de început

Durata - Deși acest mesaj atenționează cu privire la existența limitei de 40 min pt o transmisiune online, limita a fost înlaturată pe perioada pandemiei
Codul transmisiunii poate fi același pt fiecare curs
Codul transmisiunii poate fi generat automat pt fiecare curs

Elevii pot intra online cu parolă sau fără. In cazul când se bifează opțiunea trebuie precizat ă și parola
La inceperea cursului, **Video** poate fi **On** sau **Off** atât pt profesor (Host) cât și pentru elevi (Participants). Se poate modifica în timpul cursului.
Se recomandă alegerea opțiunii **Computer Audio** celelalte opțiuni fiind inactive pt versiunea free
Activează afișare meniu
Alegerea aplicației de tip calendar care să anunțe ora de început a cursului printr-un mesaj care apare pe ecran
Activează intrarea elevului doar cu acceptul profesorului
Activează intrarea elevilor și inainte de intrarea profesorului
Activează intrarea elevilor cu Microfonul Inactiv (Mute)

Înregistrare automata a transmisiunii

Confirmare date privind programarea activității online



După finalizarea planificării unei activități online programul afișează datele acesteia, respectiv: Link-ul transmisiunii, Meeting ID și password, care vor trebui transmise elevilor.

Pentru a activa transmisia online astfel planificată, în fereastra principală a aplica ției Zoom se alege opțiunea **"Meetings"** î n care sunt afișate toate transmisiunile online planificate. Prin selectarea opțiunii **Copy Invitation** se copiază datele transmisiunii online care trebuie transmise elevilor prin e-mail. Prin selectarea opțiunii **"Start"** se activează transmisiunea online.

3. **Opțiuni principale**. Indiferent de opțiunea aleasă pentru activarea transmisiunii online (**"New Meeting"** sau **"Schedule"**), în timpul transmisiunii online, în partea de jos a ferestrei video sunt afișate următoarele opțiuni principale atât pentru profesori cât și pentru elevi:
   Opțiunile uzual folosite sunt:

Mute/Unmute - Activează/dezactivează microfonul. Selectarea săgeții permite setări avansate Audio prin selectarea opțiunii **"Audio Settings"**.

Stop video/Start video – Activează/dezactivează camera video. Selectarea săgeții permite setări avansate Video prin selectarea opțiunii **"Video Settings"**
.

Security – Afiș ează lista de opțiuni care contribuie la securitatea transmisiunii online:
Lock Meeting – blocheaz ă intrarea noilor participanț i; **Enable waiting room** – intrarea online se face doar cu accept; **Share Screen** – permite studenților să-ș i partajeze ecranul; **Chat** – permite studenților sa aibă acces la Chat; **Rename Themselves** – permite studen ților s ă-ș i modifice numele afiș at in lista de participanți;
Remove Participant – Înlătură un elev din cursul online; Dezactivează microfonul elevilor la intrarea online; Profesorul permite elevilor activarea microfonului, Prof. permite elevilor să-și modifice numele afișat

Manage Participants–activează fereastra cu lista participanților online în care se permite, doar profesorului, activarea sau dezactivarea microfoanelor și dezactivarea camerelor video.
Mute All, Unmute All – Off sau On pentru toate microfoanele elevilor.
... – afișează următoarea listă de opțiuni:
Semnal sonor la profesor pt. Intrare și
ieșire participanți Intrarea online se
face doar cu acceptul profesorului
Profesorul blochează intrarea noilor participanți.

Chat – afișează fereastra de Chat care permite mesaje text între participanții la transmisia online. Mesajele Text pot fi trimise tuturor prin alegerea opțiunii **Everyone**, sau doar unui anumit participant selectat din listă.

Opțiunea **File** permite partajarea unor fișiere de maxim 512 MB pe care ceilalți participanți le pot downloada doar în cadrul transmisiunii online.

Share Screen – afiș ează fereastra de mai jos ș i permite partajarea online pentru toț i participanț ii a conținutului ecranului sau a unei aplicaț ii active. Profesorul alege modul de partajare: câte un participant pe rând sau mai mulți participanți simultan.

Advanced Sharing Options permite profesorului să aleagă cine poate partaja: **Only Host** – doar profesorul sau **All Participants** - toți participanții.

Aplicația partajată este vizibilă tuturor participanților și afișează un meniu în partea de sus a ecranului similar cu meniul anterior. Meniul este vizibil doar la trecerea cu mouse-ul în zona de sus.

Opțiunile noi care apar in acest meniu sunt:

- **Annotate** – afișeaz ă un meniu cu instrumente de desenare și eviden țiere a informa ț iilor de pe ecran. Aceste schițe explicative se ș terg in final cu opțiunea **Clear** .
- **Remote Control** – permite transferul controlului asupra tastaturii ș i mouse-ului unuia dintre participanții online. Opț iune utilă în cazul laboratoarelor de calculatoare când profesorul intervine pe calculatorul studentului pentru ajutor, modific ări ș i verificări. Transferul se face selectiv.
- **Stop Share** – incheie partajarea ecranului sau a aplica ției, revenind la transmisiunea video.
- **Record** – permite înregistrarea transmisiunii online, care la final va fi convertit ă în format mp4 (în jur de 10 Mbytes pe minut). Fi ș ierul e salvat pe propriul Hard Disk putând fi trimis apoi student ilor care nu au putut participa online, folosind platforma Wetransfer.
- **Reactions** – permite atât profesorului cât și elevului exprimarea aprecierii asupra activității online prin afișarea, timp de 5 secunde, a unuia din simbolurile: **Clap** – aplauze sau **Thumbs up** – Ok.
- **End Meeting** – Profesorul incheie transmisiunea online prin selectarea opțiunii **End meeting for All**. Pe ecranul studenților aceasta opțiune apare ca **Leave Meeting**.

4. **Datele necesare elevilor** pentru a se conecta la transmisiunea online, sunt accesibile profesorului prin selectarea butonului de informații din stânga sus a ferestrei transmisiei video:

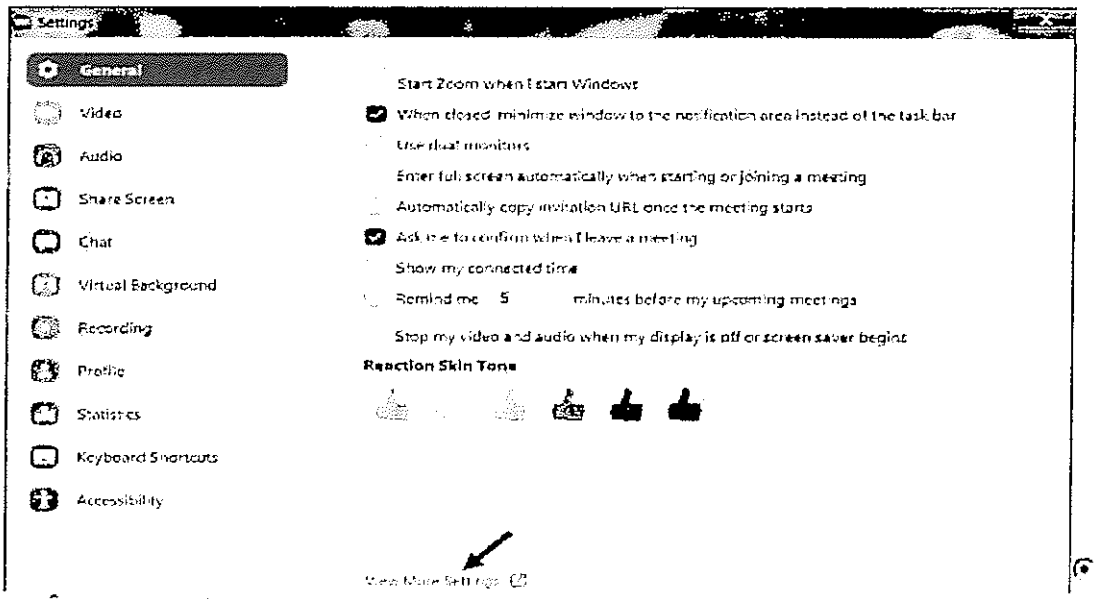
Profesorul va trebui s ă transmită elevilor una din variantele de date:

- **Invitation URL** care poate fi copiată cu **Copy URL.**
- **Meeting ID** și **Password**;

5. <u>Conectarea online a elevilor</u> se face în două moduri diferite în funcție de datele primite de la profesor prin e-mail:

   - **Invitation URL** – Conținutul copiat de profesor cu **Copy URL** este de fapt un link direct la transmisiunea online. Elevii vor selecta link-ul din mail-ul primit, fiind direc ționaț i în aplica ția Zoom care îi introduce direct în online făr ă parolă sau cod Meeting ID.
   - **Meeting ID** ș i **Password** – E l e v i i vor lansa aplicația Zoom și din meniul principal (fig. 1) vor selecta opțiunea **"Join"** pentru a participa la transmisiunea online. Elevii vor introduce în prima fereastră (fig. 2) **Meeting ID** validat cu **"Join"** și în a doua fereastră (fig. 3) parola (**Password**). Opțiunea " **Share screen"** poate fi selectată de elevi dar nu e recomandată deoarece este activat doar modul de partajare a ecranului elevului, nefiind posibilă vizualizarea conținutului video transmis de profesor. Opțiunile accesibile studen ților în timpul activit ăț ii online sunt aceleaș i cu cele de la punctul 3.

6. **Opțiuni avansate** pentru controlul transmisiunii online sunt accesibile, doar profesorului, din fereastra principală Zoom cu ajutorul iconiței **Settings** :



În urma selectării iconiței **Settings** este afișată fereastra Settings care permite realizarea set ărilor pentru fiecare aspect al aplicației Zoom: Video, Audio, Share Screen, Chat, etc.

Setări avansate suplimentare

Majoritatea acestor opțiuni sunt accessibile și din opțiunile prezentate la punctele 2 și 3, având avantajul că aici sunt grupate pe categorii. În mod implicit aplicația Zoom pornește cu setările cele mai uzuale care sunt suficiente pentru sus ținerea în bune condiții a activităților de învățământ online. Există însă și Setări avansate suplimentare care nu sunt permise din meniurile programului, fiind accesibile cu opțiunea **View More Settings** din care cele accesibile din versiunea gratuită sunt:

Host video (implicit Off) – Începe transmisiunea online cu video "On" pentru profesor;
Participants video (implicit Off) – Începe transmisiunea online cu video "On" pentru elevi. Se poate modifica în timpul transmisiunii online;

Audio Type – Permite alegerea sistemului audio folosit de participanți. Se recomandă alegerea opțiunii "Computer Audio". Opțiunea "Telephone and Computer Audio" sau "Telephone" implică folosirea unui telefon fără Android pentru a iniția o convorbire telefonică formând un număr de telefon din Statele Unite care permite participarea audio la discuțiile online. Cele două opțiuni sunt inactive în versiunea gratuită;

Telephone and Computer Audio **Telephone** **Computer Audio**

Join before host (implicit Off) – Permite participanților să intre online înainte de intrarea online a profesorului (pentru transmisiunile planificate anterior);
Require a password when scheduling new meetings (implicit On) – Va fi generată o parol ă când se programează o transmisiune online. Dacă opțiunea este "Off" participanții pot intra fără parolă ;
Require a password for instant meetings (implicit On) – Se va genera automat o parol ă aleatorie când se inițiază o transmisiune online cu opțiunea "New meeting";

Embed password in meeting link for one-click join (implicit On) – Parola transmisiunii va fi inclus ă în link-ul trimis ca invitație studenților printr-un mail. Elevii pot intra cu un singur click pe link-ul din mail-ul primit;
Mute participants upon entry (implicit Off) – Dezactivează automat microfoanele studenților care intră online. Profesorul poate alege dacă elevii își pot activa sau nu Audio în timpul transmisiunii online;
Upcoming meeting reminder (implicit Off) – Profesorul este notificat cu privire la următoarea transmisiune online pe care a planificat-o printr-un mesaj pe ecran;
Chat (implicit On) – Se permite participanților la transmisiunea online să trimită mesaje vizibile tuturor participanților;
Private chat (implicit On) Permite participanților să trimită mesaje private unuia dintre participanți **Auto saving chats** (implicit Off) – Permite salvarea automată a tuturor mesajelor de tip chat în timpul transmisiunii online;
Play sound when participants join or leave (implicit Off) – Semnal sonor la calculatorul profesorului la intrarea/ieș irea elevilor în/din transmisiunea online;
File transfer (implicit On) – Participanții pot trimite fișiere pe care ceilalți le pot descărca în timpul transmisiunii online;
Always show meeting control toolbar (implicit Off) – Afișează permanent meniul din partea de jos a ecranului;
Show Zoom windows during screen share (implicit Off) – Afișează ferestrele Zoom în timpul partajării ecranului;
Screen sharing (implicit On) – Permite participanților să partajeze conținutul ecranului în timpul transmisiunii online. Se poate specifica dacă poate partaja doar profesorul sau toți participanții;
Annotation (implicit On) – Permite participanților s ă folosească opțiunile din meniul "Annotate" în timpul partajării ecranului cu "Share screen";
Whiteboard (implicit On) – Permite participan ților să partajeze un whiteboard în timpul transmisiunii online;
Remote control (implicit On) – Permite participanților să preia controlul tastaturii și mouse-ului celui care partajeaz ecranul cu "Share screen";
Nonverbal feedback (implicit Off) – Permite afișarea în fereastra "Chat" a unor iconițe care exprimă diferite tipuri de aprecieri asupra activității online;
Allow removed participants to rejoin (implicit Off) – Permite elevilor înlăturați în timpul transmisiunii online să se reconecteze;

- **llow participants to rename themselves** (implicit On) – Permite participanților s ă-i redenumească numele din lista de participanți;
- **Breakout room** (implicit Off) – Permite profesorului să împartă participanții în grupuri mici în vederea intrării online;

Remote support (implicit Off) – Permite profesorului să aibă acces la tastatura și mose-ul unui elev;
Far end camera control (implicit Off) – Permite unui elev să preia controlul camerei video de pe calculatorul profesorului;
Virtual background (implicit On) – Permite orică rui participant s ă înlocuiască fundalul din imaginea sa video cu o imagine preluată dintr-un fiș ier format grafic;
Only show default email when sending email invites (implicit Off) – Permite utilizatorului s ă invite participanți prin e-mail folosind un anumit program de po ștă electronică e-mail;
Waiting room (implicit On) – În momentul intrării online fiecare student a ș teapt ă acceptul profesorului care va folosi opțiunea "Admit" pentru a permite intrarea online;

Show a "Join from your browser" link (implicit Off) – Permite utilizatorului să se conecteze online direct din browser-ul internet fără să instaleze aplicația zoom. Această variantă are facilități limitate
When attendees join meeting before host (implicit On) – Anunță profesorul când elevii se conectează înainte de conectarea sa;
When a meeting is cancelled (implicit On) – Anunță elevii că transmisiunea online a fost anulată

IMPORTANT:

- La instalarea programului Zoom, in funcție de programul de Antivirus folosit, pentru download-ul fișierului de instalare este necesară dezactivarea timp de 10 minute a programului de Antivirus.
- La transmiterea de către profesor a invitației pe mail, programul are un mic neajuns în sensul că nu activează link-ul trimis și deci elevul nu poate selecta acest link. Pentru a înlătura acest neajuns este suficient de introdus <ENTER> la sfârșitul link-ului pentru a-l activa.

SECURITATE ȘI BUNE PRACTICI ÎN ON-LINE

Din punct de vedere al securității platformelor, fiecare a avut probleme la un moment dat, dar în general sunt sigure și nu necesită cunoștințe avansate în domeniu, doar bunele practici generale cu privire la parole și protecția datelor personale.

Navigare mai sigură pe internet:

- se 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 (încearcă să folosești opțiunea NotScript sau NoScript);
- verifică secțiunea de contact a site-urilor web (adresă, număr de telefon, e-mail);
- verifică destinația reală a link-urilor prin trecerea cursorului mouse-lui peste acesta și vizualizarea adresei reale în partea stângă-jos a browser-ului;
- atenție la ce plugin-uri instalezi, de multe ori acestea vin însoțite de software malițios;
- nu apăsa pe link-urile din cadrul ferestrelor de tip pop-up;
- verifică existenta „https://" în partea de început a adresei web, înainte de a introduce informații personale.

Siguranța datelor unui sistem PC/laptop

Cea mai importantă variabilă în siguranța datelor stocate pe un PC/laptop este existența conexiunii acestuia la internet. Majoritatea sistemelor PC de azi vor fi conectate la internet, internetul fiind necesar desfășurării activităților zilnice. Menținerea unui sistem offline elimină riscul de atac cibernetic dar, nu asigură siguranța împotriva pierderii de date. Defectarea unității de stocare va duce automat la pierderea informației. Și atunci, cea mai bună și sigură cale de a evita un asemenea incident este crearea de copii de siguranță pe alte unități de stocare.

Dacă se dorește protejarea datelor și împotriva furtului fizic al dispozitivului de stocare, datele pot fi criptate. Sistemele de operare moderne permit acest lucru, Windows de exemplu folosește BitLocker (o aplicație standard preinstalată în versiunea Pro a Windows 10), datele odată criptate pot fi accesate doar furnizând parola stabilită în momentul criptării.

Navigarea pe Internet și confidențialitatea

V-ați întrebat vreodată dacă se vede pe ce site-uri intrați și ce e-mail-uri trimiteți? Răspunsul este da. Informația de la sursă la destinație călătorește prin multe noduri de comunicație, gestionate de Internet Service Provider (ISP) sau instituții sau chiar organizații guvernamentale. Un ISP ca să poată gestiona comunicațiile web, va putea ști sursa și destinația pachetelor sau datelor transmise. Voi exemplifica câteva situații uzuale și alternativele:HTTP sau HTTPS?

Este foarte simplu. O conexiune HTTP nu criptează datele transmise, majoritatea browserelor moderne vă vor anunța în momentul în care o conexiune este nesigură (HTTP). Nesigură înseamnă ca datele transmise pot fi vizibile de oricine care „ascultă" pe traseul pachetelor de date.

Conexiunea HTTPS folosește o criptare a datelor ce permite comunicarea sigură de la sursă la destinație, fără a fi vizibile unui terț.

Chiar dacă navigați internetul în mod „Privat" cum există posibilitatea în browserele moderne, acest mod vă protejează de urmărire prin intermediul site-urilor, dar furnizorul de internet va putea ști oricum pe ce site-uri intrați.

În momentul în care accesați un site, există câteva etape ce permit stabilirea legăturii și mai apoi transferul de informații. Unul dintre acești pași estetransformarea numelui site-ului (de ex uvt.ro) în adresa IP a serverului (de ex 193.230.241.1). Rețelele funcționează doar comunicând de la adresa IP la IP . Numele unui site există doar pentru a ușura reținerea de către utilizatori a adresei.

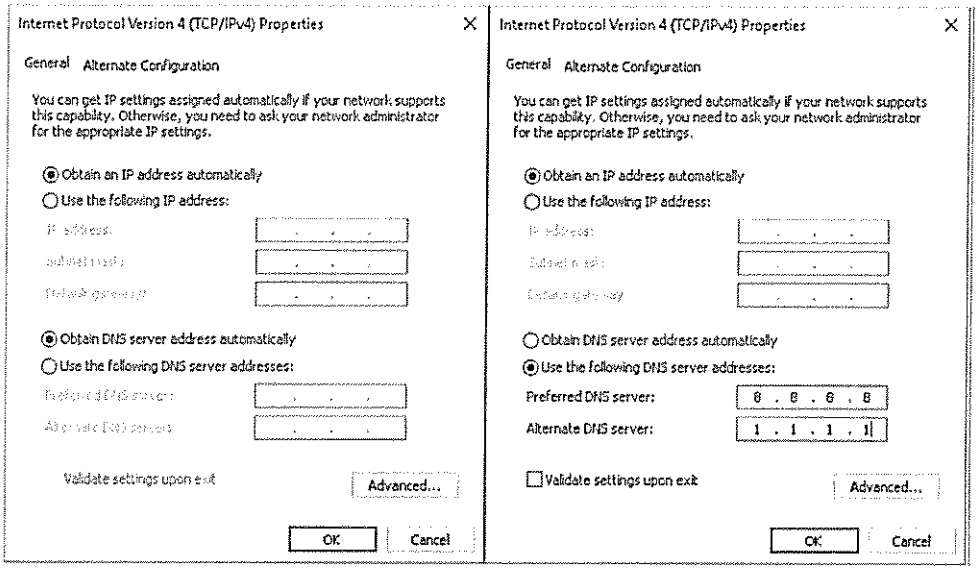
Transformarea numelui site-ului introdus de utilizator în adresa IP o face un server DNS (domain name server).

Verificarea browser-ului și asigurarea protecției navigării online

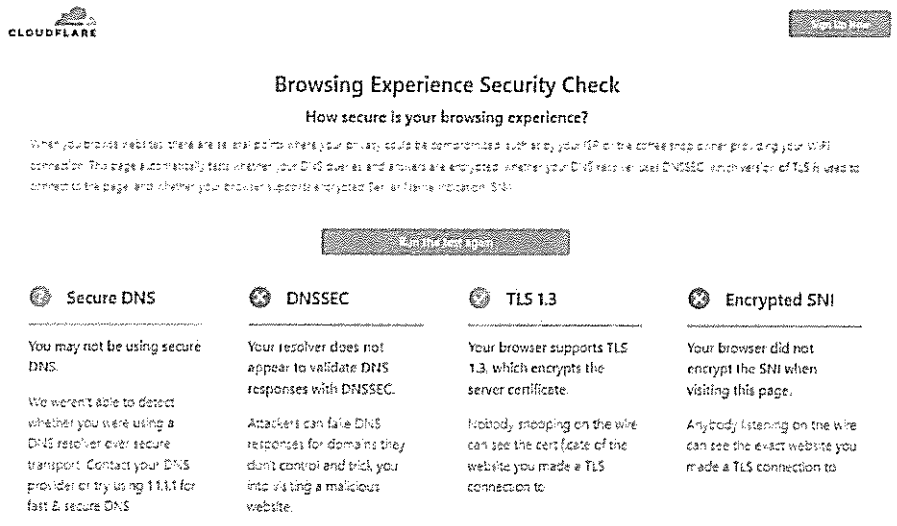
Există câteva ajustări ce se pot face pentru a ne asigura siguranța comunicației pe internet.

Se poate schimba serverul DNS de la care se fac interogările adreselor paginilor web, trecând de la cel al ISP-ului la unul global, cum e cel de la Google (8.8.8.8) sau Cloudflare (1.1.1.1)

Pentru browser, se poate face o verificare folosind un utilitar online la adresa cloudflare.com/ssl/encrypted-sni/ . În funcție de setările browser-ului, verificare poate returna rezultate după cum urmează:



Mai jos observăm că utilitarul ne-a raportat existența unor elemente nesigure în configurație.



Securitatea rețelei, comunicațiilor online

Hackerii (infractori cibernetici) sau utilizatorii neatenți pot să compromită rețelele de calculatoare și datele. Securitatea rețelei este alcătuită din hardware, software, politici și proceduri concepute pentru a apăra împotrivaamenințărilor interne și externe ale sistemelor informatice ale companiei sau instituției. Mai multe straturi de hardware și software pot preveni amenințările și deteriorarea rețelelor de calculatoare și pot împiedica împrăștierea acestora în cazul în care acestea intră în defensivă.

Amenințări frecvente la adresa sistemelor dvs.:

- Viruși, viermi, troieni, spyware, malware, adware și botnet-uri
- Atacuri „zero hour"
- Atacuri hacker
- Denial of Service (DoS) și Atacuri Distructive Denial of Service (DdoS)
- Furtul de date.

Aceste amenințări pot să exploateze:

- Rețele fără fir nesecurizate
- Software-ul și hardware-ul neprotejat
- Site-uri web nesecurizate
- Aplicații potențial nedorite (PUA)
- Parole slabe
- Dispozitive pierdute
- Utilizatorii nepricepuți sau rău intenționați.

Obțineți ultimele actualizări sau patch-uri.

Cyber-criminalii exploatează vulnerabilitățile din sistemele de operare, aplicațiile software, browserele web și plug-in-urile de browser atunci când este oprită aplicarea de patch-uri și actualizări.

În special, verificați dacă computerele rulează versiunile curente ale acestor programe foarte utilizate:

- AdobeAcrobat și Reader
- Adobe Flash
- Oracle Java
- Microsoft Internet Explorer
- Microsoft Office Suite

Păstrați un inventar pentru a vă asigura că fiecare dispozitiv este actualizat în mod regulat, inclusiv dispozitive mobile și hardware de rețea. Și asigurați-vă că Windows și celelalte dispozitive mobile utilizate au activată actualizarea automată.

Utilizați parole puternice

Definiția unei parole puternice este una dificil de detectat de oameni și de computere, este de cel puțin 6 caractere, de preferință mai mult, și utilizează o combinație de litere mari, mici și simboluri.

Symantec oferă sugestii suplimentare:

- Nu utilizați niciun cuvânt din dicționar. Evitați, de asemenea, substantive sau cuvinte străine.
- Nu utilizați numele, pseudonimul, al unor membri ai familiei sau animalele de companie.
- Nu folosiți numere pe care cineva le-ar putea ghici, ca numere de telefon și numere din adresa personală.

Autentificarea cu mai mulți factori este cea mai sigură metodă de autentificare a identității. Cu cât sunt mai mulți pași pe care utilizatorii trebuie să le ia pentru a-și dovedi identitatea, cu atât mai bine. De exemplu, în plus față de o parolă, utilizatorii ar putea fi obligați să introducă un cod PIN.

Utilizați e-mailurile bazate pe „cloud" și partajarea de fișiere în loc de VPN.

- Creați și impuneți politici de acces la utilizatori. Fii atent când acordați acces elevilor/preșcolarilor.
- Înainte de a acorda dispozitivelor mobile acces complet la rețea, verificați-le pentru software-ul antivirus actualizat, firewall-uri și filtre de spam.

Eliminați conturile inactive

Hackerii utilizează conturi inactive pentru a avea acces și a-și deghiza activitatea.

Atacurile de tip „phishing"

Un atac de „phishing" are loc atunci când cineva încearcă să vă determine să îi dezvăluiți informații personale online. Atacurile de phishing au loc de obicei prin e-mail, prin anunțuri sau prin site-uri care arată la fel ca site-urile pe care le accesați în mod obișnuit. De exemplu, puteți primi un e-mail care arată ca și cum ar fi de la banca dvs., în care vi se solicită să confirmați numărul contului bancar.

Informațiile pe care vi le pot solicita site-urile de phishing

- Numele de utilizator sau parolele
- Coduri numerice personale
- Numerele conturilor bancare
- Coduri PIN (numere de identificare personală)
- Numerele cardurilor de credit
- Numele dinainte de căsătorie al mamei dvs.
- Ziua dvs. de naștere

Cum evitați atacurile de phishing

De fiecare dată când primiți un mesaj de la un site care vă solicită informații personale, inclusiv un simplu login, trebuie verificate câteva informații și urmăriți niște pași. În cazul în care primiți un astfel de mesaj, nu oferiți informațiile solicitate fără să verificați dacă site-ul respectiv este legitim (în primul rând adresa lui). Dacă este posibil, deschideți site-ul în altă fereastră în loc să dați clic pe linkul din e-mail.

Criptovirus (ransomware-ul)

Ransomware este un tip de malware din criptovirologie care amenință să publice datele victimei sau să blocheze permanent accesul la acestea, dacă nu se plătește o răscumpărare. În timp ce unele ransomware simple pot bloca sistemul într-un mod care nu este dificil pentru o persoană experimentată să elimine, malware-ul mai avansat utilizează o tehnică numită extorcare criptovială, în care criptează fișierele victimei, făcându-le inaccesibile și solicită o plată de răscumpărare pentru cheia de decriptare. Într-un atac de extorcare criptoviral implementat corect, recuperarea fișierelor fără cheia de decriptare este o problemă dificilă - și dificil de urmărit monedele digitale precum Ukash și criptocurrency sunt folosite pentru răscumpărări, ceea ce face dificilă urmărirea și urmărirea penală a făptuitorilor.

Cu Ransomware atacurile sunt de obicei efectuate cu ajutorul unui troian care este deghizat ca un fișier legitim că utilizatorul este înșelat în descărcare sau de deschidere atunci când ajunge ca un atașament de e-mail. Cu toate acestea, un exemplu de profil înalt, viermele "WannaCry", a călătorit automat între computere, fără interacțiunea cu utilizatorul datorită vulnerabilității serviciului SMBv1 din Windows (ce permite partajarea de fișiere în rețea).

BUNE PRACTICE ÎN FOLOSIREA DISPOZITIVELOR MOBILE

Cybercriminalii continuă să caute modalități de a exploata vulnerabilitățile din aplicații, sisteme de operare și software, încercând să valorifice defectele de securitate înainte ca producătorii să le găsească și să le elimine. Iată câțva dintre pașii simpli care pot fi făcuți pentru a vă proteja dispozitivul mobil:

- Actualizați periodic sistemul de operare și aplicațiile. Noi vulnerabilități sunt tot timpul descoperite, iar producătorii lucrează pentru a-și repara aplicațiile și software-ul de îndată ce acestea sunt sesizate. Pentru iOS, utilizatorii pot verifica actualizările de sistem din Setări> General> Actualizare software. Utilizatorii de Android pot căuta acest lucru în Setări> Despre> Actualizare sistem.
- Pentru a vă asigura că toate aplicațiile sunt actualizate, utilizatorii iOS pot accesa App Store pentru a verifica actualizările disponibile. Utilizatorii Android pot face același lucru accesând Magazinul Play.

- Utilizați funcțiile de securitate relevante integrate. Puteți îmbunătăți securitatea dispozitivului dvs. mobil utilizând aplicații încorporate anti-furt cum ar fi Găsiți iPhone-ul meu. Această aplicație vă poate ajuta să găsiți telefonul, să urmăriți unde este sau unde a fost și să ștergeți datele de la distanță în cazul în care nu puteți recupera dispozitivul. Utilizatorii pot activa funcția din Setări> Conturi și parole> iCloud> Găsiți iPhone-ul meu.
- Utilizatorii Android au aceeași caracteristică pe care o pot accesa la google.co.uk/android/devicemanager. Dacă doresc să șteargă datele dispozitivului și să îl păstreze blocat în cazul în care dispozitivul dispare, aceștia pot accesa Setări> Securitate> Administratorii de dispozitive și pot lăsa activat Managerul de dispozitiv Android.
- Aplicarea permisiunilor pentru aplicații. Aplicațiile uneori necesită mai mult decât permisiunile implicite de bază. Asigurați-vă că aplicațiile instalate au acces numai la funcțiile de care au nevoie. Examinați permisiunile pe care le este permis să le folosească ca actualizări și erori ulterioare și le-ar fi putut cauza scurgerea datelor de utilizator. Utilizatorii iOS pot configura această opțiune în Setări> Confidențialitate.
- Utilizatorii iOS pot accesa setările> ID-ul de atingere și codul parolă> Blocarea parolei pentru a dezactiva funcțiile care pot fi accesate chiar și atunci când ecranul de start este blocat. Pentru utilizatorii de dispozitive Android, aceștia pot limita informațiile care apar în notificări prin configurarea setărilor de notificare ale dispozitivului.
- Utilizatorii Android 8.0 pot verifica ce aplicații au permisiunile accesând Setări>Aplicații și notificări> Permisiunile aplicațiilor. De asemenea, utilizatorii pot acorda permisiuni pentru aplicații în timp ce aplicația rulează, ceea ce oferă mai mult control asupra funcționalității aplicației. Dacă o aplicație afișează un mesaj care spune că are nevoie de o anumită permisiune, utilizatorii pot decide în acel moment dacă este necesar.
- Serviciile de localizare sau setările, care de obicei fac parte din funcția de setări rapide a iOS și Android, permit aplicațiilor și site-urilor web să utilizeze informații din rețele celulare, Wi-Fi, GPS și Bluetooth pentru a determina locația aproximativă a utilizatorului. Când permiteți accesul la locație pentru dispozitivele iOS, este recomandat să selectați numai în timp ce utilizați aplicația în loc de tot timpul, deoarece împiedică o aplicație malware care poate rula în fundal să fure informațiile despre locația dispozitivului. Utilizatorii de sisteme Android pot evita riscul prin oprirea locației dispozitivului, în Setări.
- Evitați conectarea la rețele Wi-Fi nesigure. Dezactivați funcția de conectare automată Wi-Fi pe smartphone-urile sau tabletele dvs. Utilizatorii ar trebui să se abțină de la conectarea la hotspoturi publice deoarece nu sunt sigure și conectarea la acestea poate expune dispozitivul la o multitudine de riscuri. Dacă este necesară conectarea, evitați autentificarea în conturile cheie sau serviciile

financiare. Configurarea unui VPN reprezintă, de asemenea, o modalitate bună de a asigura datele trimise și primite online.

- Descărcați aplicații din surse de încredere. Anumite magazine de aplicații ale unor terțe părți s-au dovedit a fi probabil mai mari ca transportatorii de aplicații rău intenționate, așa că descărcați întotdeauna din surse de încredere. Fiți vigilenți și verificați comentariile de pe pagina aplicației, pentru a se asigura că este legitimă. Utilizatorii care folosesc aplicațiile de plată mobilă și de jocuri populare ar trebui, de asemenea, să fie precauți, deoarece au devenit în trecut ținte ale terorismului cibernetic.
- Cunoașteți riscurile de jailbreaking / rootkit. Producătorii plasează restricții de securitate și garanții pe dispozitivele lor pentru a proteja dispozitivele și datele utilizatorilor. Jailbreaking sau rootkit elimină aceste limitări, lăsând sistemul mai vulnerabil la malware și alte amenințări.
- Aveți grijă la apelurile sau mesajele nesolicitate. Atacatorii folosesc o varietate de metode pentru a determina utilizatorii să descarce programe malware sau să dezvăluie informații personale. Scanați sau verificați toatemesajele, apelurile sau e-mailurile de la expeditori necunoscuți înainte de a le deschide.
- Setați blocările automate pe dispozitivele mobile. Asigurați-vă că dispozitivul mobil se blochează automat și că are un cod de acces puternic - un model simplu sau o parolă de accesare rapidă nu oferă suficientă siguranță. Dacă un dispozitiv este pierdut sau furat, o parolă puternică împiedică pe oricine să acceseze rapid informațiile personale. Utilizarea caracteristicilor biometrice de autentificare, cum ar fi scanerul de amprente digitale și recunoașterea facială, fac deblocarea dispozitivului mult mai ușoară și îmbunătățesc securitatea.
- Limitați informațiile personale oferite aplicațiilor și site-urilor Web. Înscrierea pentru un serviciu nou sau descărcarea unei noi aplicații uneori necesită informații personale. Aveți grijă să nu dezvăluiți prea mult și să cercetați cât de sigură este aplicația sau site-ul înainte de a vă conecta.
- Gestionați ceea ce este partajat online. Asigurați-vă că utilizați setările de confidențialitate în aplicațiile și site-urile de socializare mass-media. Unele site-uri pot difuza publicului locația, e-mailul, numerele de telefon sau mai multe date în mod implicit.
- Utilizatorii ar putea, de asemenea, beneficia de soluțiile de securitate mobile pe mai multe niveluri, care pot proteja dispozitivele împotriva amenințărilor online, a aplicațiilor rău intenționate și chiar a pierderii datelor.

BIBLIOGRAFIE

- http://digital.educred.ro/
- "What is the difference between the Web and the Internet?". W3C Help and FAQ. W3C. 2009.
- "World Wide Web Timeline". Pews Research Center. 11 March 2014. Retrieved 1 August 2015. Dewey, Caitlin (12 March 2014).
- Ghid de bune practici pentru securizarea calculatoarelor și rețelelor personale (www.cert.ro)
- Ghid de Bune Practici Pentru Securitate Cibernetică (www.sri.ro)
- Dobrițoiu Maria – Instruire asistată de calculator și platforme educaționale on-line
- Mike Tabor - Enable DNS over HTTPS and Encrypted SNI in Firefox https://miketabor.com/enable-dns-over-https-and-encrypted-sni-in-firefox/
- Greg Mombert/Digital Trends - Android vs. iOS: Which smartphone platform is the best? https://www.digitaltrends.com/mobile/android-vs-ios/
- Apple and Samsung fined for slowing down phones with updates - https://www.cnet.com/news/apple-and-samsung-fined-for-slowing-down-phones-with-updates/
- Jeremy Dotson - HTTP vs. HTTPS: What's the Difference? https://biztechmagazine.com/article/2007/07/http-vs-https