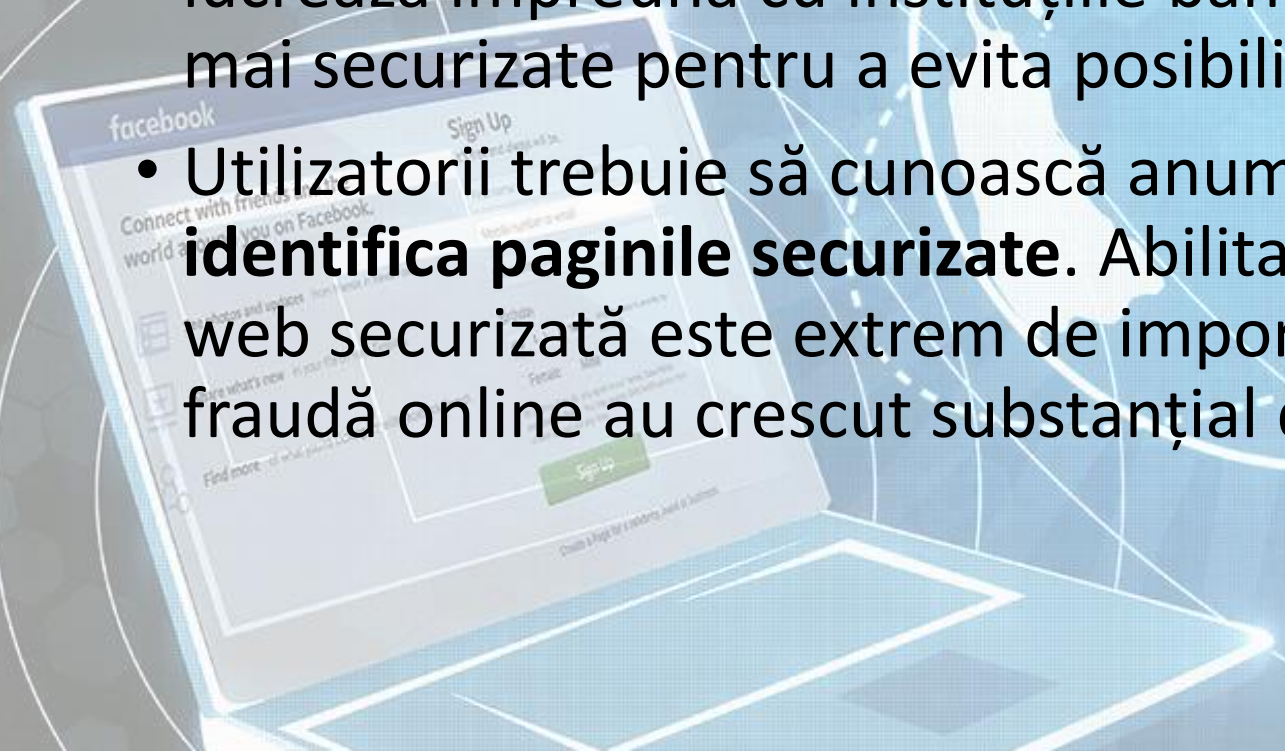
Utilizarea în siguranță a Internetului

4.1. Navigarea pe Internet

4.1.1. Conștientizarea faptului că activitățile online trebuie efectuate numai pe site-uri protejate. Identificarea unui site protejat

- Există foarte multe magazine online prin care companiile își promovează produsele sau le comercializează. Asigurarea securității tranzacțiilor online a devenit o problemă. Companiile de software lucrează împreună cu instituțiile bancare pentru a crea aplicații cât mai securizate pentru a evita posibilitatea de fraudă.
- Utilizatorii trebuie să cunoască anumite **reguli esențiale pentru a identifica paginile securizate**. Abilitatea de a recunoaște o conexiune web securizată este extrem de importantă deoarece cazurile de fraudă online au crescut substanțial de la an la an.

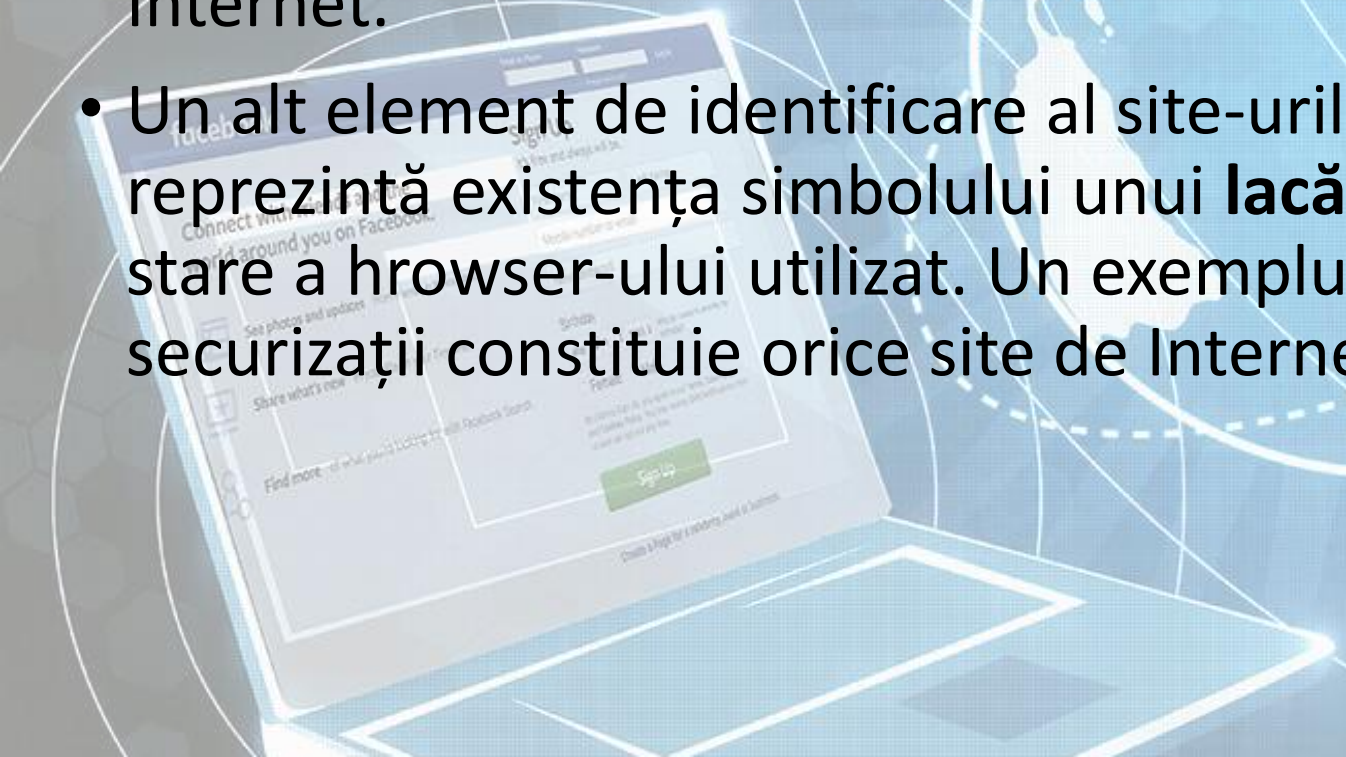


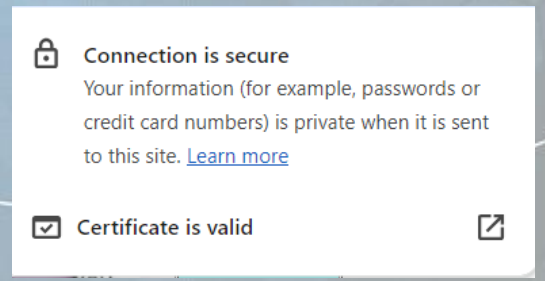
Activitățile online trebuie efectuate numai pe site-uri protejate.

- Pentru transmiterea securizată a datelor se recomandă **criptarea datelor**. În acest scop a fost creat **SSL** (Secure Sockets Layer), un **protocol web** dezvoltat pentru a transmite informații confidențiale prin Internet.
- Pentru a cripta datele, SSL utilizează un sistem criptografic cu **două chei**: una **publică**, cunoscută de oricine și una **privată**, secretă, cunoscută numai de destinatarul mesajului.
- Majoritatea browserelor web suportă SSL și multe site-uri web utilizează protocolul de utilizator pentru a transmite informații confidențiale, cum ar fi numerele cardurilor de credit.
- URL-ul care are nevoie de o conexiune SSL începe cu **https:** (în loc de **http:**).

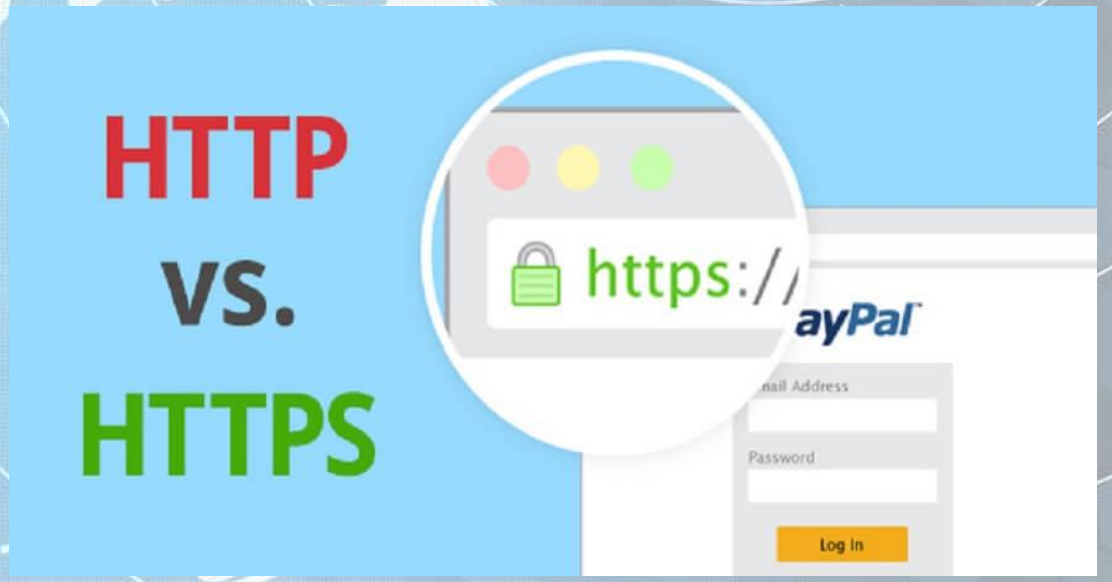
Identificarea unui site protejat

- Un site web securizat va fi identificat prin prezența textului **HTTPS** (Hyper Text Transfer Protocol Secure) în adresa sa.
- **Https** reprezintă un protocol ce oferă siguranță tranzacțiilor de pe Internet.
- Un alt element de identificare al site-urilor web securizate îl reprezintă existența simbolului unui **lacăt** în bara de adrese sau de stare a hrowser-ului utilizat. Un exemplu de astfel de site web securizații constituie orice site de Internet Banking.



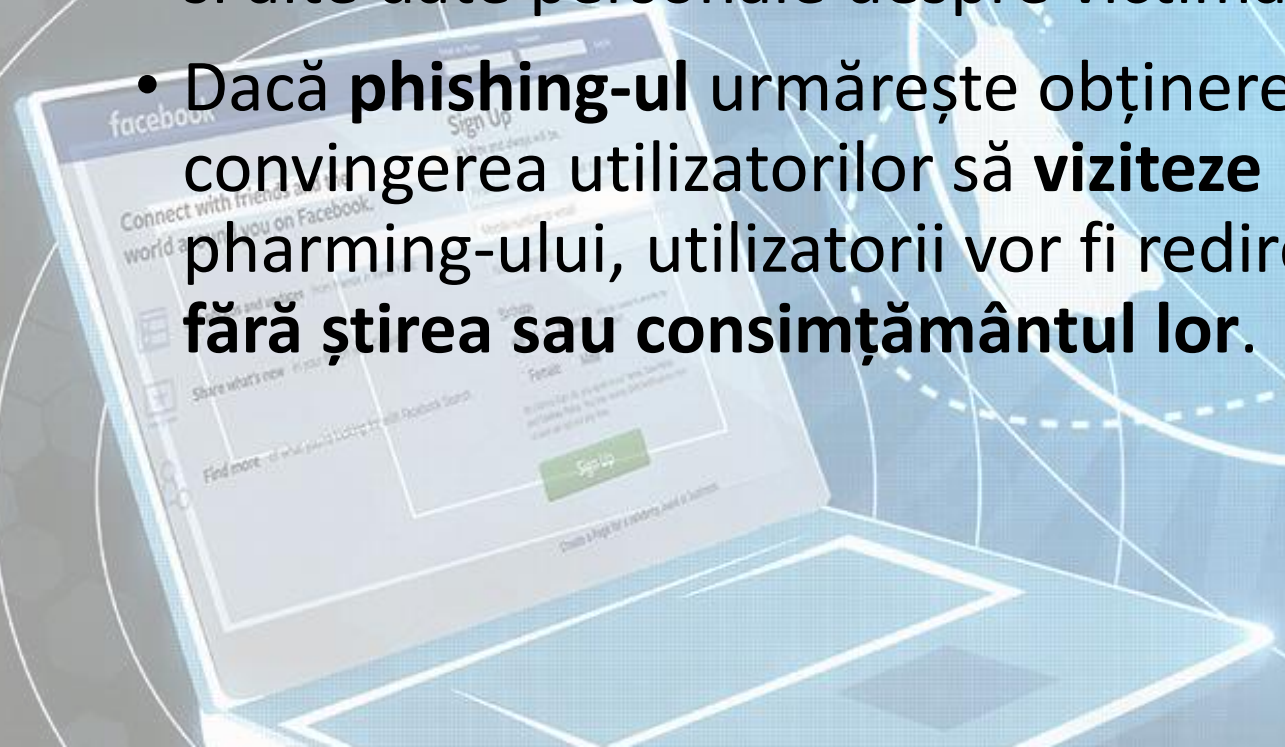


- Pentru un plus de securitate, este recomandat ca, la finalul sesiunii de lucru într- o sesiune securizată, să vă **deconectați** (mai ales dacă vă aflați pe un computer public) pentru a evita furtul de date.



4.1.2. Conștientizarea termenului de pharming

- **Pharming** este un tip de atac informatic care implica redirecționarea traficului web destinat unui site web legitim către un site fals creat de atacatori cu scopul de a fura credențialele de login, informații bancare si alte date personale despre victima fără știrea și consimțământul .
- Dacă **phishing-ul** urmărește obținerea de informații confidențiale prin convingerea utilizatorilor să **viziteze** un site web fals, în cazul pharming-ului, utilizatorii vor fi redirecționați către un site **web fals fără știrea sau consimțământul lor**.



Diferența dintre pharming și phishing

- **Phishing-**ul păcălește oamenii pe rând, în timp ce **pharming**-ul face mai multe victime deodată**.** În atacul de tip pharming, nu este necesar să fie vizate persoanele **una câte una** și nu este necesară nicio acțiune conștientă din partea victimei.
- Într-o formă de atac pharming, un cod este trimis odată cu un e-mail, cod ce **modifică fișierele gazdă** pe un computer personal.
- Fișierele gazdă convertesc apoi URL-urile în șiruri de caractere numerice pe care calculatorul le utilizează pentru a accesa site-uri web.
- Un calculator cu un fișier gazdă compromis va merge pe un site-ul Web fals chiar dacă utilizatorul va tasta URL-ul corect sau va alege URL-ul din lista de site-uri favorite. Din această perspectivă, **atacurile de tip pharming sunt mai grave și mai greu de detectat**.

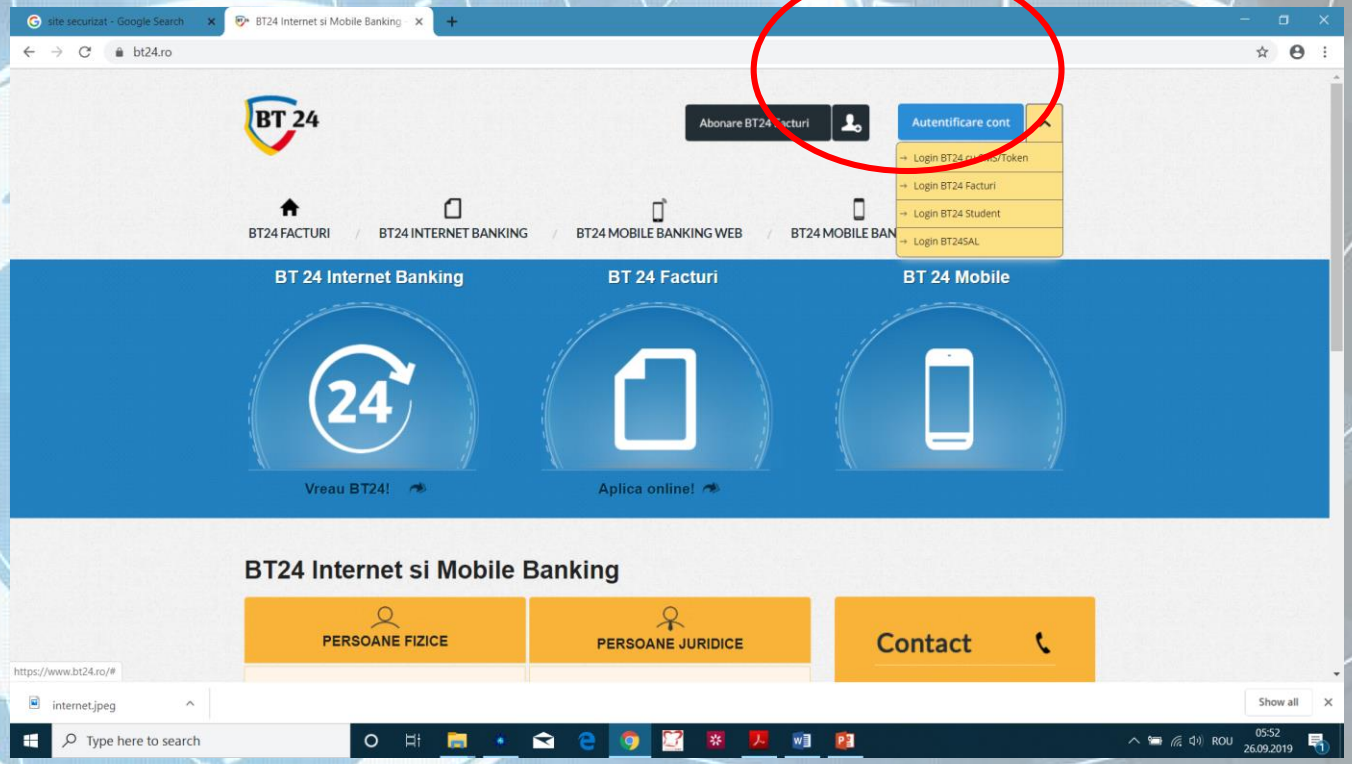
4.1.3. Înțelegerea termenului de certificat digital. Validarea unul certificat digital

- **Certificatul digital** reprezintă un instrument în stabilirea unui canal securizat pentru comunicarea informațiilor confidențiale. Certificatul digital este utilizat pentru o gamă variată de tranzacții electronice ce include: e-mail; comerț electronic, transfer electronic de fonduri.
- Certificatul digital este o semnătură electronică ce îmbracă două forme:
  - fie certificatul identifică expeditorul unui document
  - fie certificatul dovedește autenticitatea unui site Web către utilizatorii săi.
- În cazul **primei forme**, semnătura digitală este creată prin criptarea conținutului documentului, folosind cheia criptografică a expeditorului. Aceasta face ca semnătura să fie unică. Orice modificări aduse documentului afectează semnătura, oferindu-se astfel integritate. Certificatele sunt emise de autorități de certificare, care își asumă responsabilitatea pentru identificarea utilizatorilor și pentru acordarea cheilor.
- în cazul celei de **a doua forme**, certificatul se bazează pe recunoașterea sa de către autoritatea de certificare.

4.1.4. Înțelegerea termenului de "one-time password”

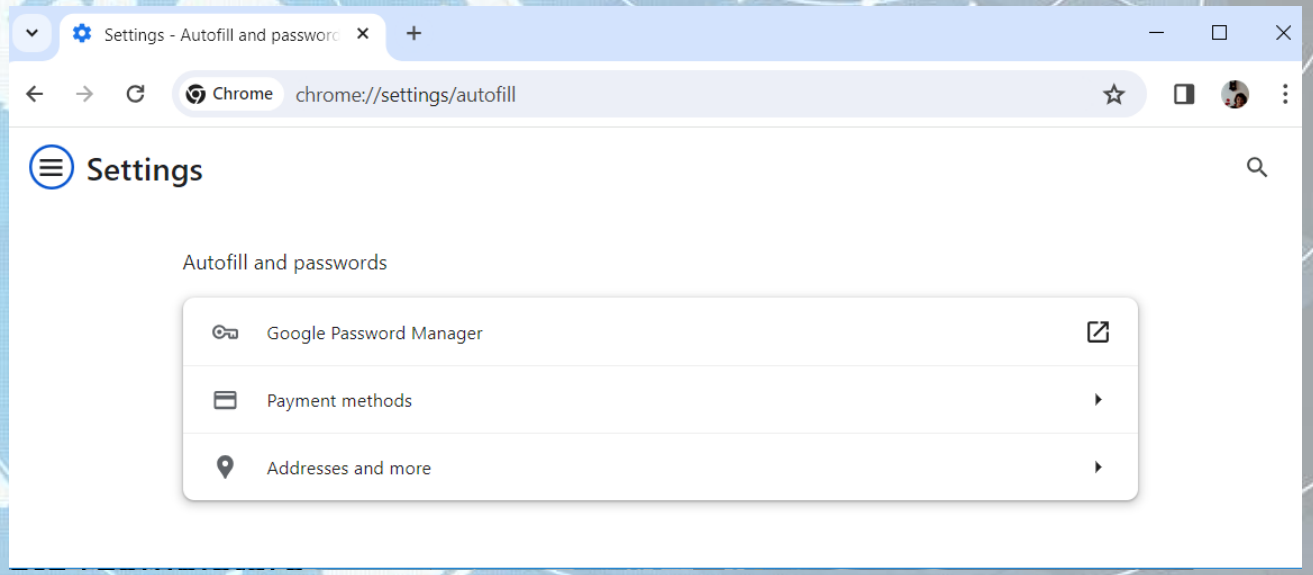
- **One-time password (OTP**) reprezintă un mecanism de logare la o rețea sau serviciu utilizând o parolă care este valabilă pentru o singură sesiune de conectare sau pentru o singură tranzacție. Acest lucru previne diferitele forme de furt de identitate prin faptul că această parolă este valabilă o singură dată. Acest tip de parolă oferă o securitate sporită, fiind folosită în tranzacții bancare, rețele corporatiste sau alte sisteme bazate pe date confidențale.
- De obicei, logarea se realizează pe baza unui nume de utilizator (care se menține mereu același) și a OTP, care se schimbă de fiecare dată.
- OTP evită o serie de deficiențe specifice parolelor tradiționale (statice). În cazul parolelor statice, acestea sunt extrem de expuse atacurilor cibernetice de tip phishing , keyboard logging etc. Spre deosebire de parolele statice, OTP nu este vulnerabil la atacurile de reluare. Acest lucru înseamnă că un potențial intrus care reușește să înregistreze o OTP, care a fost deja folosită pentru conectarea la un serviciu sau la efectuarea unei tranzacții, nu va fi capabil să abuzeze de ea, deoarece aceasta nu va mai fi valabilă.

- Parolele de tip OTP pot fi generate în diverse moduri, cea mai cunoscută și convenabilă metodă fiind utilizarea unui **token** (dispozitiv electronic capabil să genereze astfel de parole).
- Majoritatea token-urilor sunt protejate și prin codul PIN al utilizatorului, oferind o protecție suplimentară.



4.1.5. Stabilirea setărilor corespunzătoare pentru activarea, dezactivarea opțiunilor de completare și salvare automată în cadrul unui formular

- Pentru a completa automat datele de fiecare dată când se utilizează un formular online, se poate folosi opțiunea **AutoComplete** (Completare automată) oferită de browser-ul web.

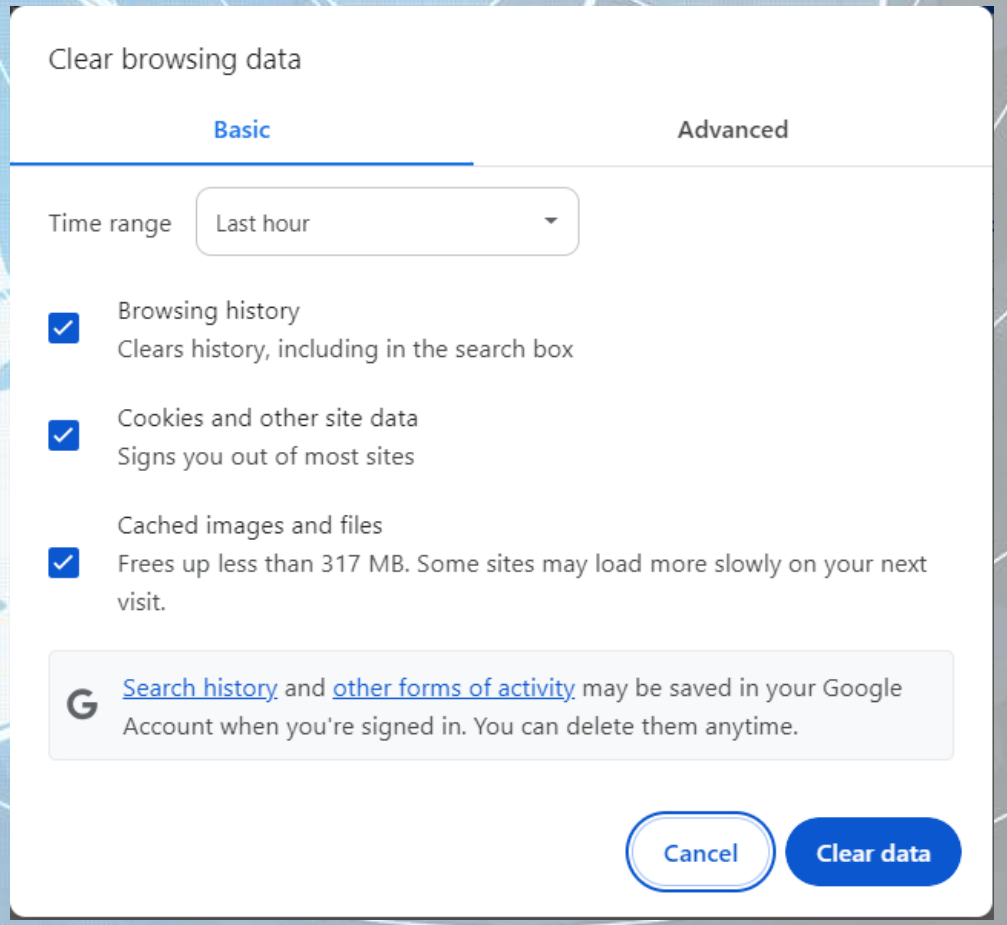


4.1.6. Înțelegerea termenului cookie

- Un Cookie (cunoscut și sub denumirea de "browser cookie" sau "HTTP cookie" sau "Internet cookie") este un fișier de mici dimensiuni, format din litere și numere, stocat pe computerul unui utilizator care accesează Internetul.
- În cadrul unui cookie, se păstrează informații referitoare la opțiunile și particularitățile utilizatorului astfel încât, la o a doua vizitare a site-ului respectiv, particularitățile să fie încărcate automat.
- Cookie-urile sunt folosite pentru autentificare, pentru următărirea comportamentului utilizatorilor și reținerea preferințelor acestora
- Un cookie nu conține programe software, viruși sau spyware și nu poate accesa informațiile de pe hard disk-ul utilizatorului.
- Cookie-urile pot fi folosite pentru scopuri negative deoarece stochează informații despre preferințele și istoricul de navigare al utilizatorilor, cookie-urile pot fi folosite ca o formă de spyware.
- În cazul în care la computerul dvs au acces și alte persoane, puteți seta browser- ul pentru a șterge datele individuale de navigare de fiecare dată când închideți browser-ul.

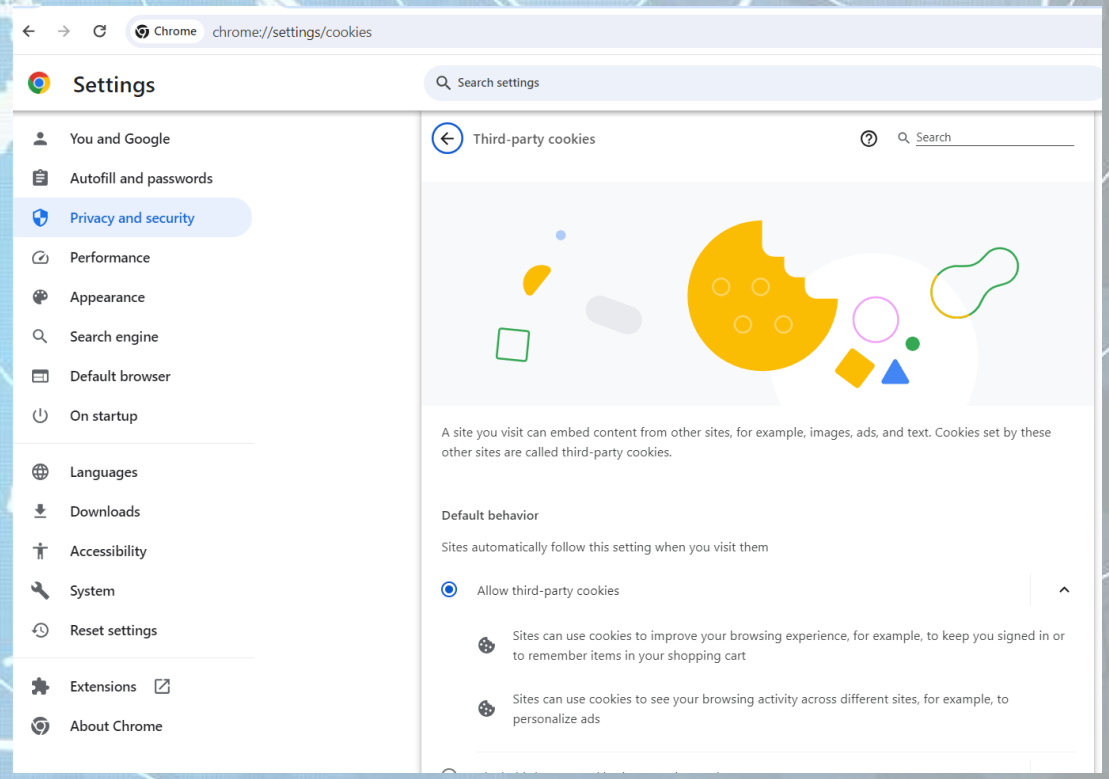
4.1.7. Stabilirea setărilor corespunzătoare pentru permiterea sau blocarea elementelor cookie

- Browser-ul de internet furnizează modalități de a controla modulele cookie stocate în computer. Ele se pot bloca sau permite sau se pot alege doar anumite site-uri de la care acceptați module cookie.



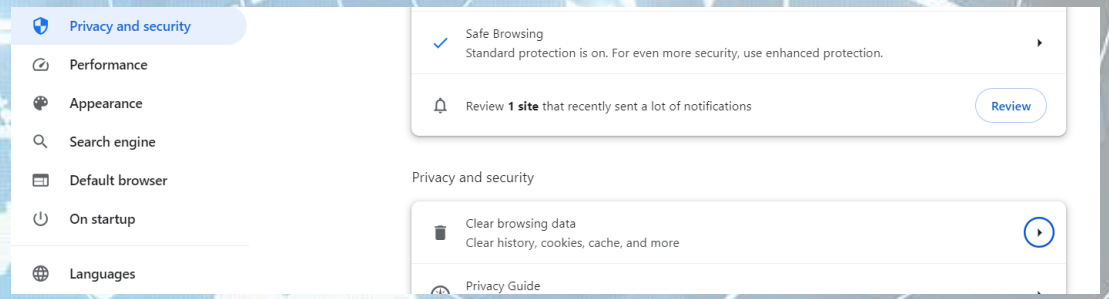
4.1.7. Stabilirea setărilor corespunzătoare pentru permiterea sau blocarea elementelor cookie

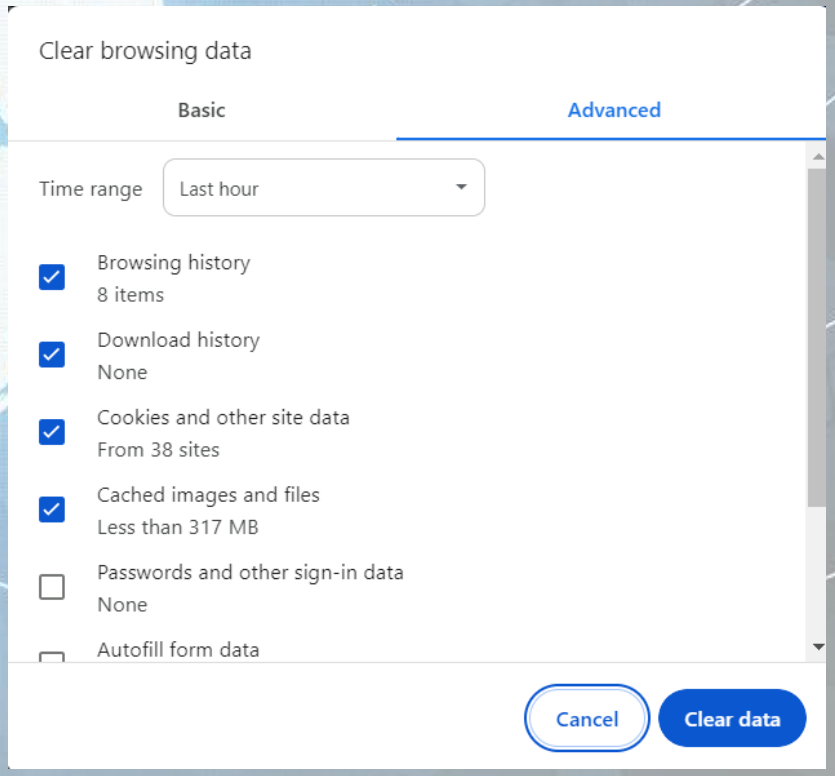
- Blocarea cookie-urilor nu înseamnă că nu veți mai primi publicitate online, ci doar că aceasta nu va mai putea ține cont de preferințele și interesele dvs, evidențiate prin comportamentul de navigare.
- La efectuarea acestor modificări, modulele cookie care sunt deja stocate în computer nu vor fi afectate. Din acest motiv, este bine să ștergeți modulele cookie stocate deja în computer înainte de a face setările pentru blocare.



4.1.8. Ștergerea datelor private dintr-un browser web, precum: istoric pagini vizitate, fișiere cache, parole, cookie, date autocompletate

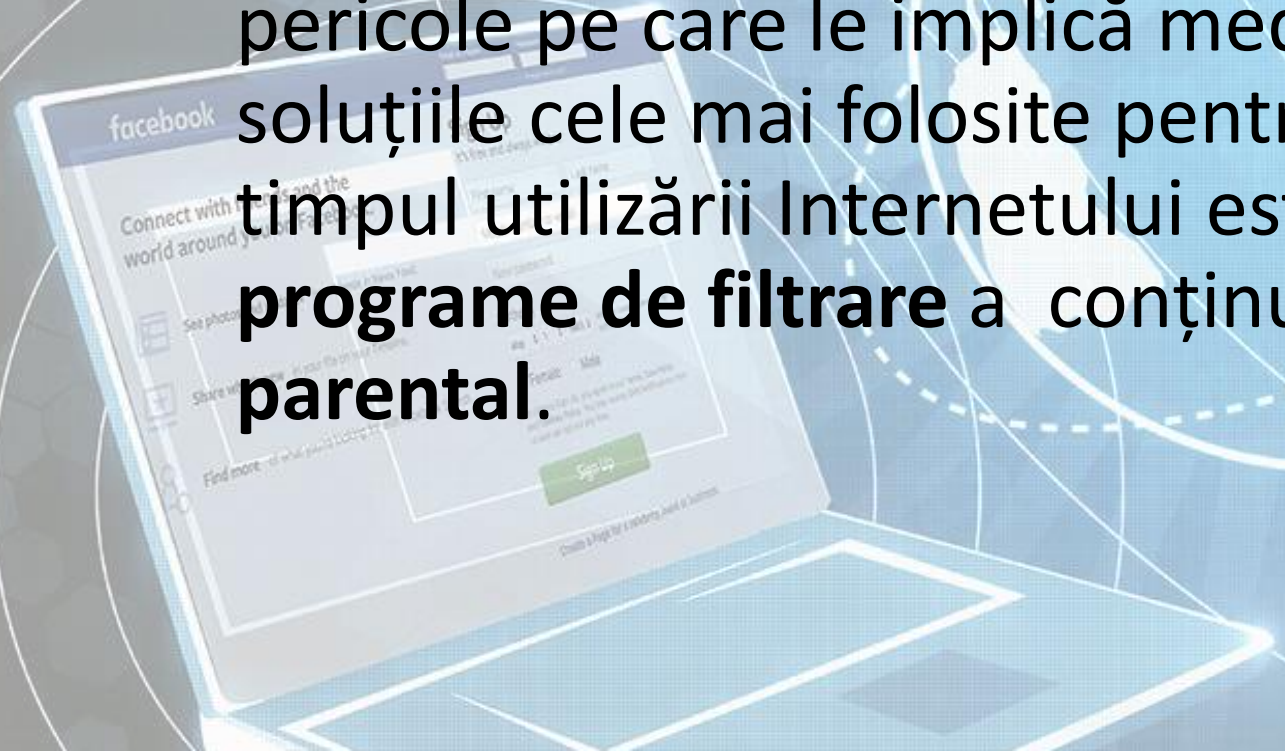
- Când același calculator este folosit de mai multi utilizatori esre recomandabilă ștergerea datelor private
- În secțiunea Privacy and seurity, se bifa acele opțiuni dorite din **Clean browsing data** (Ștergere istoric navigare)
- **După** bifarea opțiunilor dorite, se apasă butonul **Clear data.**





4.1.9. Înțelegerea scopului, funcției și tipurilor de aplicații software pentru controlul conținutului: aplicații de filtrare a paginilor web, aplicații de control parental

- Copiii folosesc Internetul pentru diverse activități: e-mail, teme, căutări pe Internet, jocuri online, rețele de socializare, mesagerie instantanee, supunându-se unor pericole pe care le implică mediul virtual. Una din soluțiile cele mai folosite pentru protejarea copiilor în timpul utilizării Internetului este folosirea unor **programe de filtrare** a conținutului web și de **control parental**.



- Aceste programe sunt disponibile contra cost sau gratuit și pot fi instalate pe calculatorul copiilor sau pot controla profilul copiilor de pe calculatorul familiei.
- Se recomandă în mod special setarea unor **profile (users) separate pentru copii** și utilizarea unor astfel de programe, atunci când părinții nu pot fi în permanență în apropierea copiilor în timp ce aceștia folosesc Internetul.
- **Programele de filtrare** reprezintă soluția de bază pentru a bloca accesul la anumite site-uri web care sunt susceptibile de a include publicitate nedorită, conținut pornografic, spyware, viruși și alte tipuri de conținut inacceptabil.
- Filtrarea se face pe baza unor **liste de adrese** sau **cuvinte restricționate**. Astfel, se blochează accesul la anumite site uri sau pagini web, în funcție de adresa sau de conținutul acestora.

- **Programele de control parental** sunt caracteristici care pot fi incluse în serviciile digitale de televiziune, computer și jocuri video, telefoane mobile și software. Programele de Control Parental reprezintă o **soluție completă pentru protejarea copiilor în timpul utilizării Internetului** și controlul activității acestora pe calculator șl Internet
- Ele oferă următoarele facilități:
  - blochează accesul la anumite pagini sau site-uri, pe baza unei liste predefinlte de cuvinte sau adrese interzise
  - permite accesul doar la anumite site-uri, pe baza unei liste predefinite de adrese acceptate
  - limitează timpul petrecut de copii pe calculator și/sau Internet, prin stabilirea unor intervale orare în care copilul poate avea acces la acestea;
  - limitează tipurile de programe și fișiere care pot fi descărcate și instalate pe calculator;
  - blochează accesul la anumite fișiere sau partiții de pe calculator;
  - limitează sau blochează accesul la setările calculatorului
  - limitează sau blochează utilizarea unor programe de către copii
  - întocmește rapoarte periodice cu activitatea copiilor pe calculator.