
AWARENESS
PARTEA NEVĂZUTĂ A
SOCIAL MEDIA

CE ÎNȚELEGEM PRIN *SOCIAL MEDIA*?

Social Media reprezintă totalitatea canalelor de comunicare bidirecțională care oferă utilizatorilor numeroase posibilități - de a accesa și consuma conținut online, de a crea și distribui conținut în mediul virtual, de a interacționa de la distanță.

Conținutul generat de utilizatori prin intermediul platformelor care găzduiesc servicii *Social Media* poate avea atât formă multimedia (imagine, audio, video), cât și text.

În prezent, în mediul virtual există o multitudine de platforme sau servicii *Social Media*, caracterizate prin specificul conținutului partajat:

- rețele de socializare (*Facebook, LinkedIN, VK, OK etc.*);
- platforme de *micro-blogging* (*Twitter, tumblr etc.*);
- servicii de partajare a imaginilor (*Instagram, Pinterest*) sau a clipurilor video (*YouTube, LiveLeak, Vimeo, Snapchat, TikTok etc.*);
- platforme wiki (*Wikipedia, Wikia etc.*);
- bloguri (*Blogger, Wordpress etc.*) și forumuri de discuții (*Softpedia etc.*);
- aplicații de mesagerie (*WhatsApp, Facebook Messenger, Telegram, Line etc.*).

Cele mai multe servicii *Social Media* presupun configurarea unor conturi de utilizator pentru accesarea serviciilor și, implicit, furnizarea de date cu caracter personal, precum: nume, data nașterii, adresă de *e-mail*, număr de telefon, adresă de contact, loc de muncă, relații familiale etc.

IMPORTANT! Atunci când introduceți astfel de date pe platformele *Social Media*, fiți conștienți că:

- datele cu caracter personal pot fi disponibile pentru toate entitățile cu acces la platformele și serviciile *Social Media*, fie în mod public, fie dacă acestea plătesc pentru accesul la astfel de informații;

- unele persoane sau entități vă pot utiliza datele publice pentru crearea de conturi false care, ulterior, pot fi folosite în scopuri ilicite, inclusiv pentru colectarea sau extragerea de date și informații personale despre alți membri ai cercului dumneavoastră relațional.

CARACTERISTICI ALE PLATFORMELOR *SOCIAL MEDIA*

Interacțiunea dintre utilizatori - este, poate, principala caracteristică a platformelor *Social Media*. Într-un fel sau altul, toate platformele asigură utilizatorilor posibilitatea de a crea rețele sau cercuri sociale virtuale, în funcție de interese comune, locații geografice, relații stabilite în viața reală etc.

Platformele pot facilita conexiunile anonime dintre utilizatori, mai ales în situațiile în care nu se solicită completarea de date de identificare reale, care să poată fi verificate. Acest aspect poate fi exploatat de diverse entități care urmăresc promovarea unor interese obscure sau pentru propagandă teroristă, prin crearea sau identificarea de grupuri cu interese comune.

> Platforma *Twitter* este recunoscută pentru utilizarea sa involuntară pentru astfel de activități, precum și pentru numărul mare de conturi închise sau blocate din această cauză.

Interacțiunea dintre utilizatori se poate manifesta sub formă de comentarii, aprecieri ale mesajelor publicate sau republicarea mesajelor acestora.

Partajarea de conținut - în funcție de specificul lor, platformele *Social Media* permit partajarea de conținut multimedia sau text, general sau în anumite grupuri de prieteni. Utilizatorii pot identifica diferite canale sau grupuri cu conținut specific, la care pot contribui.

Abonarea la fluxuri de informații - cele mai multe platforme oferă utilizatorilor posibilitatea de abonare la fluxuri de conținut ale altor utilizatori, pentru a fi notificați cu privire la apariția de articole noi, în funcție de interese predefinite.

EXEMPLE DE ATACURI CIBERNETICE ASUPRA CONTURILOR *SOCIAL MEDIA*

SCAM - unul dintre cele mai frecvente tipuri de atacuri asupra conturilor unor utilizatori ai platformelor *Social Media*. Victimele sunt contactate și înștiințate asupra faptului că le sunt cunoscute parolele de la conturile de *e-mail* sau de la alte servicii *online* și că activitatea în mediul virtual le este supravegheată. Scopul final al acestui tip de atac este reprezentat de obținerea de sume de bani, în schimbul păstrării secretului cu privire la datele presupus a fi fost extrase.

GRAYWARE - tip de atac cibernetic ascuns, cel mai adesea, în spatele unor articole virale, *click-bait* sau reclame *online*. Acesta nu are ca efect producerea de daune fizice asupra datelor din calculator sau din conturile de pe platforme *Social Media*. Atacurile *grayware* conduc la diferite *site*-uri web care solicită utilizatorilor completarea unor chestionare pentru a accesa conținutul articolului. Rezultatele chestionarelor sunt colectate și vândute mai departe, pentru a fi folosite pentru încercări de spargeri de conturi personale sau pentru alte tipuri de atacuri la scară mai mare. Soluțiile de protecție instalate pe majoritatea sistemelor electronice nu oferă protecție în fața acestor atacuri, cea mai bună metodă de protecție fiind reprezentată de o conduită *online* adecvată.

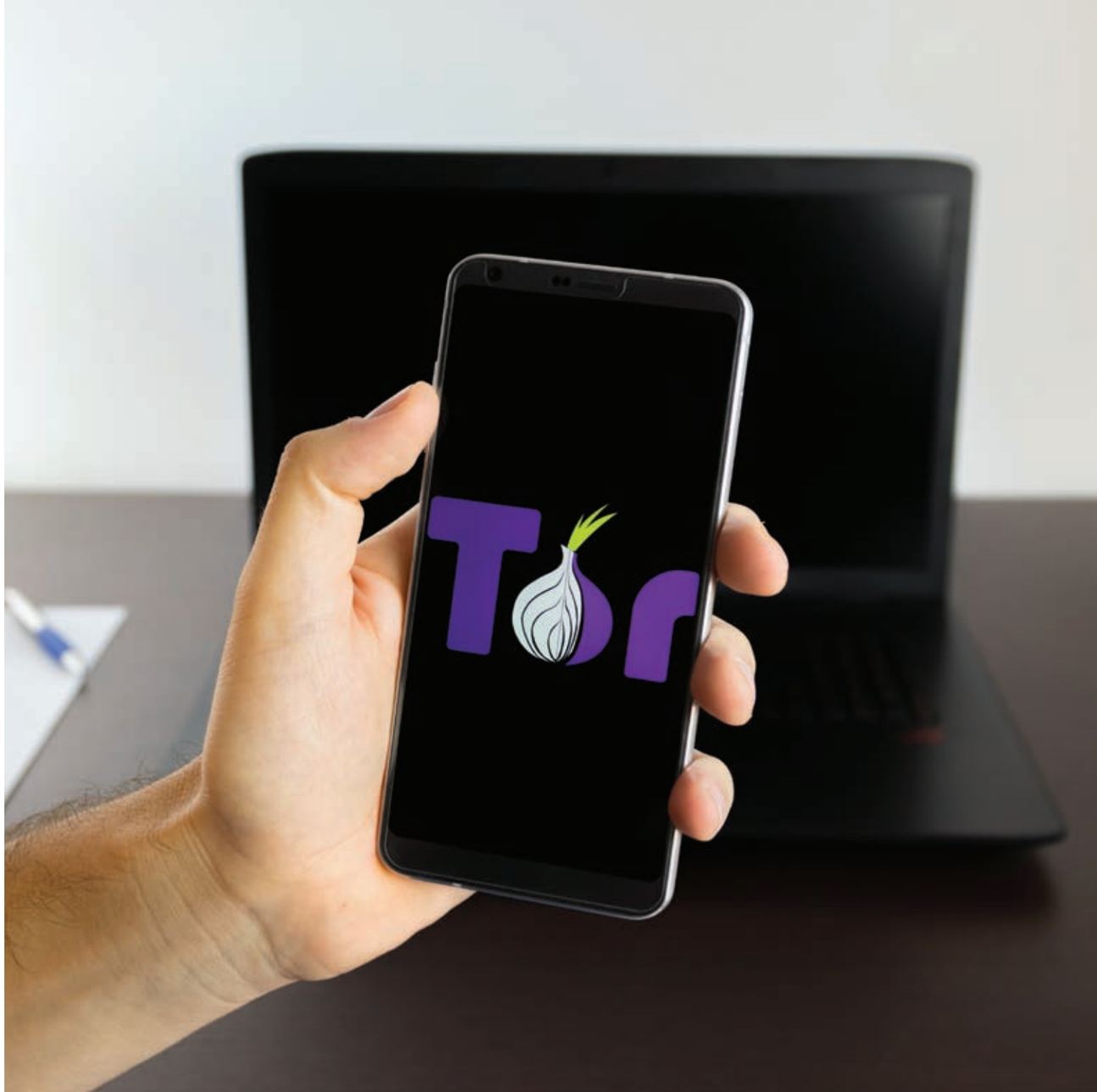
MĂSURI DE SECURITATE PENTRU ACCESAREA PLATFORMELOR *SOCIAL MEDIA*

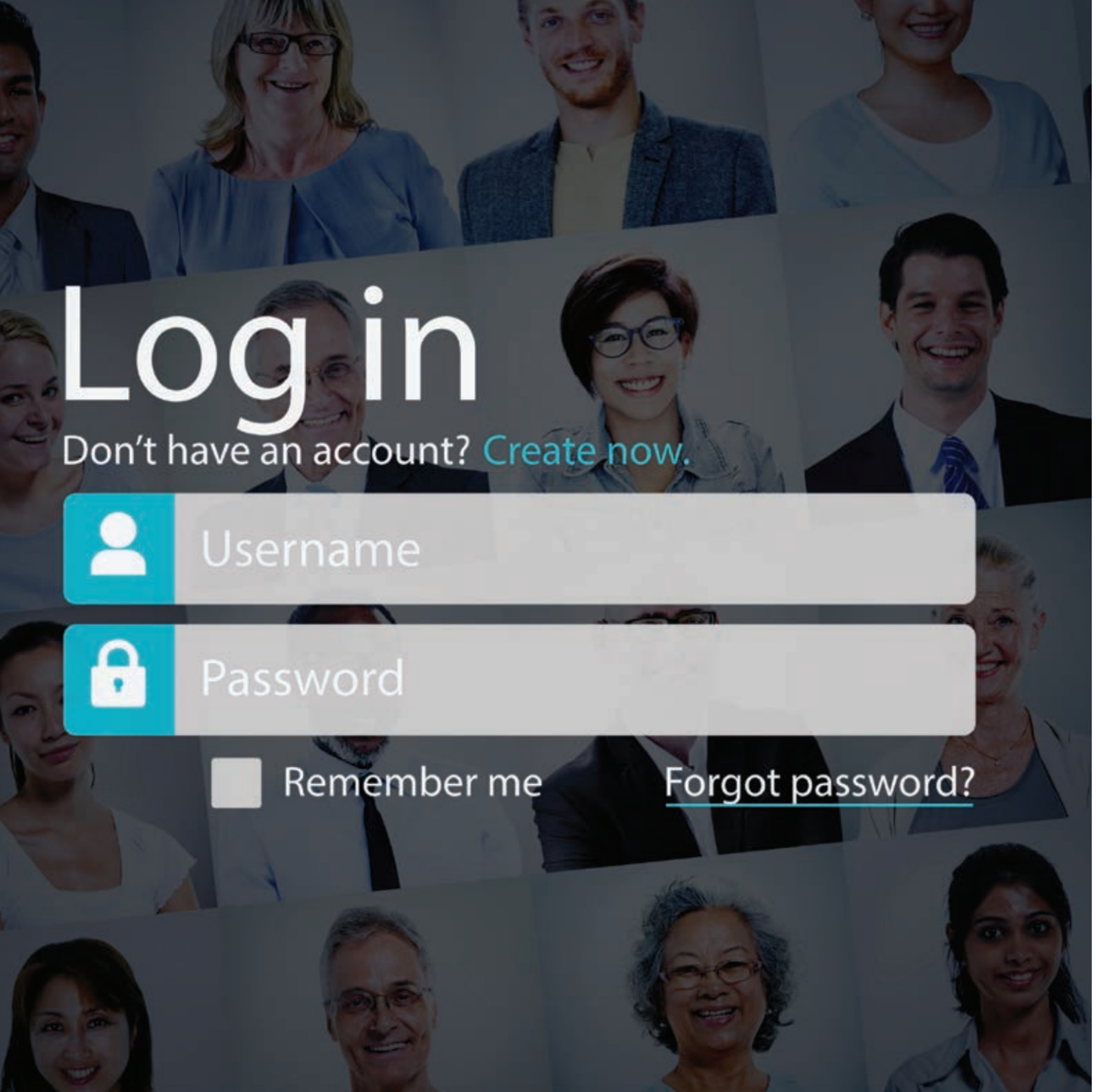
Utilizarea funcționalităților de anonimizare din *browser*

Majoritatea *browser*-elor curente (*Mozilla Firefox, Google Chrome, Microsoft Edge etc.*) beneficiază de **funcționalități primare de anonimizare a activităților *online*** (*Private Browsing, Incognito, InPrivate*).
Activarea acestora **permite navigarea *online* fără salvarea istoricului de căutare sau a numelor de utilizatori și parolelor** și **previne instalarea de fișiere *cookie*** care înregistrează activitățile desfășurate de utilizatori (chiar și atunci când *browser*-ele sunt închise sau dezactivate) sau configurația acestora.
La închiderea unui *browser* care a fost utilizat cu funcționalitățile de anonimizare, toate activitățile online vor fi șterse automat, fără posibilitatea de a mai fi accesate ulterior.

Utilizarea unor aplicații de anonimizare *online* (VPN, Tor)

În situațiile în care se dorește și mai multă anonimitate, se pot **utiliza aplicații *Virtual Private Network* (VPN)**, care permit accesarea Internetului prin servere dedicate în acest sens, situate în alte regiuni geografice, în alte state sau chiar pe alte continente.
Aplicațiile VPN pot fi gratuite sau cu licență plătită. Versiunile plătite oferă funcționalități suplimentare, precum: blocarea automată a accesului la rețeaua Internet în situația în care serverul VPN devine temporar nefuncțional, posibilitatea selectării punctului de acces la Internet sau scanarea automată a traficului.
Dacă se dorește anonimizarea *quasi*-totală a activităților online, se poate opta pentru utilizarea **rețelei *Tor*** și a aplicației ***Tor Browser.***





BUNE PRACTICI ÎN ACCESAREA SERVICIILOR *SOCIAL MEDIA*

Crearea adreselor de *e-mail* asociate conturilor *Social Media*

Pentru configurarea unui cont de utilizator pe majoritatea platformelor *Social Media,* este necesară utilizarea unor adrese de *e-mail* precum *Gmail, Yahoo!* etc.
Dacă se configurează astfel de adrese *e-mail* pe serviciile *Gmail* și *Yahoo!*, este necesară introducerea suplimentară a unui număr de telefon sau a unei alte adrese de *e-mail*, utilizate pentru validare sau recuperarea parolei.
În cazul fiecărui cont de *e-mail* nou creat este necesară completarea, în funcție de situații punctuale, a următoarelor categorii de date: **nume, prenume, nume de utilizator, parolă, zi de naștere, sex, număr de telefon, locație**.
Pentru **configurarea parolelor este necesară utilizarea unor șiruri complexe de minim 8 caractere**, care ar trebui să conțină, obligatoriu, litere mari, litere mici, cifre, caractere speciale (de exemplu: K#h0lY!p).

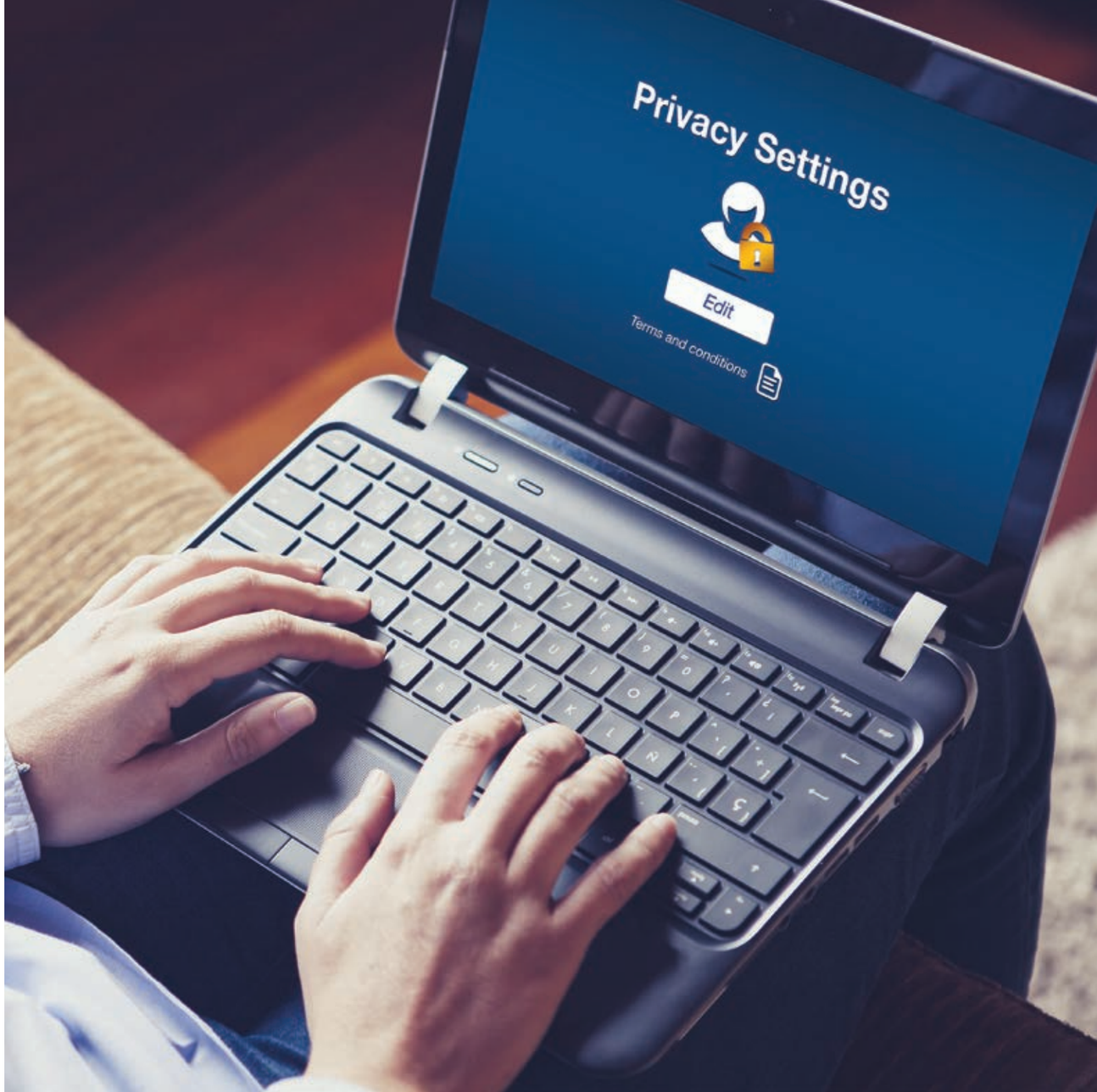
Crearea și configurarea conturilor pe platforme *Social Media*

Pentru configurarea conturilor pe platformele *Social Media* este necesară o adresă de *e-mail* sau un număr de telefon, pentru verificarea faptului că este vorba despre un utilizator uman care solicită accesarea serviciilor și nu despre un instrument automat (robot). În acest sens, platformele vor trimite fie un *link* de validare a contului (în cazul în care se utilizează o adresă de *e-mail*), fie un cod prin SMS (în cazul în care a fost utilizat un număr de telefon).
Majoritatea platformelor *Social Media* oferă mecanisme de anonimizare/ascundere a datelor cu caracter personal, pentru toți utilizatorii sau pentru categorii special definite de către administratorii conturilor, în funcție de necesități sau de situații punctuale.

DE REȚINUT! Fiecare dintre noi utilizăm cel puțin o platformă *Social Media*. Aceste rețele au devenit o parte importantă a vieții cotidiene și oferă o multitudine de facilități, încurajează comunicarea rapidă și interacțiunile fără a ține cont de granițe.

Pentru a utiliza în siguranță *Social Media* sunt indicate:

- gestionarea setărilor de confidențialitate pentru protejarea datelor;
- setarea de parole de acces complexe, prin alegerea unor combinații de litere (majuscule și minuscule), simboluri și cifre (cu cât are mai multe caractere, cu atât este mai sigură);
- utilizarea de parole diferite pentru conturi *Social Media* și schimbarea acestora la intervale regulate de timp;
- evitarea furnizării de date cu caracter personal dacă nu este necesar;
- acceptarea selectivă a cererilor de prietenie. Dacă nu cunoști persoana care îți solicită prietenia, este indicat să nu accepți cererea - poate fi un cont fals!;
- evitarea accesării *link*-urilor suspecte distribuite pe platforme *Social Media*;
- prudență în distribuirea *online* a conținutului.



AWARENESS

Un material elaborat în cadrul
PROGRAMULUI DE *AWARENESS*
AL SERVICIULUI ROMÂN DE INFORMAȚII