INSTITUTUL DE CERCETARE ȘI
PREVENIRE A CRIMINALITĂȚII

SIGURANȚA PE INTERNET

POLIȚIA ROMÂNĂ

INSTITUTUL DE CERCETARE ȘI PREVENIRE A CRIMINALITĂȚII

2024

INTRODUCERE

Criminalitatea informatică sau cybercriminalitatea reprezintă în prezent una dintre principalele amenințări la adresa siguranței publice, fiind o problemă în expansiune și din ce în ce mai agresivă în majoritatea statelor membre ale Uniunii Europene[1].
Deși utilizat frecvent, termenul de cybercrime (sau, folosit sinonim acestuia, criminalitate informatică) reclamă unele precizări. Conceptul de cybercrime nu presupune în mod obligatoriu derularea întregului lanț de acțiuni în mediul virtual. Astfel, din literatura de specialitate putem distinge următoarea dihotomie:

- Infracțiuni dependente de mediul online (cyber-dependent crimes): infracțiunile care au apărut odată cu progresul tehnologic, în absența căruia nu pot exista și care, în consecință, nu pot fi săvârșite în context fizic;
- Infracțiuni derulate prin intermediul mijloacelor digitale (cyber-enabled crimes): infracțiunile tradiționale, care existau înainte de existența internetului și care sunt facilitate de acesta.

Pentru mai multă claritate, ilustrăm transpunerea unor infracțiuni din spectrul clasic în mediul virtual:

Categorie	Tipar clasic	Tipar virtual
Infracțiuni împotriva proprietății/ patrimoniului	Înșelăciune Fals Furt de identitate	Spam Phishing Catfishing (înșelăciunea ori șantajul prin intermediul unei identități virtuale false)
Violență interpesonală	Hărțuire Șantaj	Trolling Cyberbulling Șantaj prin intermediul sistemelor informatice
Violență sexuală	Abuzul sexual împotriva copilului Ademenirea copilului în scop sexual Utilizarea fără drept a imaginilor cu caracter sexual	CSAM (child sexual abuse materials) markets Grooming online Revenge porn (deseori însoțit de fenomenul doxxing*) Sextortion**
Crimă organizată	Vânzarea de articole ilegale Spălare de bani	Portaluri de vânzări Dark web Cărăuși de bani Mixing de criptomonede

*Prin doxxing se înțelege expunerea online a datelor personale ale unei persoane fără acordul acesteia (de ex: nume, adresă, loc de muncă etc.)

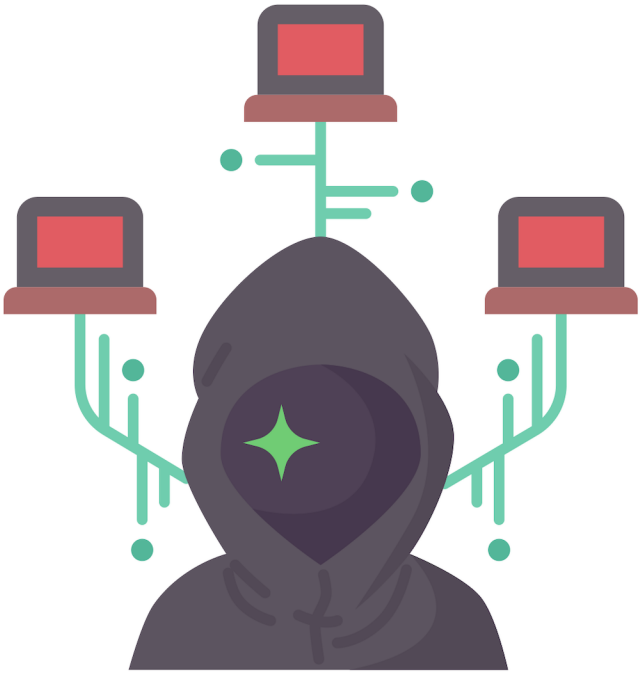
** Prin sextortion se înțelege amenințarea cu publicarea unor informații de natură sexuală cu scopul de a determina victima să aibă un anumit comportament (să îi dea bani etc.)

[1] Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

În cadrul unui demers investigativ susținut de Comisia Europeană[1] sunt prezentați factorii de risc ai criminalității informatice:

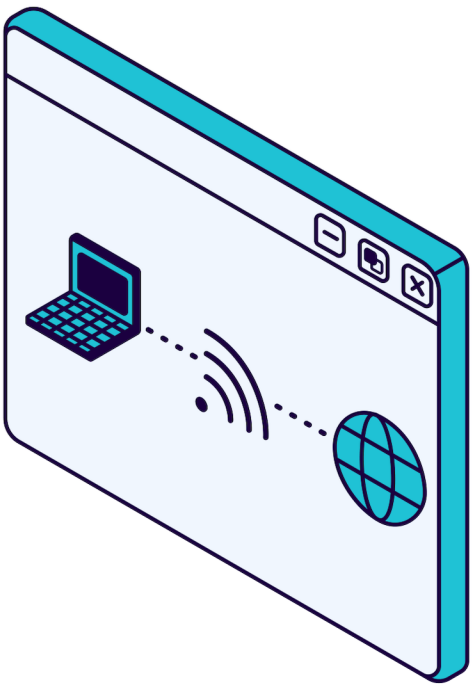
- **Vulnerabilitățile** legate de **software** sau, în unele cazuri, **hardware**: erori de scriere a codului inițial, cu potențial de rectificare în viitorul apropiat (ceea ce în termeni de specialitate se numește bug), dar care constituie o breșă exploatată de infractorii cibernetici.
- **Anonimizarea**: posibilitățile extinse de ascundere a identității pe care le au infractorii din mediul virtual (aplicații, facilități de tip VPN, Dark Web, rețele anonimizate).
- Apariția și extinderea **criptomonedelor**: piața cripto este evaluată în prezent la peste un trilion de dolari, însă tranzacțiile sunt rulate fie sub pseudoidentitate virtuală, fie în cvasiabsența unor elemente de identificare. În condițiile în care piața cripto este foarte puțin reglementată sau chiar lipsită de reglementări, posibilitățile autorităților polițienești de a acționa sunt reduse dramatic.
- **Cybercrime-as-a-service**. În ultimii ani, criminalitatea informatică a dobândit un accentuat caracter industrial, sub acest aspect înscriindu-se conceptul de „cybercrime-as-a-service". Astfel, infractorii informatici care dețin cunoștințe avansate în domeniul digital își pun la dispoziție serviciile tehnice în favoarea unor sume de bani, către alți utilizatori. Astfel de practici conduc la schimburi de know-how între indivizi cu preocupări și capacități similare, favorizând ceea ce putem numi capacitatea infracțională a acestora și posibilitatea apariției unor celule de colaborare. Deja arhicunoscutul DarkWeb pune la dispoziția utilizatorilor forumuri și platforme de tip marketplace, cunoscute în literatura de specialitate drept „hacker shops" și destinate exclusiv tranzacționării instrumentelor și cunoștințelor în scopul comiterii infracțiunilor informatice.

[1]Julia Davidson, Mary Aiken, Kirsty Phillips, and Ruby Farr, 2022, Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour, University of East London, https://www.ccdriver-h2020.com/files/ugd/0ef83d_a8b9ac13e0cf4613bc8f150c56302282.pdf



- **Controlul tuturor facilităților** pe care tindem să le legăm ideii de viață modernă, normală, civilizată (alimentare cu apă, transport, energie) prin intermediul calculatoarelor: atacurile asupra infrastructurii critice, deși puțin cunoscute, pot avea efecte extinse asupra desfășurării normale a vieții de zi cu zi.

- **Extinderea căilor de atac**: extinderea gamei de dispozitive inteligente conectate la internet a deschis, pe lângă numeroasele facilități destinate publicului larg, noi orizonturi pentru răufăcători, generând noi ținte pentru aceștia.



MOTIVAȚIE

- Datele existente pe plan internațional arată o incidență mare a actelor infracționale din sfera cibernetică în rândul adulților. Astfel, un studiu derulat la nivel global în perioada noiembrie-decembrie 2022 pe un eșantion de 7.021 de adulți din Australia, Franța, Germania, India, Japonia, Noua Zeelandă și Marea Britanie și în ianuarie 2023 pe un eșantion de 5.004 de adulți din Statele Unite a arătat faptul că *41% dintre* respondenți au avut computerul sau dispozitivul mobil infectat cu viruși, 35% s-au confruntat cu tentative de înșelăciune prin intermediul dispozitivului mobil/ prin SMS, 30% cu acte de phishing, 24% au primit un e-mail de șantaj, 23% s-au confruntat cu spargerea contului de pe rețelele de socializare, 20% cu spargerea contului de e-mail, 13% au avut de-a face cu un atac de tip răscumpărare (ransomware) și 10% dintre respondenți au avut profilurile de pe rețelele de dating piratate[8].

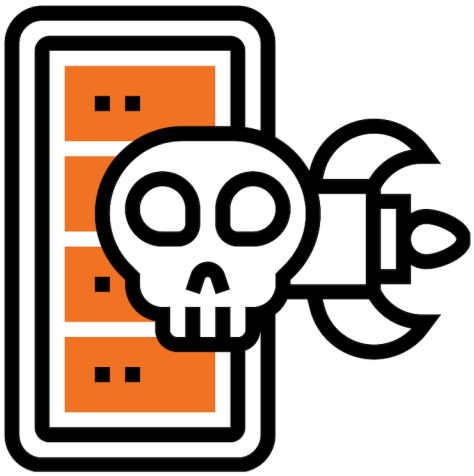
- Conform datelor Agenției Americane de Securitate Informatică și de Siguranță a Infrastructurii, *în Statele Unite* una din trei locuințe în care există computer s-a confruntat cu infectarea cu softuri malițioase, 47% dintre americani au avut datele personale făcute publice de către infractorii cibernetici, în timp ce, la nivel global, se estimează că utilizatorii au pierdut aproximativ 358$ și 21 ore în fiecare an pentru a se confrunta cu infracțiuni online[9].

[8] https://www.statista.com/statistics/1389306/cyber-crime-encounter-worldwide-by-type/

[9] https://www.cisa.gov/be-cyber-smart/facts

Sondajul online derulat de Censuswide pentru Kaspersky în 8 state europene (Marea Britanie, Franța, Spania, Portugalia, Grecia, Olanda, Germania și Italia) în perioada 03.01.2023-10.02.2023 pe 6.655 de adulți (respondenți de 16 ani și peste) atestă faptul că, deși adulții cunosc sau pretind că știu care sunt riscurile din mediul online, aceștia continuă să aibă o conduită ce îi vulnerabilizează:

- 74% postează informații personale (nume, locație) pe rețelele sociale;
- 66% au furnizat, în quizzurile de pe rețelele sociale, informații precum numele primului animal de companie, numele dinainte de căsătorie al mamei, numele străzii;
- 69% încă folosesc informații personale (precum numele echipei de fotbal favorite, numele primului animal de companie) pentru a-i ajuta să-și amintească parolele;
- 25% dintre tinerii cu vârste cuprinse între 25-34 de ani au fost victime ale phishing scam;
- Există un segment scăzut al celor care, după ce s-au confruntat cu o tentativă de phishing, au diseminat informații pentru a reduce riscul pentru ceilalți (21% dintre respondenții cu vârsta de 25-34 de ani și 15% dintre cei din intervalul 45-54 de ani) [10].



Un alt studiu, înscris proiectului CC-Driver [11], finanțat de Comisia Europeană, care a abordat proporțiile criminalității informatice în rândul tineretului cu vârste cuprinse între 16 își 19 ani din opt țări, printre care și România, a evidențiat multiple aspecte de interes pentru spațiul autohton.

Conform acestui studiu, 73% dintre respondenții din România au recunoscut că au comis cel puțin o formă de criminalitate informatică dintre cele 20 analizate sau au avut un comportament riscant ori la limita legii în mediul online, țara noastră poziționându-se pe locul 2 după Spania în ceea ce privește comportamentele deviante sau ilegale din mediul online.

[10] Kaspersky Report, 2023, Ignorance is Bliss: Most adults are leaving themselves open to cybercrime, despite knowing the dangers, https://media.kasperskydaily.com/wp-content/uploads/sites/86/2023/04/24175910/Kaspersky-Adult-consumer-Report-v5.pdf, accesat la 07.07.2023

[11] Davidson, J., Aiken, M., Phillips, K. and Farr, R. 2022. European Youth Cybercrime, Online Harm and Online Risk Taking: 2022 Research Report. London, United Kingdom Institute for Connected Communities, University of East London, disponibil la https://repository.uel.ac.uk/item/8v59y, accesat ;a 01.02.2024

- Prin prisma atributelor biologice și psiho-sociale (vârstă scăzută, lipsa unei maturități emoționale și cognitive depline), copiii au fost considerați un grup vulnerabil la pericolele din mediul virtual, aspect ce s-a transpus în mai multe studii și programe destinate creșterii siguranței online în rândul acestora, derulate de către Institutul de Cercetare și Prevenire a Criminalității în colaborare cu partenerii săi. Exemple în acest sens stau proiectele „Tu cui dai accept?”, „ROCyberex–Perfecționare, cooperare și prevenire în lupta împotriva criminalității informatice” sau „Eroii Internetului”.
- Populația adultă are însă, la rândul său, unele vulnerabilități în ceea ce privește utilizarea în siguranță a internetului, această situație fiind asociată, în principal, cu efectuarea unor operațiuni mai puțin răspândite în cazul copiilor (plăți, achiziții online), dar și cu existența unui segment al populației căruia îi lipsesc competențele digitale și care a început să utilizeze recent internetul, aspecte valabile mai ales atunci când vorbim de o populație cu o medie de vârstă ridicată.
- Analizând tendințele înregistrate în ultimii ani și schimbările provocate în rândul populației de pandemia de Covid-19, unele surse identifică tinerii sub 25 de ani ca grupul cel mai susceptibil a se confrunta cu tentative de fraudă online, în timp ce pe cel de-al doilea loc se situează persoanele vârstnice, cu precizarea că, pe măsură ce crește vârsta victimelor, cresc prejudiciile, astfel că populația vârstnică este cea mai vulnerabilă la a suferi pagube în urma unor fraude informatice[6].
- Datele din alte țări atestă o creștere a utilizării internetului în rândul populației vârstnice, aceasta fiind considerată a fi segmentul de populație în rândul căruia se înregistrează cea mai mare creștere a numărului utilizatorilor de internet[3]. De exemplu, în Marea Britanie, ponderea persoanelor de 55 de ani și peste care utilizează internetul a crescut de la 67% în 2015 la 81% în 2020[4].
- Și în România datele arată că între 2015 și 2020 numărul persoanelor cu vârsta de peste 55 de ani utilizatoare de internet crescuse cu 76%, iar între 2020 și 2023 cu încă 28%. Dacă în 2015 ponderea utilizatorilor de internet în rândul persoanelor vârstnice reprezenta 28%, aceasta crescuse la 65% în 2023[5].

[3] Dawes Centre for Future Crime at UCL, Older adults as victims of online financial crime, disponibil la https://www.ucl.ac.uk/future-crime/sites/future_crime/files/ucl_policy_briefing_-_older_people_and_financial_crime_december21.pdf, accesat la 07.07.2023

[4] ibidem

[5] Institutul Național de Statistică, TEMPO online, TIC108D – Persoane de 16 – 74 ani, care au accesat vreodată Internetul, pe grupe de vârstă și POP105A – Populația rezidentă la 1 ianuarie pe grupe de vârstă și vârste, sexe, medii de rezidență macroregiuni, regiuni de dezvoltare și județe, http://statistici.insse.ro:8077/tempo-online/#/pages/tables/insse-table/, accesat la 29.01.2024

[6] LexisNexis Risk Solutions Cribercrime Report July to December 2020, The New Cybercrime Landscape. Global Risks, Regional Trends, Industry Opportunity, p. 46, disponibil la https://risk.lexisnexis.com/insights-resources/research/cybercrime-report - accesat la 06.07.2023

SCOP ȘI OBIECTIVE

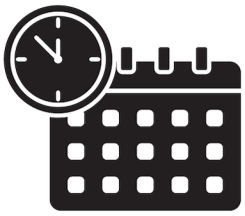
Scopul acestei cercetări a fost ca, prin descrierea obiceiurilor de utilizare a internetului de către populația adultă din România și identificarea vulnerabilităților acesteia, să sprijine demersurile preventive îndreptate spre creșterea nivelului de conștientizare a utilizatorilor de internet cu privire la amenințările cibernetice și la măsurile pe care le pot lua pentru a se proteja.

Obiectivele studiului:

1. Descrierea comportamentelor de utilizare a internetului, cu precădere a celor care reprezintă vulnerabilități în ceea ce privește siguranța online;
2. Identificarea celor mai frecvente infracțiuni cu care se confruntă utilizatorii de internet.

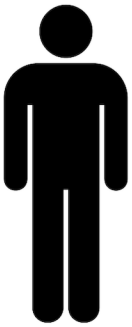
METODOLOGIE

Studiul a fost realizat la nivel național pe un eșantion de **2.136 de respondenți.**



Datele au fost colectate în perioada **05.12.2023-31.12.2023.**

Chestionarul, realizat prin intermediul **Google Forms**, a fost **distribuit la nivel național** cu ajutorul unui cod QR ce a fost afișat în diverse locuri publice.



În vederea asigurării reprezentativității, răspunsurile au fost ponderate în funcție de vârstă, gen și mediu de rezidență, astfel încât să reproducă structura populației conform ultimelor date ale Institutului Național de Statistică.

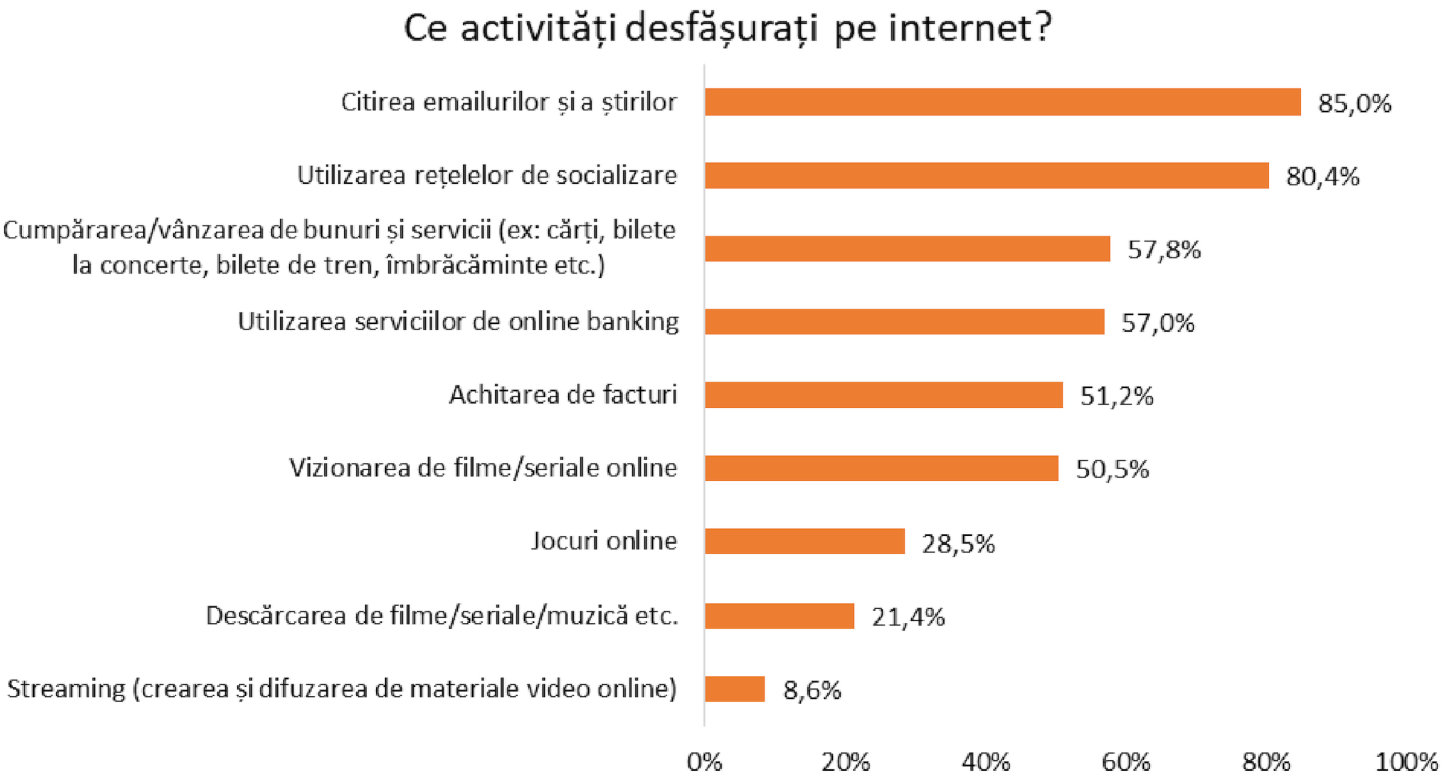
Respondenții au **vârsta** cuprinsă între **18 și 70 de ani și utilizează zilnic sau aproape zilnic internetul.**

ACTIVITĂȚI DESFĂȘURATE ÎN MEDIUL ONLINE

- Dintre cei care utilizează internetul în mod frecvent, **84,3% citesc emailuri și știri, iar 80,6% accesează rețelele de socializare atunci când folosesc internetul**, acestea fiind cele mai frecvente activități desfășurate.

- Aproximativ **50%** dintre respondenți **cumpără sau vând bunuri și servicii online, folosesc servicii de online banking, se uită la filme și seriale sau achită facturi.**

- Doar **o treime dintre utilizatori se joacă online sau descarcă diverse lucruri de pe internet,** în timp ce doar **8,6% creează și difuzează materiale video online.**



ACTIVITĂȚI DESFĂȘURATE ÎN MEDIUL ONLINE

Există **diferențe** în ceea ce privește **activitățile desfășurate pe internet de către bărbați și femei**. Astfel, **bărbații joacă mai des jocuri online** (**75,1%** dintre cei care desfășoară o astfel de activitate), **creează și difuzează materiale online (69,3%)** și **descarcă filme, seriale sau muzică (68,1%).**

Utilizatorii din **mediul urban** reprezintă aproximativ **trei cincimi** dintre cei care utilizează internetul pentru **online banking**, dintre cei care **cumpără/vând bunuri și servicii, achită facturi ori vizionează filme/seriale prin intermediul internetului.**

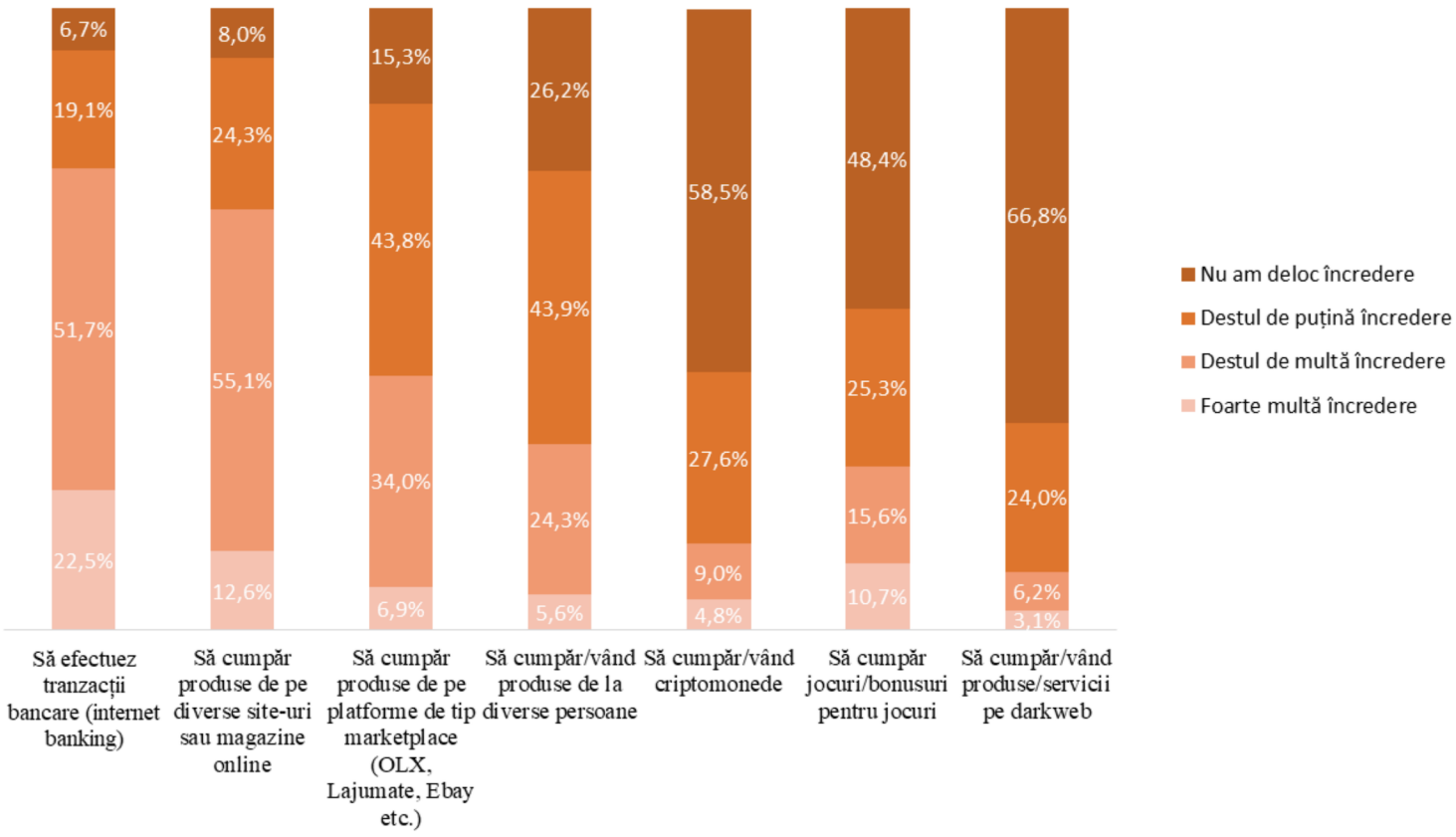
În ceea ce privește activitățile desfășurate pe internet în funcție de vârstă, utilizatorii ce au între 18 și 30 de ani au preocupările cele mai diverse. Dintre utilizatorii care **cumpără/vând servicii online**, **42,1% cei care realizează o astfel de activitate prin intermediul internetului sunt tinerii cu vârsta cuprinsă între 18 și 30 de ani**, dublu față de celelalte categorii de vârstă.

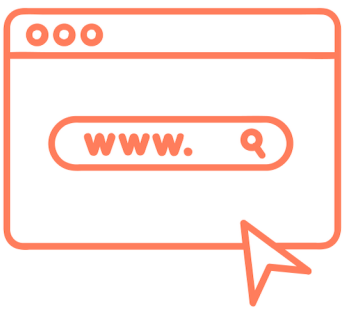
7 din 10 persoane care descarcă filme/seriale/muzică, se joacă online sau fac streaming pe internet au vârste cuprinse între **18 și 30 de ani**.

ACTIVITĂȚI DESFĂȘURATE ÎN MEDIUL ONLINE

Aproximativ **1 din 4 utilizatori nu au suficientă încredere să folosească servicii de internet banking, 1 din 3 nu sunt încrezători în a face cumpărături online, iar mai mult de două treimi dintre respondenți nu ar cumpăra jocuri sau bonusuri pentru jocuri ori nu ar cumpăra/vinde produse de la diverse persoane prin intermediul internetului.** Această lipsă de încredere poate fi cauzată de lipsa cunoștințelor tehnice necesare pentru a realiza astfel de activități pe internet în condiții de siguranță.

Cât de multă încredere aveți să realizați următoarele activități pe internet?



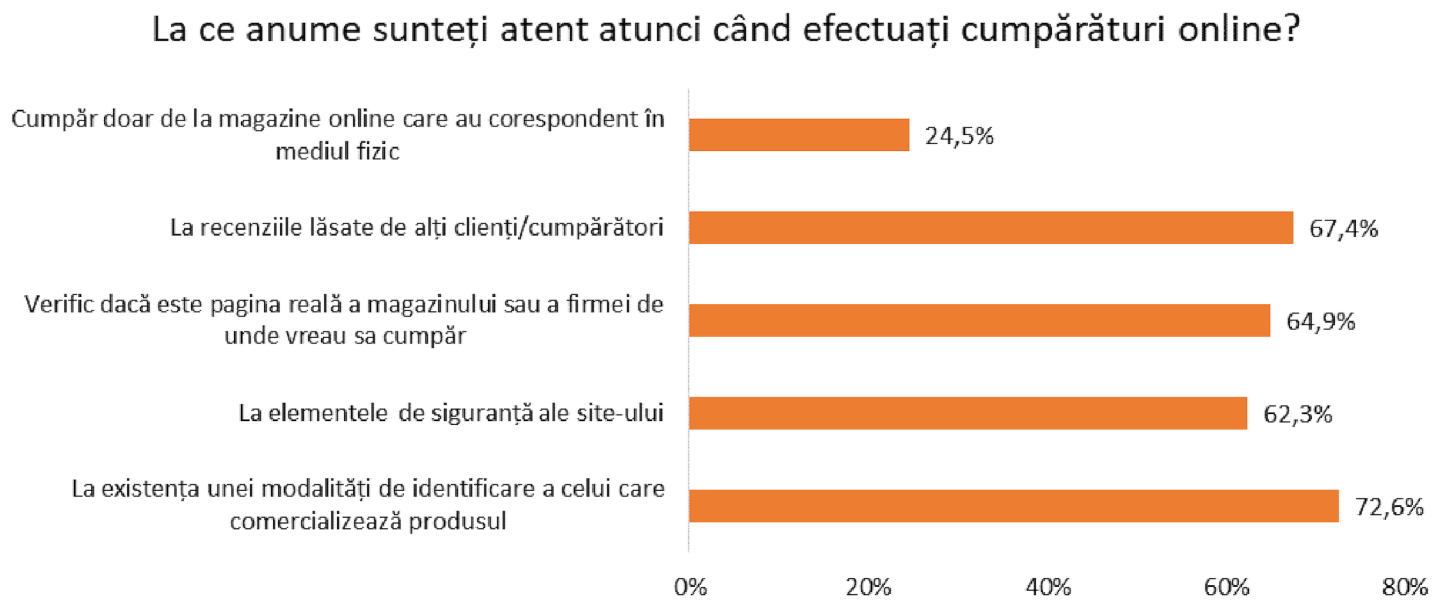


MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET

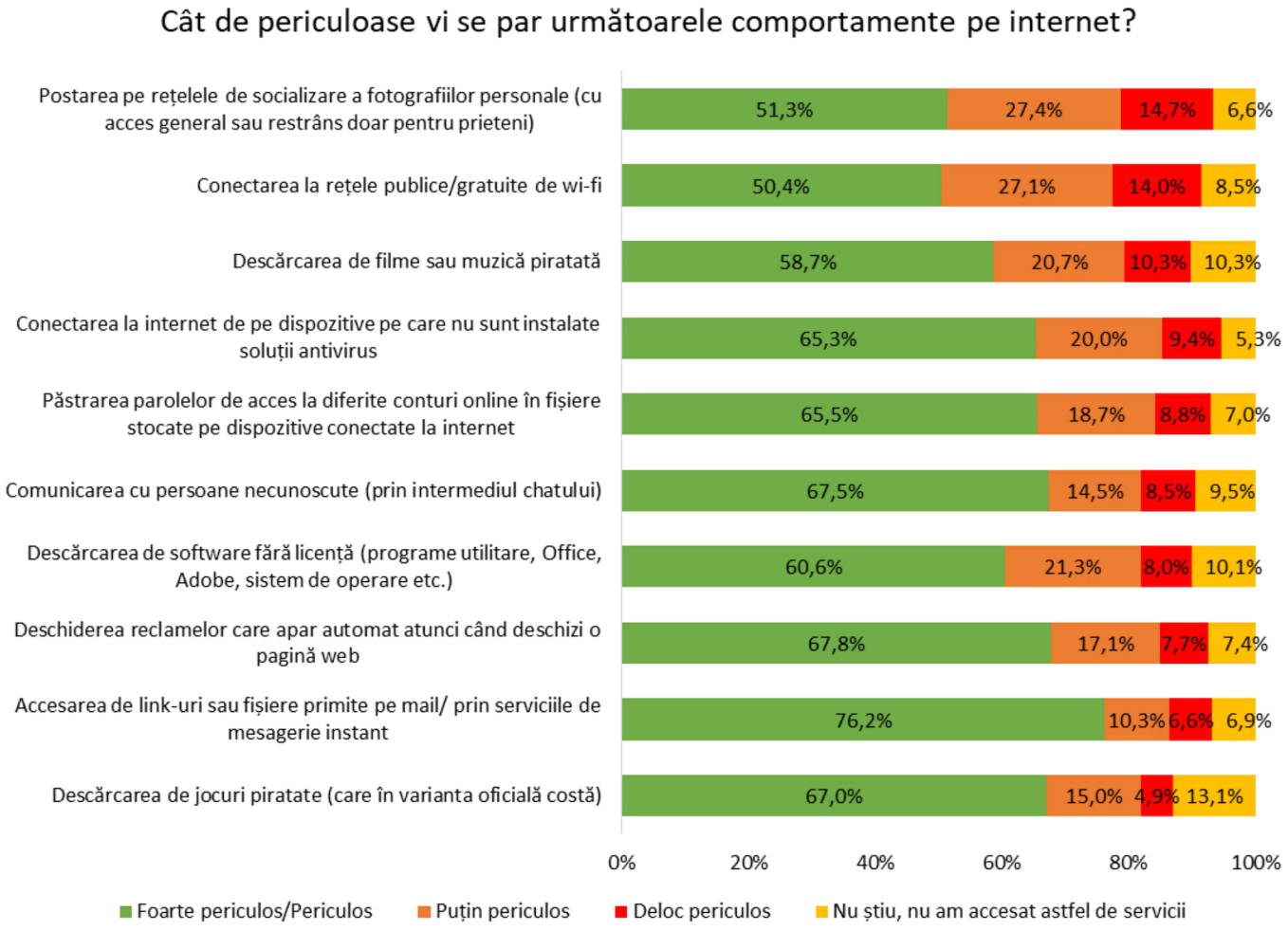
88,8% dintre respondenți consideră că **sunt foarte bine sau relativ bine pregătiți pentru a utiliza internetul în siguranță**, fără a deveni victima unor infracțiuni, însă analiza răspunsurilor arată că nu toți iau măsurile de siguranță necesare.

Atunci când fac cumpărături online, **aproximativ o treime dintre respondenți nu sunt atenți la recenziile lăsate de alți clienți/ cumpărători, nu verifică dacă este pagina reală a magazinului sau a firmei de unde vor să cumpere și nu verifică elementele de siguranță ale site-ului pe care îl accesează**. Totodată, **27,4% nu sunt atenți la existența unei modalități de identificare a celui care comercializează produsul.**

Luând în considerare vârsta, **1 din 2 dintre cei cu vârsta cuprinsă între 18 și 30 de ani** sunt atenți la elementele de siguranță ale site-ului, în timp ce doar **1 din 5 dintre persoanele care au vârsta cuprinsă între 31 și 70 de ani** verifică existența acestor elemente.



MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET

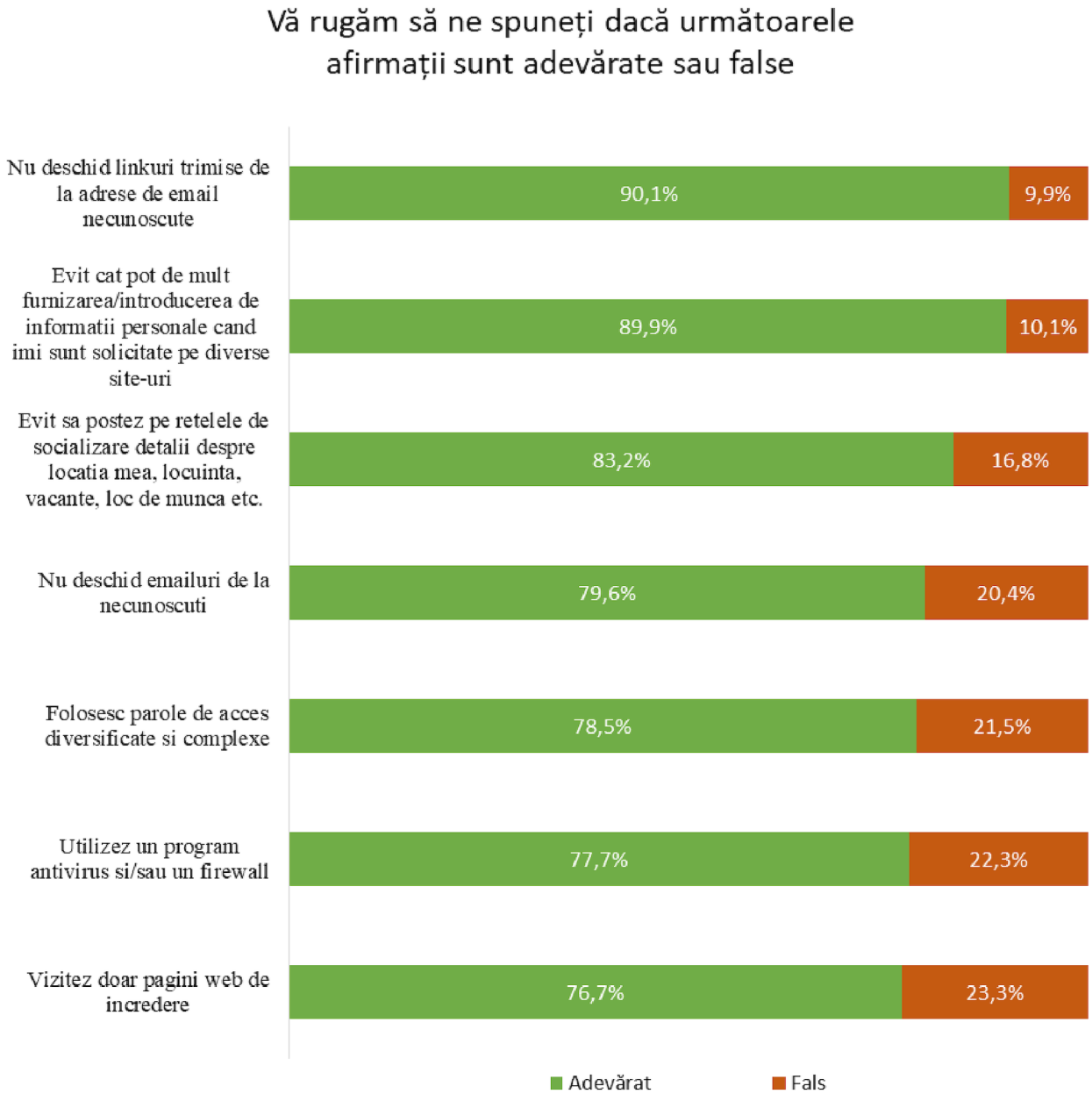


Majoritatea persoanelor care folosesc internetul în fiecare zi înțeleg, la nivel declarativ, riscurile pe care le presupun anumite comportamente în mediul online, însă minimizează pericolele în cazul unora dintre ele:

- aproximativ **14%** dintre utilizatori cred că **nu este deloc periculos să posteze pe rețelele de socializare fotografii personale** (fie cu acces general, fie cu acces restrâns doar pentru prieteni) sau **să se conecteze la rețele publice/gratuite de wi-fi;**
- **1 din 10** persoane consideră că **nu este deloc periculos să descarce filme sau muzică piratată**, ori **să se conecteze la internet de pe dispozitive care nu au un antivirus instalat;**
- **8,8%** dintre internauți **ignoră riscurile** păstrării parolelor de acces la diferite conturi online în fișiere stocate pe dispozitive conectate la internet.

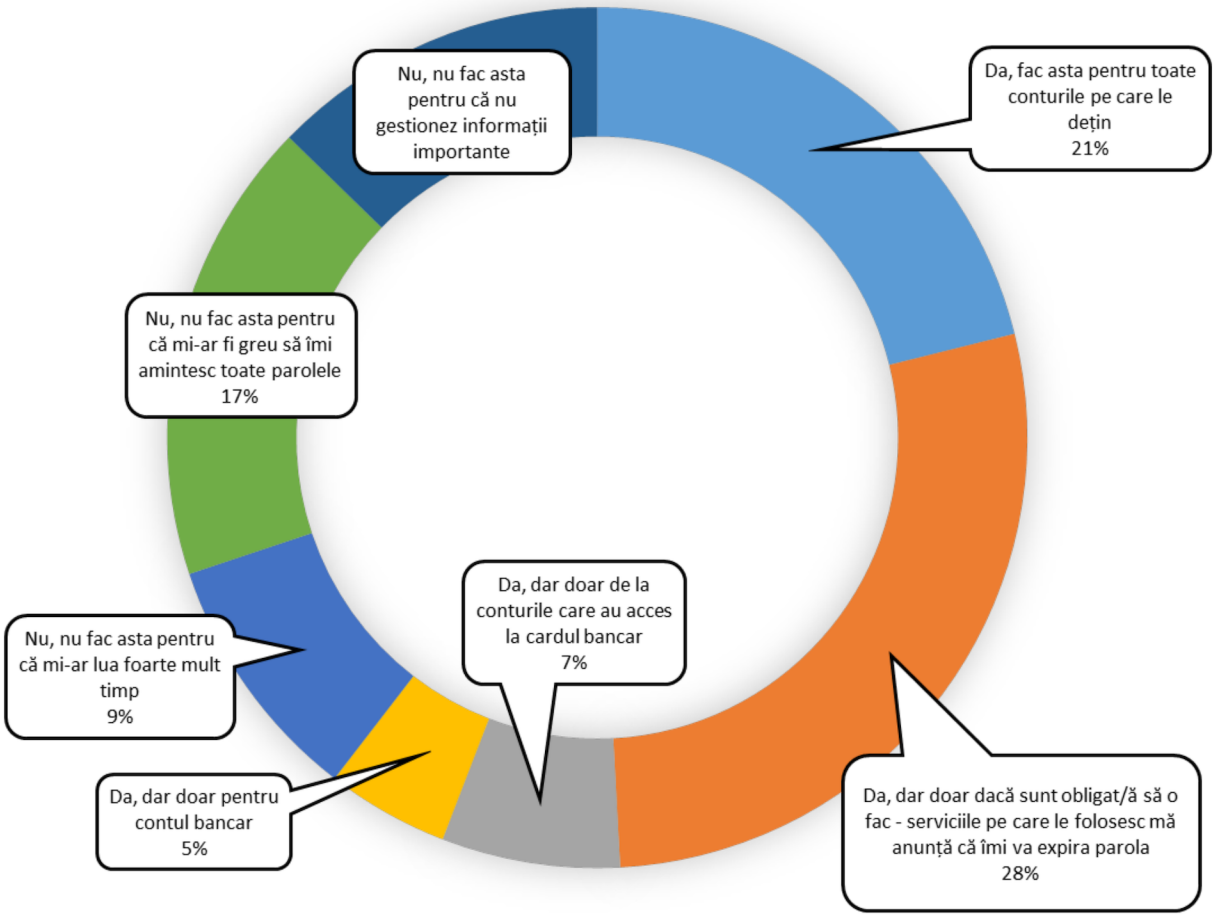
MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET

Aproximativ **20% dintre respondenți nu iau măsuri de siguranță elementare** precum folosirea unui antivirus/firewall sau utilizarea unor parole de acces diversificate și complexe ori accesarea exclusivă a paginilor web de încredere, deși majoritatea utilizatorilor care folosesc internetul în fiecare zi nu deschid link-uri primite de pe adrese de email necunoscute (**90,1%**), evită să furnizeze date personale pe diverse site-uri (**89,9%**) sau prin intermediul rețelelor de socializare (**83,2%**).



MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET

Obișnuiți să vă schimbați parolele periodic de la conturile pe care le folosiți?



39,5% dintre utilizatorii care folosesc internetul în fiecare zi **nu obișnuiesc să își schimbe periodic parolele**, fie pentru că le-ar fi greu să și le amintească (**17,4%**), fie pentru că nu consideră că gestionează informații importante (**12,7%**) ori le-ar lua foarte mult timp (**9,4%**).

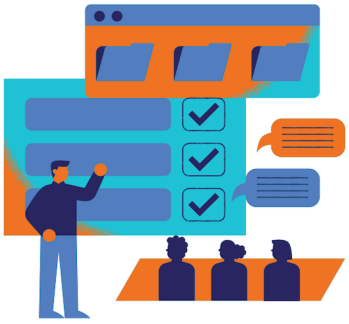
Mai mult, **42,1% dintre respondenți recunosc că folosesc aceeași parolă pentru mai multe conturi** pentru a le fi mai ușor să și le amintească.

În ceea ce privește autentificarea în doi pași (sau mai mulți), **27,4%** dintre utilizatori o folosesc doar pentru conturile pentru care este obligatoriu, în timp ce **18,9%** preferă să folosească servicii care nu îi obligă să implementeze această măsură de siguranță.

MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET

64,2% dintre utilizatorii care folosesc internetul în fiecare zi preferă să introducă manual datele cardului atunci când fac o plată online. **27,4% își salvează datele cardului** în aplicațiile pe care le utilizează frecvent, în timp ce **doar 8,4% folosesc carduri virtuale ce pot fi utilizate o singură dată**.

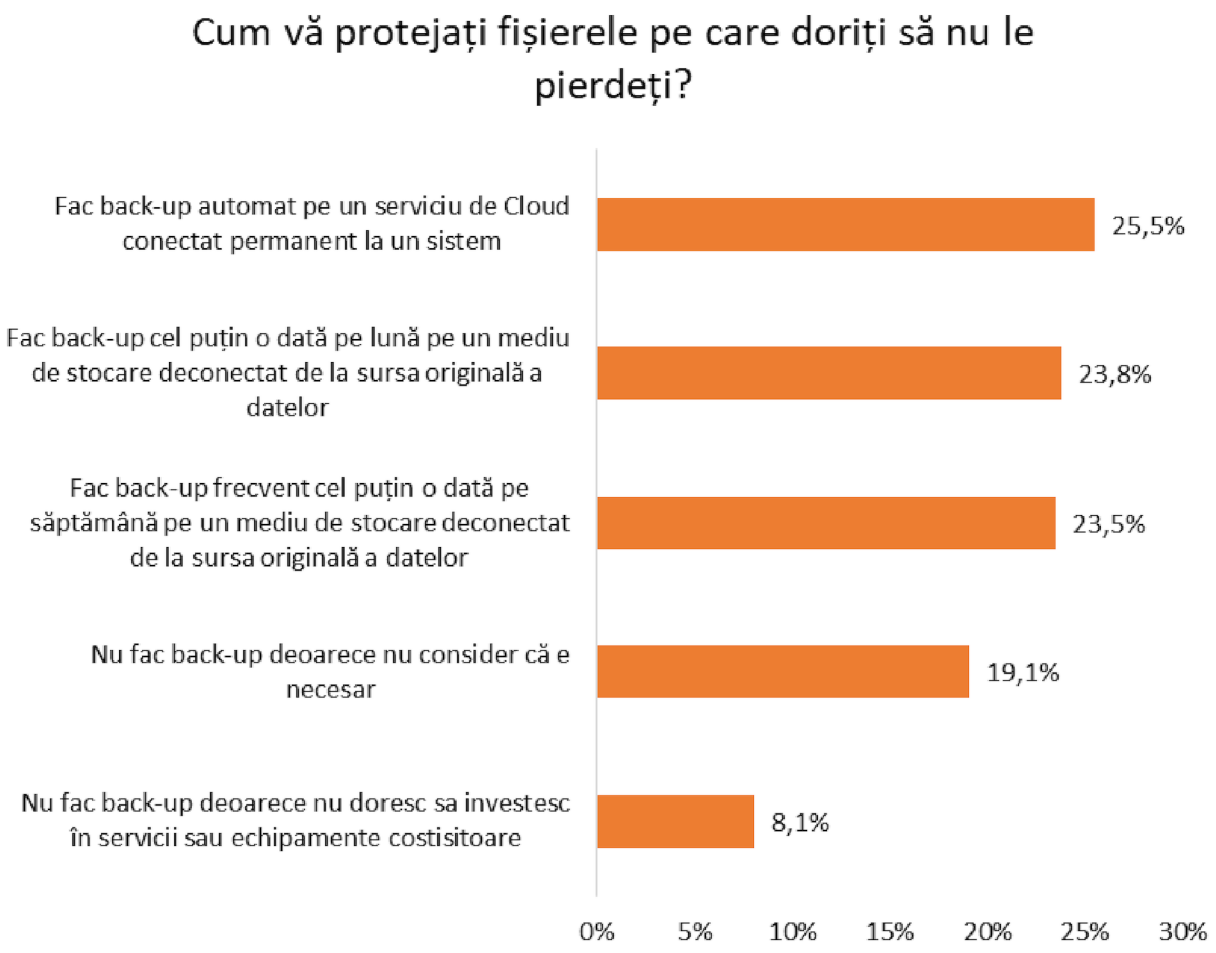
Aproape o cincime dintre respondenți amână cât de mult pot sau dezactivează permanent actualizările sistemului de operare și ale aplicațiilor pe care le folosesc pentru că sunt lente sau îi încurcă.



În ceea ce privește protejarea calculatorului de viruși sau de alte pericole din mediul online, **38,4% dintre utilizatori recunosc că nu instalează un antivirus** pe dispozitivele pe care le folosesc, **48,5% nu au grijă ce site-uri vizitează și ce fișiere descarcă**, iar **54,2% nu mențin sistemul de operare actualizat.**

17,8% dintre respondenții de **gen masculin** consideră că **au suficiente cunoștințe în domeniu** și că **se pot proteja singuri** fără niciun ajutor, spre deosebire de **5%** dintre respondenții de gen feminin.

MĂSURI DE SIGURANȚĂ ÎN TIMPUL NAVIGĂRII PE INTERNET



Deși **47,3%** dintre respondenți **fac back-up datelor cel puțin o dată pe săptămână sau o dată pe lună**, **27,2% dintre aceștia nu folosesc această formă de securizare a datelor**, fie pentru că nu consideră că e necesar (**19,1%**), fie pentru că apreciază că e nevoie să investească în servicii sau echipamente costisitoare (**8,1%**).

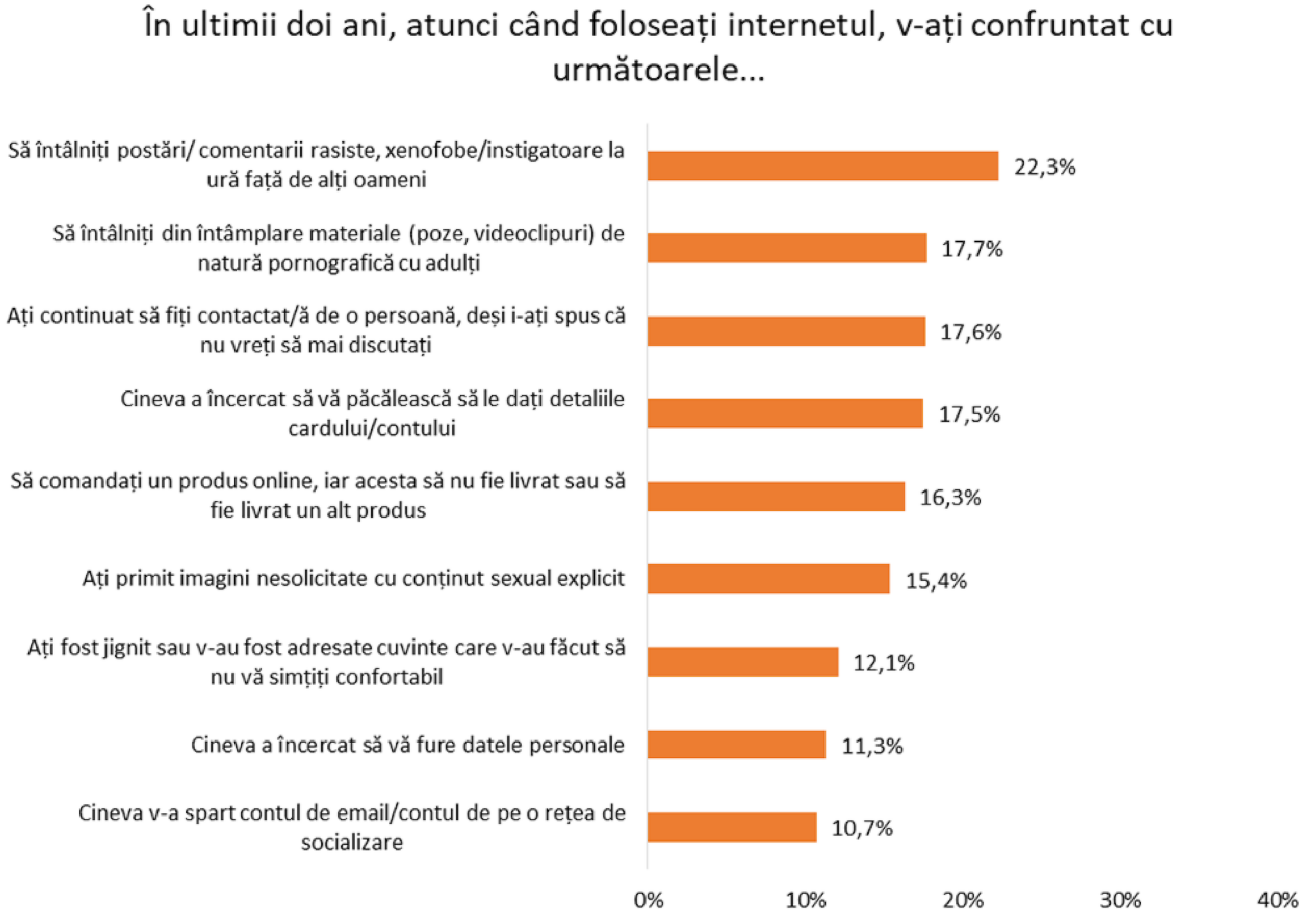
Astfel, utilizatorii devin vulnerabili la atacuri de tip **ransomware,** existând un risc mai mare să plătească „răscumpărarea" pentru a-și debloca datele, dacă realizează ulterior că acestea erau importante pentru ei.

De asemenea, **25,5%** dintre cei care utilizează internetul în fiecare zi **folosesc servicii de Cloud pentru a face back-up**, însă și acestea sunt destul de vulnerabile în fața atacatorilor cibernetici, dacă nu sunt protejate în mod corespunzător.

VICTIMIZAREA PRIN INTERMEDIUL INTERNETULUI

În ceea ce privește victimizarea prin intermediul internetului, **40,6%** dintre respondenți au afirmat că **nu s-au confruntat cu niciuna dintre situațiile de victimizare prezentate**.

Cele mai frecvente situații în care s-au regăsit respondenții sunt prezentate în graficul de mai jos.

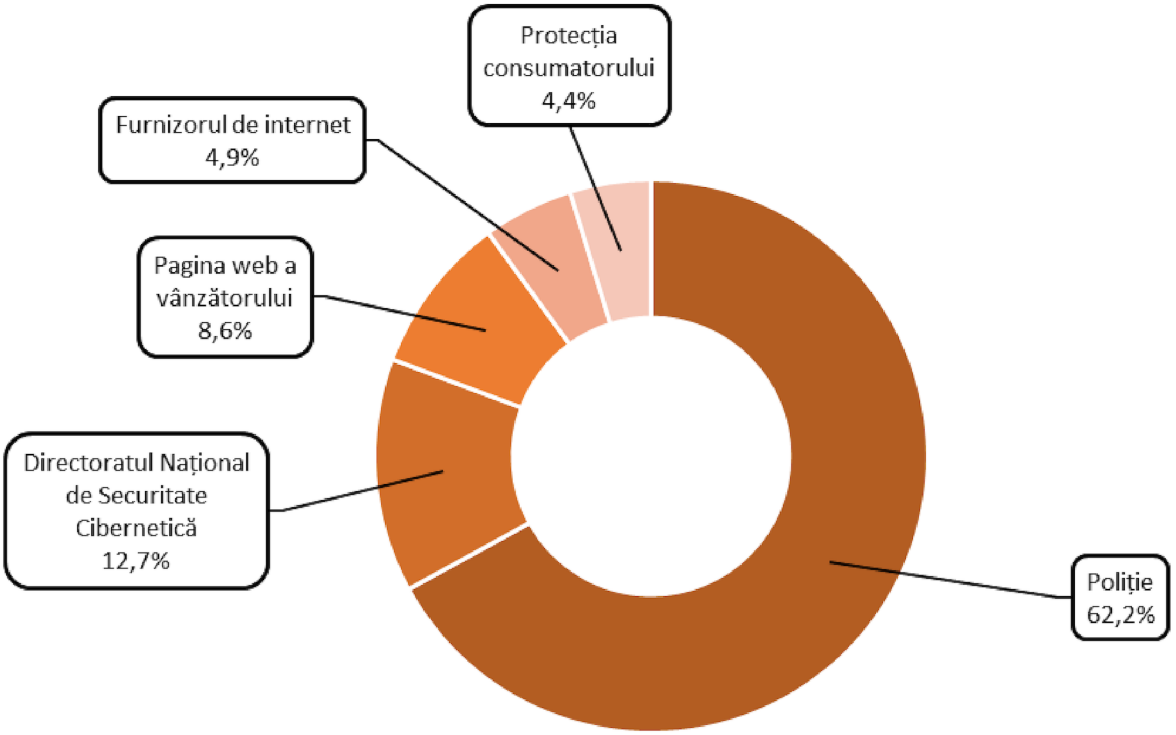


Pe lângă situațiile prezentate mai sus, sub 10% dintre utilizatorii frecvenți de internet s-au confruntat cu următoarele:

- diferite persoane s-au conectat la conturile lor fără ca ei să fie de acord (**8,9%**)
- au fost amenințați de cineva în mediul online (**6,2%**)
- alte persoane au publicat comentarii jignitoare la adresa lor pe rețelele de socializare (**5%**).

VICTIMIZAREA PRIN INTERMEDIUL INTERNETULUI

În cazul în care sunteți victima unui atac cibernetic la cine apelați?



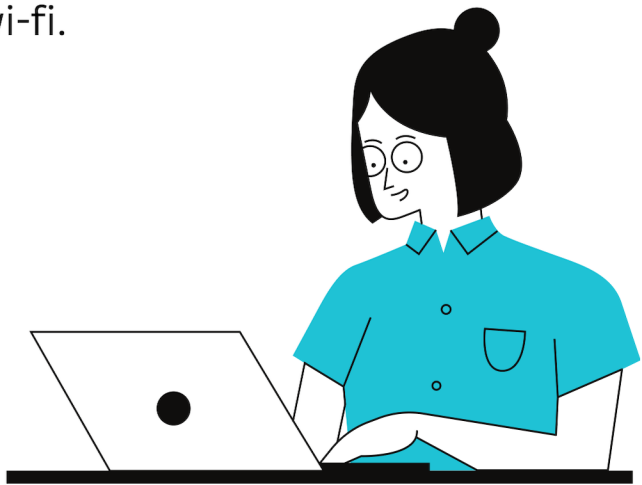
Cei mai mulți dintre respondenți (**62,2%**) susțin că, în cazul în care ar deveni victima unui atac cibernetic, **ar apela la ajutorul poliției**.

De asemenea, de un nivel ridicat de încredere pentru rezolvarea unor astfel de situații se numără și **Directoratul Național de Securitate Cibernetică (12,7%), pagina web a vânzătorului (8,6%), furnizorul de internet (4,9%) și protecția consumatorului (4,4%)**.

Deși în număr mic, există și respondenți care **au recunoscut că nu știu la cine să apeleze (1,4%)** dacă devin victime ale unor astfel de infracțiuni.

CONCLUZII

- Datele studiului derulat în rândul utilizatorilor frecvenți de internet (cei care utilizează rețeaua zilnic sau aproape zilnic) arată o incidență crescută a utilizării acestuia mai ales pentru **informare și socializare (peste 80% dintre respondenți).**
- Un procent mai scăzut **(aproximativ jumătate)** dintre aceștia utilizează internetul pentru realizarea de achiziții, internet banking sau achitarea de facturi.
- La aceste valori contribuie nesiguranța pe care o au utilizatorii să realizeze anumite operațiuni pe internet. Astfel, **un sfert dintre utilizatorii** frecvenți de internet **nu au încredere** să efectueze operațiuni de internet banking, **o treime** să cumpere produse de pe diverse site-uri sau magazine online, **aproximativ 60%** să cumpere produse de pe platformele de tip marketplace sau să vândă/ cumpere produse de la diverse persoane.
- **Majoritatea** utilizatorilor de internet **declară o atitudine foarte precaută** cu privire la achizițiile de jocuri/bonusuri pentru jocuri, tranzacțiile cu criptomonede, sau achizițiile de pe darkweb, doar procente mici simțindu-se încrezători să realizeze astfel de activități.
- Cu toate acestea, rugați să își evalueze competențele digitale, **9 din 10 utilizatori apreciază că sunt bine sau foarte bine pregătiți** să folosească internetul în siguranță.
- Analizarea comportamentului efectiv în mediul virtual relevă însă o serie de **operațiuni online al căror risc este subestimat de utilizatorii frecvenți de internet**.
- **Aproximativ 14% dintre utilizatori cred că nu este deloc periculos** să posteze pe rețelele de socializare fotografii personale (fie cu acces general, fie cu acces restrâns doar pentru prieteni) sau să se conecteze la rețele publice/gratuite de wi-fi.



- **1 din 10 persoane** consideră că **nu este deloc periculos** să descarce filme sau muzică piratată, ori să se conecteze la internet de pe dispozitive care nu au un antivirus instalat.
- Mai mult, **8,8% dintre internauți ignoră riscurile** păstrării parolelor de acces la diferite conturi online în fișiere stocate pe dispozitive conectate la internet.
- Datele arată, totodată, o lipsă de vigilență a unei ponderi semnificative a respondenților în navigarea pe internet.
- Astfel, la efectuarea cumpărăturilor online, **o treime dintre respondenți nu verifică** elementele de siguranță ale site-ului sau dacă este pagina reală a magazinului/ firmei de unde vor să cumpere și nici nu sunt atenți la recenziile lăsate de alți cumpărători, în timp ce **aproximativ un sfert nu acordă atenție** existenței unei modalități de identificare a celui care comercializează produsul.
- Un grad mai mare de vigilență/ prudență se înregistrează în rândul **tinerilor de până în 30 de ani** comparativ cu internauții de peste 30 de ani în ceea ce privește cumpărăturile online și elementele de siguranță la care trebuie să fie atenți.
- Și în alte situații conduita internauților este caracterizată de o lipsă de adoptare a unor măsuri de siguranță, chiar dacă procentul celor care dau dovadă de prudență este mai ridicat.
- Se observă că **aproximativ o cincime dintre aceștia** declară că nu au grijă să acceseze doar pagini web de încredere, nu utilizează programe antivirus și/sau firewall și nu utilizează parole de acces diversificate și complexe.
- De asemenea, **unul din șase internauți nu are nicio reținere să posteze pe rețelele sociale date** privind locația sa, locuință, vacanțe sau locul de muncă, iar **unul din zece respondenți** deschide linkuri trimise de la adrese de email necunoscute și nu evită să furnizeze date personale pe diverse site-uri.
- În condițiile în care riscul de a deveni victima unui atac cibernetic este direct influențat de adoptarea unor măsuri de siguranță este îngrijorător faptul că **4 din 10 internauți nu schimbă periodic parolele conturilor pe care le gestionează și folosesc aceeași parolă pentru mai multe conturi.**

- **Un sfert dintre respondenți** utilizează autentificarea în doi pași **doar pentru conturile unde acest lucru este obligatoriu.**
- Nici protejarea generală a calculatorului/ dispozitivului de pe care utilizează internetul împotriva virușilor nu reprezintă o prioritate pentru un segment important al internauților având în vedere că **aproximativ o cincime dintre respondenți amână cât de mult pot sau dezactivează permanent actualizările sistemului de operare** și ale aplicațiilor pe care le folosesc pentru că sunt lente sau îi încurcă, **mai mult de o treime nu instalează un antivirus** pe dispozitivele pe care le folosesc, iar **aproximativ jumătate nu au grijă ce site-uri vizitează sau ce fișiere descarcă și nu mențin sistemul de operare actualizat.**
- O lipsă de interes manifestă unii internauți inclusiv față de protejarea fișierelor și datelor pe care le dețin în condițiile în care **un sfert dintre aceștia nu fac back-up** deoarece apreciază că nu e necesar sau nu doresc să investească în această formă de securizare a datelor.
- În ceea ce privește **victimizarea** în mediul online, **aproximativ 1 din 5 persoane** a întâlnit postări/comentarii rasiste, xenofobe sau instigatoare la ură, materiale de natură pornografică cu adulți, au fost contactați de anumite persoane, deși nu au mai dorit acest lucru ori anumite persoane au încercat să le păcălească să le dea datele cardului.
- În cazul în care devin victima unui atac cibernetic, **62,2% dintre respondenți** susțin că ar apela la **ajutorul poliției**. Totodată, deși în număr mic, **1,4%** dintre respondenți au recunoscut că **nu știu la cine să apeleze** în cazul în care ar deveni victima unei astfel de infracțiuni.

POLIȚIA ROMÂNĂ

INSTITUTUL DE CERCETARE ȘI PREVENIRE A CRIMINALITĂȚII

www.politiaromana.ro
prevenire@politiaromana.ro