



# SECURITATEA OPERAȚIONALĂ ȘI REZILIENȚA PERSONALĂ: O PREZENTARE GENERALĂ A ȚĂRILOR DIN VECINĂTATEA ESTICĂ



# SECURITATEA OPERAȚIONALĂ ȘI REZILIENȚA PERSONALĂ: O PREZENTARE GENERALĂ A ȚĂRILOR DIN VECINĂTATEA ESTICĂ

Manual cu privire la Amenințările de Securitate Cibernetică, Informațională, Contrainformațională și Personală din partea Regimurilor Autoritare Străine, Oprimare Internă și Hărțuire

## Autori

**Georgia:** Fundația de Dezvoltare a Mass-media – Mariam Pataridze, Sopho Gelava, Tinatin Gogoladze

**Moldova:** IPIS – Institutul pentru Inițiative Strategice – Victoria Olari

**Ucraina:** Centrul Media de Criză din Ucraina – Liubov Tsybulska, Oleksandra Tsekhanovska

**Recomandări de securitate operațională:** Echipa Centrului „European Values” în domeniul politicilor de securitate

## Editor

**Andrea Michalcová,** Centrul „European Values” în domeniul politicilor de securitate



Acest raport a fost creat cu sprijinul financiar al Comisiei Europene. Comisia Europeană nu își asumă nici o responsabilitate pentru faptele sau opiniile exprimate în această publicație sau pentru orice utilizare ulterioară a informațiilor conținute în aceasta. Întreaga responsabilitate revine autorului publicației.

**Drepturile de autor asupra imaginilor:** Pagina 7: Juan Antonio Segal/Flickr, Pagina 11: Veaceslav Bunescu/Flickr

## 1. INTRODUCERE

Acest raport este urmare a unui an de cooperare între organizațiile societății civile (OSC) și grupurile de reflecție din Europa Centrală și Vecinătatea Estică (VE). Este o parte a Proiectului privind îmbunătățirea și împărtășirea lecțiilor învățate în domeniul rezilienței și autoprotecției, care evaluează capacitatea societății civile din Georgia, Ucraina și Moldova de a utiliza îndrumările Centrului „European Values” în domeniul politicilor de securitate (EVC) în securitatea operațională și expunerea metodelor nelegitime de influență. Aici, le adaptăm abordarea și o aplicăm la realitățile politice din VE.

Autorii au efectuat o cercetare de birou amănunțită ale informațiilor din surse deschise, sondaje publice și rapoarte de investigații relevante. Cercetarea de birou a fost realizată prin interviuri structurate cu experți și oficiali locali relevanți. Reprezentanții mass-media, precum și experții în politică externă și securitate din organizațiile societății civile au furnizat cea mai mare parte a informațiilor. Datorită sensibilității subiectului, am decis să nu publicăm lista numelor persoanelor intervievate, care poate fi obținută de la echipa editorială a Centrului „European Values” în domeniul politicilor de securitate.

Cercetătorii noștri s-au concentrat pe situațiile în domeniul mediatic din Georgia, Ucraina și Moldova:

În Georgia, unele studii de caz privind influența malignă străină sunt disponibile, însă există un număr mic de evaluări detaliate și comparabile privind întreaga scală a influenței maligne străine și, în consecință, puține recomandări de politici specifice pentru campaniile de advocacy conduse de societatea civilă. Mai multe state care operează în afara cadrului UE-NATO proiectează influență malignă în Georgia, prin activități diplomatice, folosind politica energetică și economică, desfășoară război informațional și sprijină grupuri interne de orientare radicală sau mainstream cu potențial subversiv. Țările post-sovietice, cum ar fi Georgia, sunt deosebit de vulnerabile la răutatea precipitată de aceste grupuri, care nu numai că sunt bine documentate din rapoartele SUA și UE, dar sunt și sensibile atenției publicului; așa-numitul „proces de grănițare” a adus un val de căderi de curent la georgieni. Acțiunile ostile în Georgia prin intermediul anumitor OSC, mass-media și agenți de influență și forțe politice au drept scop discreditarea procesului de integrare euro-atlantică al țării și alimentarea scepticismului privind dezvoltarea democratică. Alegerile prezidențiale recente desfășurate pe 28 octombrie 2018 au arătat cât de strâns unele campanii au fost legate de corupție și dezinformare, toate stând în calea activităților organizațiilor societății civile<sup>1</sup>.

Ucraina este, de asemenea, plină de provocări pentru agenți care solicită responsabilitate de la guvern. Chiar și după ce OSC-urile au câștigat dreptul de a activa deschis și liber în domeniul problemelor de politică publică în urma Revoluției Dignității, mai recent acestea (în special la sfârșitul anului 2018, cu un an înainte de alegerile prezidențiale și parlamentare) au întâmpinat mai multe presiuni din partea statului. Pentru a discredita activiștii civici, guvernul a inițiat o nouă lege care impunea pe acei care lucrează în domeniul combaterii corupției să-și declare veniturile și bunurile în mod public<sup>2</sup>. După critici puternice din străinătate, plus

1 Crosby, Alan. “Sex, Lies, And Audiotape: Just Another Election Campaign In Georgia.” *RadioFreeEurope/RadioLiberty*. Accesat pe 24 octombrie 2018. <https://www.rferl.org/a/sex-lies-and-audiotape-presidential-election-campaign/29561804.html>

2 “Ukrainian Civil Society Unites to Counter Mounting Threats”. *Freedom House*. Accesat pe 18 aprilie 2018. <https://freedomhouse.org/article/ukrainian-civil-society-unites-counter-mounting-threats>



o rezistență masivă a activiștilor înșiși, această propunere a fost abandonată. Mai multe OSC și activiști civici s-au confruntat cu atacuri fizice și verbale directe. Regiunile estice ale Ucrainei sunt zone deosebit de dificile, în care autoritățile locale pro-ruse și poliția corupte sunt insensibile la atacurile fizice asupra jurnaliștilor. Cel mai șocant exemplu este istoria activistei anticorupție Katerina Gandziuk din Herson, care a fost atacată cu acid sulfuric. Gandziuk a criticat poliția și autoritățile de securitate și a condamnat corupția în departamentul regional al Ministerului Afacerilor Interne. Ea a făcut publică implicarea poliției în mai multe cazuri de corupție. A murit din cauza rănilor suferite 3 luni mai târziu.

Actorii societății civile au pierdut teren și în Moldova<sup>3</sup>, în special după 2016, când guvernul a ajuns în alte mâini și a trecut sub controlul deplin al Partidului Democrat din Moldova. În 2017, Ministerul Justiției a încercat să introducă în legislație interdicția activităților politice și de advocacy legislativă<sup>4</sup> de către OSC care primesc fonduri străine. Dispozițiile controversate au fost incluse într-un proiect de lege la sfârșitul lunii martie 2018, dar ulterior au fost abandonate. După ce s-au opus modificării controversate a sistemului electoral, OSC-urile din Moldova sunt supuse în mod constant unor atacuri din partea oficialilor publici și a altor entități afiliate partidului de guvernământ<sup>5</sup>, inclusiv din partea mass-media, bloggerilor și trolilor online. Mai multe OSC din Moldova au raportat agresiuni între anii 2016 și 2018. Acestea includ acuzații calomnioase de implicare cu persoane acuzate de fraudă bancară în valoare de 1 miliard de euro în 2014 sau în scandalul „Laundromat”. Un caz important recent implică o anchetă parlamentară cu privire la o călătorie în Parlamentul European<sup>6</sup> întreprinsă de mai mulți activiști, jurnaliști și două figuri cunoscute ale opoziției, care a fost sponsorizată de o OSC poloneză, Open Dialog Foundation. Oficialii parlamentari au invocat că Fundația era un servitor pro-rus, având scopul de a destabiliza situația politică din Moldova și unii dintre ei și-au expus părerea că participanții la călătorie să fie cercetați sub acuzația de trădare. Adesea, astfel de operațiuni de asasinare a personajelor sunt însoțite de publicarea schimburilor de e-mailuri private ale activiștilor menționați sau a conversațiilor acestora din diferite aplicații de mesagerie, ceea ce arată că criticii vocali ai guvernului sunt vulnerabili la atacuri cibernetice.

Situația generală a OSC din aceste trei țări țintă a fost critică. Se face foarte puțin pentru susținerea lor. Prin urmare, EVC a decis să sensibilizeze aceste medii și să împărtășească cele mai bune practici din domeniul securității operaționale și personale, în baza consultărilor cu mai mulți experți în securitate.

Plasând amenințările pe categorii, noi am identificat principalele obstacole în funcționarea continuă a acestora și am formulat următoarele recomandări.

- 
- 3 Macrinici, Sorina. "Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accesat în aprilie 2018. <https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf>
  - 4 RFE/RL's Moldovan Service. "Moldovan NGOs Reject Proposed Ban On Foreign Funding" *RadioFreeEurope/RadioLiberty*. Accesat pe 12 iulie 2017. <https://www.rferl.org/a/moldova-ngos-reject-foreign-funding-ban/28612337.html>
  - 5 Macrinici, Sorina. "Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accesat în aprilie, 2018. <https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf>
  - 6 Dulgher, Maria. "An outline of the 'Open Dialog' scandal. PAS and DTPP in the gunsight of the Moldovan Parliament." *Moldova.org*. Accesat pe 13 noiembrie, 2018. <https://www.moldova.org/en/outline-open-dialog-scandal-pas-dtpp-gunsight-moldovan-parliament/>

## 2. METODOLOGIE: CATEGORIZAREA AMENINȚĂRILOR ȘI RĂSPUNSURILE SUGERATE LA ACESTEA

CATEGORIE	AMENINȚARE	CE TREBUIE DE FĂCUT	DESCRIERE	EXEMPLU DE AMENINȚARE VERBALĂ SAU SCRISĂ
1	E-mail general de ură fără adresare directă sau cu indiciu de amenințare	Scrieți un e-mail către o persoană de contact din cadrul organizației dvs. <sup>7</sup> în aceeași zi <sup>8</sup> .	Mesaj fără adresare directă, care evaluează în mod grosolan și negativ instituția, fără specificarea mai departe a amenințării sau amenințare implicită	„Te culci, fiind plătit de Dumnezeu știe cine. Învață cum să lucrezi cu mâinile. Evreii și poponarii ca tine vor termina prost. Ne vom ocupa noi de tine.”
2	Mesaj adresat cu indiciu de amenințare	Scrieți un e-mail către o persoană de contact din cadrul organizației dvs. în aceeași zi, raportați personal superiorului dvs./șefului pazei din organizația dvs.	Mesaj adresat cu indiciu de amenințare trimis direct persoanei sau specificând acea persoană, fără specificarea mai departe a amenințării/amenințarea este doar implicită; apeluri telefonice anonime, fără amenințări explicite.	„Cum îndrăznești să insulti președintele în așa fel, primitivule. Las’ că-ți vin de hac. Abia aștept să văd cum vă ard birourile plătite de SUA. Știu unde le aveți, idioților.”
3	Mesaj adresat de amenințare sau amenințare iminentă	Sunați imediat superiorul dvs./șeful pazei din organizația dvs.	Mesaj adresat în mod special cuiva care conține o amenințare specifică împotriva persoanei respective sau persoanelor dragi. Conține informații care nu sunt publice (adresă, nume) și o amenințare iminentă.	„O avertizare nu a fost destulă pentru tine, da? Cred că trebuie să folosesc alte „argumente”, porcule. Așteaptă puțin. Știu unde trăiești – Novákova 3.”
4	Incident fizic	Dacă este necesar, sunați la 112. Sunați imediat superiorul dvs./șeful pazei din organizația dvs.	O persoană anume are impresia legitimă că este urmărită, intimidată sau există o tentativă de atac sau confruntare fizică directă.	Ai sentimentul că ești urmărit pe stradă. Orice încercări, chiar implicite, de intimidare (un străin spune, „la oprește-te, sau ...”, și pleacă).

<sup>7</sup> Este bine să aveți o setare specifică în poșta electronică pentru așa cazuri, care este apoi în mod automat transmisă șefului serviciului de securitate.

<sup>8</sup> Catalogăm pentru viitor, în cazul în care escaladează comportamentul persoanei.

### 3. CADRUL DE SURSE ALE CELOR MAI COMUNE AMENINȚĂRI DE SECURITATE ÎN ȚĂRILE VIZATE

	MOLDOVA	GEORGIA	UCRAINA
<b>SECURITATEA CIBERNETICĂ</b>	<ul style="list-style-type: none"> <li>Blocarea directă a serviciului (DDoS) (site-uri web indisponibile)</li> <li>Phishing (recepționarea de e-mail-uri false și link-uri de site-uri)</li> </ul>	<ul style="list-style-type: none"> <li>DDoS (site-uri web indisponibile)</li> <li>Phishing (recepționarea de e-mail-uri false și link-uri de site-uri)</li> <li>Ransomware (date criptate)</li> <li>Pierderea datelor (documentelor, corespondenței)</li> </ul>	<ul style="list-style-type: none"> <li>DDoS-atac (Paralizare scurtă sau pe termen mediu a operațiunilor)</li> <li>Phishing</li> <li>Pierderea datelor (documentelor)</li> </ul>
<b>SECURITATEA INFORMAȚIONALĂ</b>	<ul style="list-style-type: none"> <li>Scurgere de parole (Yahoo, Facebook)</li> <li>Spargerea contului de e-mail (dezvăluirea comunicării, furt de date)</li> <li>Discreditare online (bărfe, minciuni, insulte, etc.)</li> <li>Furtul de identitate online (uzurparea identității)</li> </ul>	<ul style="list-style-type: none"> <li>Scurgere de date personale (adresă, numărul de telefon, etc.)</li> <li>Scurgere de parole (Yahoo, Facebook)</li> <li>Spargerea contului de e-mail (dezvăluirea comunicării, furt de date)</li> <li>Discreditare online (bărfe, minciuni, insulte, etc.)</li> <li>Furtul de identitate online</li> <li>Penetrarea memoriei unui dispozitiv de tip „smart” și furtul elementelor personale pentru a șantaja cu aceste materiale (în special poze ale minorilor sau poze și videoclipuri cu minori)</li> </ul>	<ul style="list-style-type: none"> <li>Spargerea contului de e-mail (scurgere de corespondență, furt de date)</li> <li>Discreditare online (terorizare pe internet)</li> <li>Crearea de conturi false de social media și de experți</li> <li>Atacuri prin campanii și operațiuni de dezinformare</li> <li>Hărțuire și discreditare din partea entităților străine (suferă frecvent de ținte ale operațiunilor maligne rusești)</li> <li>Hărțuire din partea autorităților locale (folosirea organizației pentru câștig politic; hărțuire din partea partidului politic de guvernare)</li> </ul>
<b>SECURITATEA CONTRAINFORMAȚIONALĂ DE BAZĂ</b>	<ul style="list-style-type: none"> <li>Activități suspecte într-un circuit închis (șpionaj, urmărire, curiozitate etc.)</li> <li>Recrutare de către serviciul de informații ostil (oferte directe, promovare etc.)</li> <li>Invitație la interviu (fals)</li> <li>Interceptarea convorbirilor/supraveghere prin echipamente speciale în interiorul unei companii de televiziune</li> </ul>		
<b>SECURITATEA PERSONALĂ (FIZICĂ)</b>	<ul style="list-style-type: none"> <li>Intimidare (amenințări, persecutare)</li> <li>Șantajare</li> <li>Vandalism</li> </ul>	<ul style="list-style-type: none"> <li>Intimidare (amenințări, abuz)</li> <li>Șantajare</li> <li>Leziuni ușoare (vânătași, tăieturi, jolituri)</li> </ul>	<ul style="list-style-type: none"> <li>Intimidare în timpul călătoriilor internaționale (detenție în Rusia, Belarus, Moldova, Armenia)</li> <li>Vandalism (jaf în birou)</li> </ul>



UKRAINA

## 4. UCRAINA

### Context

Am solicitat 10 OSC din Ucraina să realizeze un sondaj pe o perioadă de patru luni cu privire la provocările curente legate de securitatea cibernetică și posibile amenințări, precum și capacitatea instituțională de a le face față și de a le depăși. Pe fundalul sectorului terțiar înfloritor, numărul relativ mic de respondenți și reticența generală a multor reprezentanți ai OSC și/sau activiști de a participa la sondaj este în sine indicativ. Bănuim că un număr esențial dintre aceștia au refuzat să participe la sondaj tocmai din unul dintre motivele pe care sondajul urmărește să exploreze – se simt preocupați de siguranța datelor lor personale, precum și de gradul de integritate cu care acestea ar fi trebuit să fie gestionate.

În cazul în care ipoteza este adevărată, este necesară mai multă sensibilizare și creare de încredere în domeniu atunci când se informează respondenții cu privire la obiectivele cercetării, în special atunci când se îndreaptă spre apele necunoscute ale securității cibernetică. Mai mult, posibili respondenți trebuie să demonstreze conștientizare și cunoașterea acestor provocări legate de securitate și să împărtășească încredere, nu doar ce ține de integritatea partenerilor, ci și în capacitățile lor de securizare, întrucât existau cazuri cunoscute de spargere și scurgeri de informații sensibile în care a fost afectată nu doar persoana-țintă, dar și cei care au fost în contact strâns cu ea.

Printre cele 10 organizații chestionate, toate au același background: lucrul în sectorul OSC, cu un accent puternic pe combaterea dezinformării și a propagandei sau, într-o măsură mai mică, pe protecția drepturilor omului. Dar, din simplu motiv că aceste organizații sunt foarte conștiente de amenințările cibernetică și informaționale, este inacceptabil să presupunem că sectorul terțiar ucrainean în ansamblu știe să navigheze prin aceste amenințări, în cazul în care ar putea să nu aibă aceleași calificări în recunoașterea amenințărilor. Luând în considerare acest lucru, datele relevă următoarele tendințe:

### Instruire în domeniul securității operaționale

Majoritatea respondenților au declarat că instruirea în domeniul securității era indisponibilă sau insuficientă. Cei care au primit asistență educațională în această materie au primit-o adesea sub formă de protocoale și/sau instrucțiuni, ceea ce nu este la fel de eficient ca învățarea practică sub forma unor ateliere, chiar dacă este pe deplin înțeles și aplicat. Una dintre organizațiile implicate a menționat că, de regulă, furnizează astfel de instruiri de securitate operațională, în timp ce ar dori, de asemenea, să își consolideze propriile capacități de reziliență. Acest lucru indică o problemă de două nivele, în care unul dintre puținii furnizori de informații relevante s-ar putea să nu aibă acces la cele mai bune și cele mai recente instrumente de combatere a amenințărilor, împărtășind expertiză limitată cu alții și rămânând vulnerabil în același timp.



## **Prezența unor ghiduri de securitate operațională**

Doar 2 dintre respondenți au un protocol standard de securitate operațională. Unul încearcă să utilizeze un ghid oferit de o parte terță, dar chiar și atunci când este adoptat în mod corespunzător, lipsa de competențe practice menționate mai sus de a-l implementa corect expune în continuare organizația unui risc. Alții nu au nici un ghid specific sau fac referință la resursele proprii.

## **Gestionarea crizelor în timpul incidentelor de securitate**

Doar unul dintre respondenți a afirmat că va apela la propriul departament IT, ceea ce arată lipsa unor specialiști tehnici capabili să dezbată eventuale atacuri cibernetice. Majoritatea susțin că s-ar adresa fie colegilor, fie partenerilor internaționali. Fără aliați bine informați, aceste organizații sunt larg deschise în fața raiderilor digitali. Asistența externă este, de asemenea, limitată și adesea nu este obișnuită cu arsenalul aplicat pe peisajul mass-media din Ucraina. Interesant este faptul că încrederea OSC în instituțiile de aplicare a legii este atât de scăzută, încât doar 2 respondenți i-au menționat ca scăpare. Indiferent de partenerii lor, toți participanții la sondaj au subliniat necesitatea unor instruiți suplimentare în materie de securitate, în mare parte în domeniul informațiilor legate de muncă și al ciberneticii, dar și pentru îmbunătățirea securității personale. De asemenea, se atestă o lipsă de resurse umane respective (specialiști IT, etc.) la care ar putea apela cu diverse probleme de securitate.

## **Provocările legate de securitate**

### Securitatea cibernetică

Majoritatea respondenților și-au exprimat îngrijorarea pentru posibilitatea scurgerii de date, pierderii informațiilor personale, DDoS, phishing și altor tipuri de atacuri cibernetice. Păstrarea și securizarea datelor este de o importanță esențială, având în vedere agresiunea experimentată de unele organizații fie direct sau prin proxy. Datorită resurselor financiare limitate pe care le dețin în războiul pe Internet, nu este surprinzător faptul că OSC au declarat că provocările securității cibernetice rămân a fi cea mai comună responsabilitate.

### Securitatea informațională

Discreditarea țintită și daunele reputaționale sunt printre preocupările principale în domeniu. Problema securității datelor cu caracter personal și pierderea potențială a acestora prin divulgarea comunicării este, de asemenea, de mare relevanță.

### Securitatea personală

Mai multe organizații și-au exprimat îngrijorarea privind faptul că membrii lor ar putea fi arestați în țări (cum ar fi în Belarus – ceea ce s-a întâmplat de fapt cu unii reprezentanți ai altor OSC din Ucraina) care au legături strânse cu Federația Rusă. Ei și-au amintit destul de clar intimidările, amenințările personale directe (inclusiv pe cele anonime), furtul, atacul și daunele materiale suferite de colegii lor, indiferent dacă au fost sau nu aceste incidente clar motivate politic.

### Amenințări de viitor

Cei mai mulți dintre respondenți anticipează amenințări informaționale îndreptate spre discreditarea organizațiilor lor respective și provocarea de daune reputaționale. În timp ce puterea perturbatoare și violentă a guvernului Federației Ruse este foarte familiară într-o țară atacată, ei se tem că propriul stat va căuta răzbunare, dacă nu este prezentat într-o lumină pozitivă. Ei se tem că noua administrație aleasă (în 2019) va impune noi politici de comunicare care vor limita sever activitatea OSC și vor implica servicii de securitate secrete sau vor expune la amenințări cibernetice, cum ar fi scurgerea de date cu caracter personal și intimidarea.

### Sursele amenințărilor

Așa cum s-a detaliat mai sus, unii dintre respondenți se tem că guvernul Ucrainei și, în special, reprezentanții partidului prezidențial „Sluga Narodu”, trimișii prezidențiali și politicienii pro-ruși vor obstrucționa activitatea lor. Amenințările externe, și anume cele provenite din Federația Rusă, sunt o altă îngrijorare, ceea ce explică în rândul respondenților specializarea lor predominantă privind influența malignă rusească. Grupurile criminale locale, care includ și funcționari publici, care se folosesc în mod abuziv de putere, adesea încurajează presiunile asupra reprezentanților societății civile locale, care încearcă să dezvăluie astfel de fapte (existența grupurilor criminale locale).



MOLDOVA

## 5. MOLDOVA

Institutul pentru Inițiative Strategice (IPIS) a realizat un sondaj privind intimidarea online și provocările legate de securitatea cibernetică cu care se confruntă jurnaliștii, OSC, activiștii și reprezentanții mass-media din Republica Moldova, care lucrează cu problemele de influență rusă, propagandă, dezinformare, corupție etc. Zece respondenți au fost selectați pentru a completa chestionarul. După analiza chestionarelor, se pot evidenția următoarele puncte:

### **Instruire în domeniul securității operaționale**

Aproape toți respondenții au declarat că nu au primit ajutor privind securitatea operațională din partea vreunei organizații naționale sau internaționale. Unii au menționat că sunt autodidacți, în timp ce alți respondenți au spus că preferă să păstreze acest lucru în cadrul organizației lor.

### **Prezența unor ghiduri de securitate operațională**

Putem trage concluzia că practica de utilizare a manualelor, ghidurilor sau procedurilor privind securitatea operațională nu sunt răspândite în rândul OSC, activiștilor și reprezentanților mass-media din Republica Moldova. Cu toate acestea, putem menționa câteva aspecte pozitive. Majoritatea organizațiilor încearcă să se protejeze folosind soluții de securitate operațională standard oferite de Google și Facebook, cum ar fi autentificarea în doi pași, program Antivirus, firewall etc.

### **Gestionarea crizelor în timpul incidentelor de securitate**

În situații de criză de securitate, majoritatea respondenților au menționat că nu au încredere în instituțiile statului, cum ar fi Poliția sau Procuratura și în mare parte evită să le contacteze. Unii au afirmat chiar că simt ostilitate din partea instituțiilor statului și se confruntă cu un comportament cinic din partea Poliției și a Procuraturii. Interesant, în situațiile în care au fost atacate, persecutate sau șantajate, organizațiile au decis că cea mai bună modalitate de a se proteja este să informeze publicul despre astfel de incidente în încercarea de a se asigura că acestea nu se vor mai repeta.

### **Provocările legate de securitate**

#### Securitatea cibernetică

Majoritatea respondenților au numit trollingul și intimidarea online din partea actorilor guvernării drept principala provocare a securității pentru ei. Organizațiile efectuează investigații și raportează despre corupție, conflicte de interese și abuz de putere comise de reprezentanții guvernării. Respondenții au menționat că au existat atacuri asupra site-urilor lor și că găseau dispozitive suspecte în apropierea birourilor lor.



### Securitatea informațională

Aproape toți cei intervievați s-au confruntat cu scurgeri de parole Facebook și spargerea contului de e-mail. De asemenea, printre respondenții noștri este înaltă îngrijorarea privind discreditarea intenționată a jurnaliștilor, activiștilor OSC, etc. Acest lucru se realizează prin duplicarea sau crearea de conturi false - furt de identitate online. Practica s-a intensificat în timpul campaniei electorale în cadrul alegerilor parlamentare din februarie 2019, când mulți jurnaliști și activiști civici depistau impostori care comentau în numele lor pe diferite pagini publice. În acest caz, Facebook a luat o decizie fără precedent de a închide 168 de conturi Facebook, 28 de pagini și opt conturi pe Instagram în Moldova, unele aparținând oficialităților guvernamentale, deoarece se bănuia că răspândesc știri false, propagandă politică și dezinformare în preajma alegerilor. Echipa de presă Facebook a declarat că, deși persoanele din spatele acestei activități au încercat să-și ascundă identitățile, analiza lor manuală a constatat că o parte din această activitate avea legături cu angajații guvernului Republicii Moldova.

### Securitatea personală

Mai mulți respondenți au raportat atacuri, amenințări, intimidare fizică și daune auto în timpul activității lor pe teren. Unele dintre aceste acțiuni au fost săvârșite de persoane neidentificate, în timp ce altele de către angajații instituțiilor de aplicare a legii. Așa a fost cazul protestului desfășurat de Occupy Guguță, când polițiștii au impus activiștii să elibereze locul de protest. De asemenea, au fost confiscate pancartele și alte materiale. Mai mult, canalele de televiziune legate de guvern au încercat să răspândească știri false despre mișcarea de protest prin infiltrarea unor persoane dubioase, a alcoolicilor în zona unde se desfășura protestul. Astfel, provocând probleme de securitate personală protestatarilor.

### Amenințări de viitor (în următorii 1-3 ani)

Majoritatea respondenților au fost deja șantajați, intimidați, atacați în judecată, hărțuiți și atacați fizic. De asemenea, ei au atras atenția asupra unor modificări ale legislației care ar putea afecta activitatea lor de zi cu zi: Legea cu privire la organizațiile necomerciale, Legea privind libertatea mass-media, Legea privind granturile din străinătate, Legea privind accesul la informație. Având în vedere subiectele pe care le evidențiază (infracțiuni financiare, corupție, abuz de putere), posibilele amenințări se pot referi la șantaj, hărțuire sau chiar detenția ilegală a rudelor. Alte amenințări posibile se pot referi la hărțuirea din partea autorităților fiscale sau chiar a organului legislativ (în perioada de raportare, Parlamentul a avut o inițiativă de a interzice finanțarea externă pentru OSC din Moldova).

### Sursele amenințărilor

Toți respondenții au indicat că cea mai mare sursă de risc reprezintă actorii interni, și anume guvernul, care acționează prin instituțiile de aplicare a legii sau prin persoane legate de guvernul Moldovei, care au condus campanii frauduloase pe Facebook, folosind tactica vestitei „ferme de troli” din Rusia. Acest lucru cauzează, de asemenea, un posibil pericol de intervenție externă, deoarece agenții Kremlinului știu să exploateze pe cei slabi în astfel de situații.



GEORGIA

## 6. GEORGIA

Fundația de Dezvoltare a Mass-media (MDF) a realizat un sondaj privind intimidarea online și provocările legate de securitatea cibernetică cu care se confruntă OSC-urile, activiști și reprezentanți ai mass-media care lucrează cu problemele legate de propaganda rusească, corupție și drepturile omului. Pentru sondaj au fost selectați 24 de respondenți, care a fost realizat folosind o metodă mixtă de anchetare. Analiza datelor colectate a relevat următoarele tendințe:

### **Instruire în domeniul securității operaționale**

Majorității respondenților nu li s-a oferit instruire sau alt ajutor procedural în domeniul securității operaționale. Mai mulți respondenți au participat la instruire cu privire la securitatea digitală, care nu a acoperit complet mecanismele de evitare a amenințărilor necesare acestei persoane/organizații.

### **Prezența unor ghiduri de securitate operațională**

Majoritatea respondenților nu utilizează ghiduri în securitate operațională în timpul activităților lor organizaționale. Doar un număr mic au elaborat reguli interne.

### **Gestionarea crizelor în timpul incidentelor de securitate**

Majoritatea respondenților au remarcat că în timpul incidentelor de securitate cibernetică apelează la serviciul IT al organizației, precum și Biroul de securitate cibernetică al Ministerului Apărării și unitatea cibernetică a Ministerului de Interne. După ce dezvăluie cazurile cu elemente de crimă, ei raportează la poliție.

În cazurile unor incidente de securitate informațională (încălcarea securității datelor cu caracter personal), respondenții raportează inspectorului pentru protecția datelor cu caracter personal și, în cazuri rare, Apărătorului Public.

Unii respondenți nu au informații cui ar trebui să se adreseze în cazuri unor diverse incidente în vederea soluționării problemei și luării unor măsuri relevante.

Aproape toți respondenții au nevoie de instruire în domeniul securității digitale (parolă, securitatea rețelei interne, detectare ransomware) și informaționale (protecția datelor cu caracter personal). Majoritatea respondenților au remarcat importanța dezvoltării abilităților care îi vor ajuta să rezolve eficient problemele în timpul diferitelor crize. Unii respondenți au remarcat că au nevoie de ajutor în planificarea continuității afacerii.

### **Provocările legate de securitate**

#### Securitatea cibernetică

Majoritatea respondenților au indicat trolling-ul și intimidarea online din partea grupurilor ultranaționaliste și actorilor guvernamentali drept principala provocare a securității. În special este demn de remarcat așa-numitul trolling guvernamental cauzat de materiale critice despre activitatea guvernului.

Atacurile de tip phishing și spargere asupra site-urilor oficiale ale organizațiilor în încercarea de a obține informații sunt de asemenea numite de respondenți drept probleme semnificative. Site-ul ([www.eurocommunicator.ge](http://www.eurocommunicator.ge)) detectorului de mituri al Fundației MDF a fost de două ori victima unor atacuri hacking din partea Luxas Hacker în 2015. În timpul primului atac a fost imposibil de urmărit hackerul, însă în timpul celui de-al doilea atac s-a stabilit că atacul s-a produs de pe o adresă IP înregistrată în Turcia. Clipurile video încărcate pe YouTube arată clar adresa unui site "Dark Mirror" <http://dark-mirror.org>. Hackerul folosea link-ul când a atacat site-ul.

Pe 28 octombrie 2019 Georgia a devenit ținta unor atacuri cibernetice masive. Hackerii au ținut site-urile guvernului și a agențiilor private ale Georgiei, precum și instituțiile media (TV Pirveli, Imedi, Maestro, Trialeti și Sakinform) și organizații neguvernamentale (Fundația de Dezvoltare a Mass-media).

Paginile de pornire ale site-urilor sparte de hackeri au fost înlocuite cu o imagine a fostului președinte al Georgiei, Miheil Saakașvili, cu titlul „I'll be back” („Voi reveni”).

Site-urile sparte de hackeri au fost încărcate pe serverele Pro-Service, un furnizor local de hosting. Potrivit companiei, aproximativ 15 000 de pagini au fost afectate ca urmare a atacului cibernetic. Ministerul de Interne a anunțat că a lansat o anchetă în temeiul articolelor 284 și 286 din Codul penal al Georgiei, care implică accesul neautorizat la sistemul informatic, precum și manipularea neautorizată a datelor informatice și/sau a sistemelor informatice.

Ministerul de Interne a declarat că „atacul cibernetic ar fi putut să fie efectuat atât din interiorul, cât și din afara țării.” „Măsurile de investigație au relevat faptul că atacul cibernetic a fost efectuat, provocând așa-numita denaturare a site-ului - modificări ale aspectului vizual al paginilor de pornire.”

„Comaniile private din Georgia oferă servicii de hosting majorității companiilor vizate. Stilul atacurilor cibernetice asupra fiecărui site este identic,” se menționa în declarație.

Toate site-urile web încărcate pe serverele companiei Pro-Service au reluat operațiunile pe 29 octombrie.

### Securitatea informațională

Discreditarea intenționată a respondenților de către grupuri radicale și trolii guvernamentali pentru a se asigura că informațiile răspândite de ei pierd legitimitate a fost numită de respondenții chestionați ca o problemă larg răspândită. În ceea ce privește securitatea informațională, majoritatea respondenților au accentuat problema dezvăluirii datelor cu caracter personal (spargerea de conturi, scurgeri de informații, dezvăluiri a comunicării, furt de identitate online).

### Securitatea personală

Un număr de organizații au devenit ținte ale atacurilor, amenințărilor (răfuială fizică, viol) și ale agresiunii din partea grupurilor ultranaționaliste, care au devenit mai puternice în ultimii ani. Jurnaliștii chestionați au remarcat cazuri de daune fizice și materiale (dispozitive și mașini stricate). Mai mulți respondenți au devenit ținte ale atacurilor fizice pur și simplu pentru că își desfășurau activitățile jurnalistice.

Jurnalistul postului TV Rustavi 2, Davit Eradze a devenit ținta unei răfuieli fizice din partea membrilor mișcării ultranaționaliste „Marșul Georgian” (2018); mai mult, casa sa a fost împușcată și pe balconul său au fost găsite cartușe pur și simplu pentru că a pregătit un reportaj TV în timpul activităților sale jurnalistice (2019);



Jurnaliștii de la Tabula au fost atacați într-un restaurant, unde atacatorii citau insulte la adresa bisericii lor din partea Tabula drept motiv (2016).

În plus, 39 de reprezentanți ai diverselor agenții media au suferit leziuni fizice în timp ce își îndeplineau atribuțiile profesionale în timpul împrăștierii mitingului împotriva ocupației din 21 iunie.

### Amenințări de viitor (în următorii 1-3 ani)

Majoritatea respondenților consideră că cazurile de trolling și intimidare online din partea grupurilor ultranaționaliste și actorilor guvernamentali, precum și discreditarea online, dezvăluirea datelor cu caracter personal și amenințările vor continua pe parcursul următorilor 1-3 ani. Potrivit acestora, unele organizații/reprezentanți pot deveni chiar ținte ale unor atacuri fizice și arestări.

### Sursele amenințărilor

Printre principalele surse de amenințări, respondenții au numit insiderii – structuri de stat, grupuri de ură angajate și încurajate de aceștia și actori marginalizați, inclusiv trolii. În ceea ce privește principala sursă de amenințări externe, respondenții au numit actorii Kremlinului și sateliții acestora (persoane fizice și organizații), deoarece unii dintre respondenții chestionați lucrează cu probleme legate de influența rusească.

Respondenții au spus că nu au primit ajutor de la donatori internaționali/guverne pentru a soluționa aceste amenințări.

## 7. CE SE POATE FACE? RECOMANDĂRI PENTRU OSC ȘI ACTIVIȘTII CIVICI

OSC ar trebui să urmeze manualul privind securitatea de bază care include domeniile de securitate cibernetică, informațională, contrainformațională și personală.

### Nivele de sensibilitate a informațiilor

În general, distingem trei nivele de sensibilitate informațională. Criteriul principal este nivelul de importanță politică, personală și de securitate pentru organizație, persoane fizice și securitate.

Motivul clasificării este de a asigura respectarea principiului dovedit în timp „nevoia de a cunoaște” – informațiile sensibile sunt oferite doar celor care trebuie să le cunoască dintr-un motiv specific.

NIVELUL DE SENSIBILITATE	CRITERIUL IMPORTANȚEI	UNDE PUTEM DISCUTA INFORMAȚIA ÎN PERSOANĂ	UNDE PUTEM DISCUTA INFORMAȚIA PRIN INTERMEDIUL ELECTRONICII
0	Informații operaționale obișnuite, care nu sunt sensibile din punct de vedere politic sau al securității, sunt de facto informații publice	Oriunde	Oriunde: e-mail, Facebook, etc.
1	<b>Informații interne</b> (informații politice non-publice care nu prezintă o amenințare la adresa securității naționale, sau a persoanelor implicate)	Numai într-o întâlnire stabilită sau bilateral cu o persoană responsabilă, <u>fără prezența dispozitivelor electronice.</u>	<u>Doar</u> semnal (mesaj sau apel) sau <u>ProtonMail</u> , nu e-mail, SMS sau apel telefonic
2	<b>Informații foarte sensibile</b> (legate de securitatea națională, identitatea surselor sensibile, informații-bombă din punct de vedere politic)	Numai într-o întâlnire stabilită sau bilateral cu o persoană implicată, <u>fără prezența dispozitivelor electronice.</u>	<b>Nicăieri, doar în persoană fără electronică</b>

**Fiecare membru al organizației trebuie să stabilească și să urmeze aranjamentele de securitate în cinci direcții:**

- Securitatea cibernetică de bază a dispozitivelor și profilelor
- Securitatea pe rețelele de socializare
- Securitatea comunicării
- Securitatea datelor
- Securitatea personală

## Securitatea cibernetică de bază a dispozitivelor și profilelor

### a. Regulile de bază de securitate

Presupunem că dvs. folosiți doar sisteme de operare pe larg utilizate. În cazul computerelor „clasice”, asta înseamnă Windows și macOS, în cazul computerelor portabile (adică tablete și telefoane mobile) iOS și Android. Produsele Apple (deși semnificativ mai scumpe) sunt considerate cele mai sigure dispozitive, urmate de Android. Vă recomandăm insistent să nu folosiți niciun produs Lenovo.

#### i. Setarea parolei

**Regula nr. 1:** Folosim parole diferite pentru conturi diferite (numere diferite, caractere speciale, etc.). Există un scurt manual despre cum se face acest lucru pe pagina web pe Mozilla.

**Regula nr. 2:** Parola trebuie să aibă cel puțin 22 de caractere fiind compusă din litere, cifre și caractere speciale.

**Regula nr. 3:** Parolele trebuie schimbate în mod ideal la fiecare 3 luni. Este convenabil să introduceți un memento în calendarul dvs.

**Regula nr. 4:** Parolele le notăm doar pe hârtie (care se păstrează într-un loc cunoscut doar de dvs., nu la locul dvs. de muncă și în fiecare parolă trebuie să lipsească întotdeauna cel puțin un caracter, astfel încât acestea să fie inutilizabile în cazul pierderii hârtiei) și niciodată în documente de tip text stocate pe computer. Există o excepție sub forma managerilor de parole, cum ar fi LastPass sau KeePas2. Un alt instrument pentru securitatea parolelor poate fi așa-numitul breloc electronic (iOS – iCloud Keychain, Windows – Smart Lock, alt 1Password), pe care vă recomandăm să îl utilizați pentru o autentificare cu doi factori sau criptarea discului (vezi mai jos).

#### ii. Autentificare cu doi factori = codul generat trebuie introdus împreună cu parola

**Regula nr. 5:** Autentificarea cu doi factori trebuie activată pentru fiecare serviciu care permite acest lucru. Codul poate fi transmis prin mesaj text sau o aplicație mobilă. Vă recomandăm să nu utilizați autentificarea mesajelor text și să setați Google Authenticator. Cel puțin, este esențial pentru Facebook, Twitter, Google și internet banking. Vă recomandăm să nu utilizați tehnologia de recunoaștere facială.

- Pagina web afișează un cod QR pe care îl scanăm folosind o aplicație mobilă. Apoi se adaugă contul respectiv. La fiecare 30 de secunde, aplicația afișează un nou cod unic, care trebuie utilizat în termenul său de valabilitate. Pentru a utiliza aplicația nu este necesar să aveți o conexiune la Internet sau chiar semnal de rețea pe telefonul mobil; dispozitivul și serverul sunt sincronizate pentru totdeauna după ce le-ați configurat pentru prima dată. Instrumente universale: Google Authenticator (iOS, Android), Authy.

**Regula nr. 6:** Întotdeauna ieșiți din aplicație sau e-mail de pe dispozitiv după terminarea lucrului, astfel încât altcineva după dvs. va trebui să se conecteze din nou. Vă recomandăm să utilizați o altă parolă și amprentă pentru a deschide aplicații importante (Signal, Wickr Me, ProtonMail).

**Regula nr. 7:** Nu vă conectați niciodată la profilurile principale (Google, Facebook, internet banking) pe dispozitivele altor persoane decât dacă este absolut necesar. Dacă o faceți, schimbați parolele după aceea. În setările de confidențialitate Facebook, activați notificările despre autentificări de pe dispozitive

nerecunoscute, în mod ideal prin e-mail. Setează parola de firmware pe dispozitivul Mac.

**Regula nr. 8:** Dacă primiți un e-mail sau un mesaj privat suspect, trimiteți-l colegilor dvs. cu un avertisment puternic (în câmpul subiectului și corpul mesajului) să nu-l deschidă și să îl trimită la [cert.incident@nukib.cz](mailto:cert.incident@nukib.cz). Specialiștii de la NUKIB vă vor ajuta să urmați pașii, dacă este nevoie (de exemplu, în caz de ransomware, etc.).

#### b. Antivirus

**Regula nr. 9:** Sistemele de operare, cum ar fi Windows 10, au deja antivirus încorporat (Windows 10). În general, nu este necesară instalarea unei protecții terțe contra plată. Dacă utilizați o astfel de protecție, evitați produsele de la Kaspersky Lab (deoarece există o suspiciune rezonabilă că este conectat la serviciile de informații ruse), Huawei sau ZTE (deoarece există o suspiciune rezonabilă că colaborează cu serviciile de informații chineze). Vă recomandăm Avast Antivirus sau Eset. Vă recomandăm insistent să nu utilizați program antivirus chinezesc (de ex., Qihoo 360, Tencent PC Manager). Vă recomandăm să utilizați 2 programe antivirus în același timp. Descărcați programul VirusScanner.

**Regula nr. 10:** Marea majoritate a atacurilor cibernetice sunt prin e-mail – phishing. Baza unei protecții funcționale împotriva virușilor este evitarea deschiderii atașamentelor de e-mail venite de la expeditori necunoscuți. Fiți în special precauți când fișierul atașat are extensie, cum ar fi .exe, .pkg, .dmg sau .app. Mai mult, nu uitați să verificați autenticitatea expeditorului înainte de a deschide atașamentul. Țineți minte că chiar și fișierele în formate precum .pdf sau .doc. pot conține procese nocive de fundal. Dacă vi se solicită, întotdeauna refuzați „activarea macrouilor” în Excel. Dacă cineva vă trimite un link, este bine să-l copiați și să-l plasați pe [virustotal.com](http://virustotal.com) mai întâi, deoarece vă va oferi cel puțin o idee dacă este de încredere. După aceea aplicați Regula nr.8.

Dacă sunteți sigur că dispozitivul a fost infectat cu malware, cel mai sigur și cel mai bine este să ștergeți conținutul media cu un instrument de ștergere a discului, să reinstalați sistemul de operare și aplicațiile și să copiați datele dintr-o copie de rezervă (după ce ați verificat că copia de rezervă nu este infectată).

Dacă bănuieți că dispozitivele sunt infectate, porniți imediat o scanare pentru malware. Chiar dacă scanarea dă rezultat negativ, continuați să fiți proactivi, urmând acești pași. Dacă încă aveți suspiciuni, folosiți un al doilea produs AV.

Acțiunile ar trebui să includă:

##### i. WINDOWS

**Pasul 1:** Deconectați computerul de la rețea. Porniți scanarea pentru malware (preferabil de pe un stick USB extern care conține AV actualizat).

**Pasul 2:** Accesați Safe Mode. Faceți acest lucru prin deconectarea și pornirea din nou a computerului. Apoi, imediat ce vedeți ceva pe ecran, apăsați mai multe ori repetat butonul FS. În mod normal, va apărea meniul Advanced Boot Options. De acolo, alegeți Safe Mode și apăsați Enter.

**Pasul 3:** Ștergeți fișierele temporare. În timp ce vă aflați în Safe Mode, trebuie să ștergeți fișierele temporare, utilizând instrumentul Disk Cleanup. Pentru a face acest lucru:

- Accesați meniul Start;



- All Programs sau doar Programs;
- Accessories-System Tools, Windows Administrative Tools (în dependență de versiune)
- Disk Cleanup;
- Scroll through the Files to Delete list, and choose Temporary Files.

Deleting these files could remove malware if it was programmed to start when your computer boots

**Pasul 4:** Descărcați și porniți un program de scanare de viruși. Dacă dispozitivul a fost infectat, atunci anti-malware-ul dvs. nu l-a interceptat. Trebuie să descărcați (pe un alt computer), apoi să-l transferați pe computerul respectiv și să-l instalați (sau să-l porniți):

- Un program de scanare în timp real, cum ar fi AVG Antivirus gratuit sau Avast Free Antivirus, care scanează pentru malware în fundal în timp ce dvs. utilizați computerul;
- Un scanner al sistemului de operare la cerere, precum Microsoft Security Scanner, dar acesta trebuie să fie pornit manual de fiecare dată când doriți să scanați

Poate apărea necesitatea să folosiți ambele tipuri de scanner pentru a elimina programul malware. În funcție de tipul programului anti-malware, poate apărea necesitatea să vă reconectați la internet și să descărcați un produs suplimentar.

Poate apărea necesitatea să eliminați virusul manual. Puteți să încercați acest lucru numai dacă aveți experiență în utilizarea Registrului Windows și știți să vizualizați și să ștergeți fișierele de sistem și de program.

**Pasul 5:** După ce ați eliminat programele malware, va trebui să restabiliți (din copiile de rezervă) sau să reinstalați orice fișier sau software deteriorat.

#### c. Actualizări de software

**Regula nr. 11:** Actualizările de software sunt absolut esențiale. Asigurați-vă că atât pe computer, cât și pe telefonul mobil al dvs. sunt activate actualizările automate.

- Dacă aveți o versiune mai veche de Windows (cum ar fi 7 sau 8), este necesar să păstrați setările de actualizare la modul implicit (adică să țineți actualizările automate activate). Dacă sistemul dorește să instaleze o actualizare, trebuie să lăsați să facă acest lucru. În Windows 10, nu există o modalitate ușoară de a dezactiva actualizările (le puteți amâna doar în versiunea Pro, pe care nu o recomandăm).
- Mac: În mod implicit, sistemul verifică automat actualizările prin intermediul aplicației Mac App Store. Apple oferă întotdeauna cel mai bun suport doar pentru cea mai nouă versiune de macOS. Activați actualizările automate în Mac/About this Mac/Updates/Advanced.
- Sistem de operare mobil: verificați în mod regulat actualizările din setările sistemului și întotdeauna mențineți cea mai actuală versiune. Pentru iPhone, vă recomandăm aplicația iVerify, care vă ghidează în mai mulți pași prin toate măsurile de securitate necesare.
- Navigatoarele implicite (Safari, Internet Explorer, Edge sau Chrome în dispozitivele Android) sunt de obicei actualizate împreună cu sistemul de operare în sine. Navigatoarele terțe, cum ar fi Chrome sau Firefox, sunt actualizate separat, de obicei în mod automat. Dacă browser-ul vă oferă o actualizare, trebuie să o instalați imediat! Deținerea unui browser web actualizat este cu adevărat alfa și omega a securității Internetului. Vă

recomandăm să instalați aplicația „HTTPS Everywhere”, care controlează pentru dvs. securitatea site-urilor web vizitate.

d. Cum să blocați și să urmăriți corect dispozitivele mobile

**Regula nr. 12:** Este esențial să utilizați un cod numeric sau alt cod pentru deblocarea dispozitivului (parolă cu cel puțin 22 de caractere). Dacă dispozitivul are un scanner de amprente, activați-l.

- De asemenea, este esențial să setați blocarea pe laptop, astfel încât acesta să se blocheze și să solicite parola de fiecare dată când îl închideți și îl redeschideți. Blocați computerul de fiecare dată când îl lăsați chiar și pentru scurt timp (apăsați butonul Windows + L).
- Cumpărați o folie de ecran care va permite să priviți ecranul doar dintr-un unghi drept și va împiedica străinii să vadă ce scrieți sau faceți din alte unghiuri. Când lucrați cu date sensibile, acordați atenție poziției dvs. față de ferestre. Cea mai bună modalitate de a obține parole și alte date este privind prin ferestre.

**Regula nr. 13:** De obicei, în setările dispozitivului există o opțiune de a șterge toate datele dacă s-a făcut un anumit număr de încercări nereușite de deblocare a acestuia. Vă recomandăm să mențineți această opțiune activată. Mai mult, este bine să aveți o parolă la cartela dvs. SIM, astfel încât să nu fie posibil să fie introdusă pur și simplu într-un alt telefon.

**Regula nr. 14:** Este obligatoriu să fie activată opțiunea urmăririi telefonului. În iOS, porniți funcția Găsiți iPhone-ul meu (aici puteți găsi instrucțiuni suplimentare, Apple descrie, de asemenea, ce ar trebui să faceți în cazul în care iPhone-ul dvs. se pierde sau este furat). Dacă utilizați Android, trebuie să instalați și activați Managerul de dispozitiv Android (Android Device Manager).

- Pierderea sau furtul unui dispozitiv: trebuie să deschideți imediat aplicația pe un alt dispozitiv sau internet (Managerul de dispozitiv Android/iCloud), să vă conectați la contul dvs. și să încercați să localizați dispozitivul. Folosind aceste instrumente, puteți șterge în siguranță toate datele stocate pe dispozitiv, chiar dacă nu este posibilă localizarea acestuia la moment – datele vor fi șterse în clipa în care dispozitivul este conectat la Internet.

**Regula nr. 15:** Dispozitivele Apple, de asemenea au o funcție numită Activation Lock. Dacă funcția Găsiți iPhone-ul meu este pornită și ștergeți dispozitivul prin intermediul acesteia, totuși el va fi asociat cu contul dvs. ceea ce înseamnă că hoțul nu îl va putea folosi sau activa, ceea ce îl va împiedica să-l vândă pe piața neagră. Dispozitivul va fi asociat cu contul dvs. pentru totdeauna, cu excepția cazului în care tastați fizic parola sau noul proprietar o va afla – ceea ce în combinație cu autentificarea cu doi factori este practic imposibil.

- Android: dacă Managerul de dispozitiv Android este activat, ar trebui să aveți acces la toate funcțiile de securitate oferite de telefonul dvs.
- Serviciile precum Găsiți iPhone-ul meu sau Android Pierdut vă permit, de asemenea, să accesați dispozitivul de la distanță și să ștergeți toate datele stocate în el în caz de pierdere sau furt

**Regula nr. 16:** De asemenea, este important să fii prudent atunci când folosești Wi-Fi sau Bluetooth pe dispozitivele mobile. Aceste servicii ar trebui întotdeauna oprite dacă nu sunt utilizate. În plus, limitați la minim numărul de aplicații care au acces la datele locației dvs. De obicei, poate fi setat în mapa Setări/Aplicații/Accese. Parcurgeți toate accesele și apreciați dacă sunt rezonabile, apoi dezactivați-le pe toate celelalte. Atragem atenție împotriva utilizării dispozitivelor Bluetooth hands-free (imprimante, căști), deoarece acestea prezintă un risc suplimentar de securitate. Vă recomandăm să achiziționați așa-

numitul „prezervativul încărcătorului”, care vă asigură că în dispozitivul dvs. curge doar energie electrică. Acest tip de penetrare a dispozitivului este foarte simplu dacă nu este luat în considerare.

**Regula nr. 17:** Camera foto și microfonul de pe dispozitivul dvs. mobil pot fi activate de la distanță. Nu purtați niciodată smartphone-ul dvs. în locuri unde acesta poate fi folosit de oponent pentru a aduna informații sensibile. În timpul întâlnirilor sensibile, îndepărtați telefonul sau, dacă este posibil din punct de vedere tehnic, scoateți bateria. Soluția ideală este să puneți toate dispozitivele electronice într-o geantă pe care apoi să o îndepărtați la cel puțin 7-10 metri distanță de dvs. În acest fel, veți putea urmări geanta, însă dispozitivele vor fi incapabile să vă „asculte” conversația. În afară de capacul camerei, vă recomandăm să dezactivați camera la computerul dvs. și să instalați aplicația „Oversight”, care ghidează utilizarea din exterior a camerei și a microfonului.

**Regula nr. 18:** Este convenabil să acoperiți camera web de pe laptop și să înlăturați coperta doar atunci când este nevoie. Același lucru este valabil și pentru telefonul mobil – acoperiți camera cu un acoperământ și scoateți-l doar atunci când este nevoie.

e. Copierea de rezervă și protocolul de urgență (în cazul pierderii/furtului dispozitivului)

**Regula nr. 19:** Vă recomandăm să faceți o copie de rezervă a documentelor personale și de lucru pe un hard disk extern criptat pe care îl țineți în siguranță acasă și off-line. Compania iStorage vinde dispozitive de hard disk externe ieftine și bine criptate. Se recomandă de păstrat datele foarte sensibile pe un computer curat izolat, care nu se conectează niciodată la Internet. Vă recomandăm să faceți copii de rezervă a calendarului personal (în mod ideal pe Google), care poate fi util dacă doriți să verificați evenimentele de acum mai mulți ani în urmă.

**Regula nr. 20:** Există o mulțime de aplicații de criptare a discurilor, gratuite și pe bani. Deseori se recomandă VeraCrypt.

**Regula nr. 21:** Copii de rezervă trebuie să faceți doar pentru documente unice și de neînlocuit. În marea majoritate a cazurilor, pentru asta nu va fi nevoie mai mult decât câteva sute de MB. Asigurați-vă că faceți o copie de rezervă cel puțin o dată pe lună.

f. În cazul pierderii sau furtului dispozitivului

**Pasul 1:** verificați locația dispozitivului utilizând serviciul de urmărire ales. Dacă ați lăsat telefonul sau tableta la școală, la serviciu sau la o cafenea, contactați personalul și luați dispozitivul cât mai curând posibil. Un astfel de scenariu nu prezintă un risc semnificativ.

**Pasul 2:** dacă localizați dispozitivul în locuri pe care nu le-ați vizitat sau vedeți că acesta se deplasează, vă sugerăm să contactați imediat poliția și să transmiteți informațiile despre locația dispozitivului. Este important de acționat rapid, deoarece veți putea vedea locația dispozitivului numai până când bateria acestuia va activa sau va fi conectat la Internet.

**Pasul 3:** dacă știți că aveți informații extrem de sensibile stocate pe dispozitiv și din anumite motive nu ați acționat conform recomandărilor din capitolele anterioare, vă recomandăm imediat să ștergeți de la distanță dispozitivul.

**Pasul 4:** schimbați imediat parolele la toate conturile.

**Regula nr. 22:** În cazul pierderii sau furtului dispozitivului, întotdeauna țineți minte că este mai bine să pierdeți, de exemplu, 14 zile de muncă terminată decât

să puneți în pericol securitatea tuturor datelor stocate pe dispozitivul dvs. Mai mult, ignorând acest lucru, puteți pune în pericol și datele stocate pe serverele cloud ale angajatorului dvs. Dacă nu puteți purta telefonul la dvs. personal (dacă este necesară depozitarea într-un vestiar), folosiți pungi de etanșare de unică folosință pentru a vă asigura că telefonul nu a fost manipulat. Acestea se numesc plicuri de securitate și pot fi achiziționate de exemplu la EuroSeal.cz.



## Securitatea pe rețelele de socializare

**Regula nr. 23:** Fiți strict în configurarea setărilor dvs. de confidențialitate pe Facebook – faceți-vă postările vizibile doar pentru prietenii dvs., eventual puteți crea diverse grupuri pentru conținut specific în rândul prietenilor. Asigurați-vă că trebuie să aprobați postările în care sunteți etichetat. Mai jos puteți găsi un manual detaliat. Nu respectați aceste reguli dacă profilul dvs. de Facebook este o prezentare publică intenționată.

The screenshot shows the Facebook Privacy Settings interface. A red arrow points to the 'Privacy Settings' link in the top right menu. The main content area is titled 'Privacy Settings' and includes a warning: 'Every time you post a status, it's a good idea to make sure it's for your friends only.' Below this, there are six numbered sections: 1. Control Your Default Privacy (set to Friends), 2. How You Connect (set to Friends), 3. Timeline and Tagging (set to Friends), 4. Ads, Apps and Websites (set to Limit use of Apps), 5. Limit the Audience for Past Posts (set to Friends Only), and 6. Blocked People and Apps (set to Manage blocked people and apps).

**About Facebook Apps**

Do not login to or link third-party sites (e.g. Twitter, Bing, LinkedIn) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information.

Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Edit your profile by changing all the options to **Only Me** (most secure) or **Friends Only**.

**Editing Your Privacy Settings**

- 1) Control Your Default Privacy** – Change to Friends Only
- 2) How You Connect**
  - a. Who can look up using your e-mail or phone number? - **Friends**
  - b. Who can look you up using the email address or phone number you provided? - **Friends**
  - c. Who can send your friend requests? - **Friends of Friends**
  - d. Who can send you Facebook messages? - **Friends**
- 3) Timeline and Tagging**
  - a. Who can post on your Timeline? - **Friends**
  - b. Who can see what others post on your timeline? - **Friends**
  - c. Review posts friends tag you in before they appear on your timeline? - **On**
  - d. Who can see posts you've been tagged in on your timeline? - **Friends**
  - e. Review tags friends add to your own posts on Facebook - **On**
  - f. Who sees tag suggestions when photos that look like you are uploaded? - **Friends**
- 4) Ads, Apps and Websites**
  - a. Apps you use – **Limit use of Apps**
  - b. How people bring your info to apps they use – **Uncheck all boxes**
  - c. Instant personalization – **Disable Personalization**
  - d. Public Search – **Disable Public Search**
  - e. Ads >subpages>Ads shown by third parties – **No one**
  - f. Ads >subpages>Ads and friends – **No one**
- 5) Limit the Audience for Past Posts** – **Limit the Old Posts to Friends Only**
- 6) Blocked People and Apps** – Here you can block certain people, events and game invites.

# MANUAL CU PRIVIRE LA AMENINȚĂRILE DE SECURITATE CIBERNETICĂ, INFORMAȚIONALĂ, CONTRAINFORMAȚIONALĂ ȘI PERSONALĂ

General

Security and login

Privacy

**Timeline and Tagging**

Blocking

Language

Notifications

Mobile

Public Posts

Apps

Adverts

Payments

Support Inbox

Videos

### Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Only me	Edit
	Review posts that friends tag you in before they appear on your Timeline?	On	Edit
Who can see things on my Timeline?	Review what other people see on your Timeline		View As
	Who can see posts you've been tagged in on your Timeline?	Only me	Edit
	Who can see what others post on your Timeline?	Only me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Only me	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

## Public Post Filters and Tools

Who Can Follow Me

Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you.  
  
Each time you post, you choose which audience you want to share with.  
[Learn more.](#)

Friends ▼

Public Post Comments	Who can comment on your public posts? Friends	Edit
Public Post Notifications	Get notifications from Nobody	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit
Comment Ranking	Comment ranking is Off	Edit
Username	You have not set a username.	Edit
Twitter	Connect a Twitter account	Edit

**Regula nr. 24:** Este înțelept să vă ascundeți adresa de acasă, numărul de telefon, e-mailul și alte date (sau să nu le introduceți de la bun început, Facebook adesea le vinde persoanelor terțe). Accesați fila „Despre” pe Facebook – ștergeți adresa dvs. și setați adresa de e-mail și numărul de telefon la „Doar eu”, astfel încât să nu fie vizibilă pentru nimeni altcineva. Priviți modul în care arată profilul dvs. din perspectiva unui prieten sau a unui străin folosind funcția „Vezi ca”. Pentru a fi sigur, căutați cu ajutorul Google adresa dvs. de e-mail, adresa de acasă și numărul de telefon pentru a vedea unde sunt accesibile aceste informații și de unde pot fi șterse. De asemenea, trebuie să repetați această procedură pentru membrii familiei.

**Regula nr. 25:** Limitați posibilitatea de a vă vedea profilul doar pentru prieteni. În fiecare lună ștergeți conținutul tuturor conversațiilor dvs. pe Facebook. Dacă cineva vă fură profilul, nu va obține date sensibile din conversațiile personale ale dvs.

**Regula nr. 26:** Nu permiteți altor motoare de căutare decât Facebook să vă aceseze profilul.

The image shows a screenshot of the LinkedIn privacy settings page. The left sidebar contains a menu with the following items: Profile privacy, Blocking and hiding, Job seeking (highlighted with a blue bar), Data privacy and advertising, and Security. The main content area is divided into three sections: Job seeking, Data privacy and advertising, and Profile privacy. Each section contains several settings with 'Change' or 'No' buttons. The Job seeking section includes 'Sharing your profile when you click apply' (set to 'No'), 'Let recruiters know you're open to opportunities' (set to 'No'), and 'Update career interests'. The Data privacy and advertising section includes 'Manage who can discover your profile from your email address' (set to 'Nobody'), 'Manage who can discover your profile from your phone number' (set to 'Nobody'), 'Representing your organization' (set to 'No'), 'Profile visibility off LinkedIn' (set to 'No'), 'Advertising preferences' (set to 'No'), and 'Two-step verification' (set to 'On'). The Profile privacy section includes 'Edit your public profile' (set to 'No'), 'Manage active status' (set to 'No'), 'Display your active status' (set to 'No'), 'Hide active status from select people' (with a search bar), 'Who can see your connections' (set to 'Only you'), 'Viewers of this profile also viewed' (set to 'No'), 'Sharing profile edits' (set to 'No'), 'Profile viewing options' (set to 'Private mode'), 'Notifying connections when you're in the news' (set to 'No'), and 'Who can see your last name' (set to 'Abbreviated').

**Job seeking**

**Sharing your profile when you click apply** Change No  
Choose if you want to share your full profile with the job poster when you're taken off LinkedIn after clicking apply

**Let recruiters know you're open to opportunities** Close  
Share that you're open and appear in recruiter searches matching your career interests

We take steps not to show your current company that you're open, but can't guarantee complete privacy. [Learn more](#)

No ☐ Update career interests

**Data privacy and advertising**

**Manage who can discover your profile from your email address** Change Nobody  
Choose who can discover your profile if they have your email address

**Manage who can discover your profile from your phone number** Change Nobody  
Choose who can discover your profile if they have your phone number

**Representing your organization** Change No  
Choose if we can show your profile information on your employer's pages

**Profile visibility off LinkedIn** Change No  
Choose how your profile appears via partners' and other permitted services

**Advertising preferences** Change No  
Choose whether LinkedIn can serve interest-based advertising through our platform for services

**Security**

**Two-step verification** Change On  
Activate this feature for enhanced account security

**Profile privacy**

**Edit your public profile** Change  
Choose how your profile appears to non-logged in members via search engines or permitted services

**Manage active status** Close  
Choose how your active status is displayed to your connections

**Display your active status**  
Show my connections when I'm active on LinkedIn or available on mobile

No ☐ \*Changes may take up to 30 minutes

**Hide active status from select people**  
Type connection name

\*When hiding your status from someone, you'll also lose the ability to see when they're online

**Who can see your connections** Change Only you  
Choose who can see your list of connections

**Viewers of this profile also viewed** Change No  
Choose whether or not this feature appears when people view your profile

**Sharing profile edits** Change No  
Choose whether your network is notified about profile changes

**Profile viewing options** Change Private mode  
Choose whether you're visible or viewing in private mode

**Notifying connections when you're in the news** Change No  
Choose whether we notify people in your network that you've been mentioned in an article or blog post

**Who can see your last name** Change Abbreviated  
Choose how you want your name to appear

**Regula nr. 27:** Dezactivați anunțurile personalizate.

**Regula nr. 28:** Când utilizați Facebook pe telefonul dvs., limitați sau dezactivați accesul aplicației la locația dvs.

**Regula nr. 29:** Fotografiile realizate pe un smartphone conțin o mulțime de date sensibile despre ora și locația în care au fost făcute. Dacă este posibil, nu le distribuiți direct pe rețelele de socializare sau dezactivați localizarea pentru fotografii. În plus, reduceți dimensiunea fotografiei și editați-o (aceasta va corupe metadatele fotografiei). iVerify, de asemenea poate șterge metadatele pentru dvs. În caz contrar, riscați să expuneți informațiile despre software și sistemul dvs. operațional.

**Regula nr. 30:** Nu vă conectați la Facebook prin alte pagini web – o astfel de autentificare întotdeauna distribuie datele dumneavoastră.

**Regula nr. 31:** Nu adăugați oameni pe care nu îi cunoașteți ca prieteni. Dacă nu ați fost strict în această chestiune în trecut, parcurgeți-vă prietenii actuali și ștergeți din lista de prieteni pe cei pe care nu îi cunoașteți de fapt. Acest lucru nu se aplică celor care au un profil public în mod deliberat.

**Regula nr. 32:** LinkedIn este adesea folosit pentru colectarea datelor personale. Dacă trebuie să utilizați această rețea, plasați acolo doar informații cunoscute public. Verificați ce informații ați plasat deja pe LinkedIn. Căutați cu atenție orice legătură care duce la familia dvs. sau prietenii apropiați (altă decât cunoscută public), deoarece există riscul de „apropriere” (cine va lua legătura și cum va fi utilizat pentru a vă câștiga încrederea).

a. Securizarea informațiilor sensibile despre dvs. și persoanele apropiate

**Regula nr. 33:** Decideți ce informații doriți să protejați. Elementele esențiale sunt adresa dvs. de acasă, informațiile despre rudele dvs. și afacerile personale care ar putea fi abuzate de un oponent (de exemplu, că aveți o criză în relație). Împărțiți informațiile în trei grupuri:

- publice (pot fi găsite online și le postați pe rețelele de socializare)
- private (de exemplu. adresa dvs. de acasă sau identitatea partenerului dvs., care este cunoscută doar prietenilor)
- sensibile (accesibile numai pentru un număr limitat de persoane în care aveți încredere deplină)

**Regula nr. 34:** Fiți conștienți că orice veți posta pe rețele de socializare va deveni o informație practic imposibil de șters și care s-ar putea dovedi utilă oponentului dvs. după mai mulți ani de la publicarea acesteia. Prin urmare, nu postați fotografii ale casei dvs., copiilor dvs. și ale prietenilor apropiați sau rudelor. Vă recomandăm să parcurgeți toate fotografiile dvs. pe Facebook, Twitter sau Instagram și să le ștergeți pe acelea care dezvăluie identitatea locurilor sau a persoanelor pe care doriți să le protejați.

**Regula nr. 35:** Dedicăți câteva ore pentru a selecta informațiile despre dvs. pe care le considerați private sau sensibile și căutați-le cu ajutorul Google pentru a vedea dacă nu au apărut undeva. Procedând astfel, veți afla ce informații despre dvs. sunt accesibile publicului prin surse deschise. Parcurgeți profilul prietenilor apropiați sau a rudelor și cereți-le să șteargă fotografiile deja postate cu dvs. și să nu mai posteze în viitor. Dacă doriți să vă protejați rudele, nu puteți să-i aveți în lista de prieteni (numele de familie identic îi face ușor de găsit), ceea ce solicită o serie suplimentară de pași pentru protecția retrospectivă a identității lor – autorii acestui manual vă vor oferi cu bucurie un alt set de măsuri mai sensibile.

**Regula nr. 36:** Adresa dvs. permanentă este parțial informație publică, care este disponibilă în bazele de date ale statului sau în contractele comerciale. În cazul

în care nu doriți ca reședința dvs. să poată fi găsită ușor, schimbați adresa dvs. permanentă, de exemplu, la casa părinților sau a altor rude. Este posibil să vă stabiliți adresa permanentă comercial prin intermediul organizației.

**Regula nr. 37:** Setați o notificare în Google Alerts, care vă va trimite un e-mail dacă numele dvs. (sau combinația de nume, titlul postului sau angajatul dvs.) apare pe oricare site web. Faceți acest lucru pentru diferite combinații de nume, poziție sau angajator. Rezultatele nu vor include rețelele de socializare.

#### b. Anonimatul pe Internet

Toată activitatea dvs. pe Internet transmite un anumit nivel de informații despre identitatea dvs. Aceste informații pot fi analizate, comparate și utilizate pentru crearea profilului dvs. care poate descoperi o mulțime de informații sensibile despre comportamentul dvs. online. Chiar dacă nu există așa ceva ca anonimat complet pe Internet, vă sfătuim să încercați cel puțin să minimalizați volumul de informații pe care le împărtășiți despre dvs., mai ales dacă desfășurați activități sensibile. Ceea ce poate părea banal astăzi în cinci sau zece ani poate fi folosit pentru analiza psihologică a profilului dvs.:

**Regula nr. 38:** Utilizați DuckDuckGo (<http://duckduckgo.com>) ca motor principal de căutare. Acest motor utilizează conexiunea codificată și nu stochează nici adrese IP, nici istoricul căutării. Ștergeți conectarea automată în toate celelalte browsere. Cookie: în browserele utilizate în mod obișnuit (Chrome, Firefox, Internet Explorer, Safari) puteți utiliza ferestre private/anonime care nu salvează cookie. Cu toate acestea, adresa dvs. IP se identifică, iar furnizorul dvs. de Internet vă poate urmări activitatea online.

**Regula nr. 39:** Un serviciu bun pentru distribuirea anonimă și confidențială a documentelor este Crabgrass (<https://we.riseup.net/crabgrass>), unde puteți să vă înregistrați anonim și să îl folosiți pentru distribuirea documentelor în echipa dvs.

**Regula nr. 40:** Pentru a vă acoperi identitatea online, vă recomandăm să utilizați o versiune plătită a VPN. Recomandarea noastră ar fi VPNSecure.me, Proton VPN sau Avast și nu numai pe laptop, ci și pe telefon sau tabletă. Dacă vă conectați vreodată la o rețea Wi-Fi nesecurizată, este foarte ușor de urmărit cu precizie acțiunile dvs. Niciodată nu faceți nimic sensibil pe o rețea Wi-Fi nesecurizată. Niciodată nu actualizați software-ul de pe o rețea Wi-Fi nesecurizată. Schimbați parola Wi-Fi de acasă la fiecare 3 luni. Vă recomandăm să folosiți „comutatorul de ucidere” VPN, care vă deconectează imediat de la internet în cazul unei conexiuni slabe, asigurându-vă că sunteți acoperit în permanență de VPN.

**Regula nr. 41:** Există o singură modalitate de a atinge un nivel ridicat de anonimat pe Internet și aceasta este folosirea Tor, un browser web special. Nu vă recomandăm să-l utilizați în mod obișnuit – este destul de lent, pe lângă alte lucruri - ci doar atunci când doriți să vă asigurați că unele activități online nu vor fi asociate cu dvs. (acest lucru nu implică doar activități ilegale; s-ar putea să doriți să vă protejați din cauza afirmațiilor sensibile din punct de vedere politic, comunicării cu unele persoane care nu doriți să devină publică, etc.). Dacă utilizați Tor, nu instalați plug-in-uri sau descărcați torrenturi în același timp. De asemenea, se recomandă să nu deschideți documente prin Tor (chiar fișiere .doc și .pdf). Dacă trebuie să lucrați cu documente, deconectați-vă temporar computerul de la Internet.



## Securitatea comunicării

### a. Codificarea comunicării

Dacă scrieți informații sensibile de mână într-un carnet, vă recomandăm să le distrugeți în fiecare zi (rupeți în bucăți mici și aruncați în toaletă). Acest lucru va asigura faptul că nu veți uita undeva carnetul cu notițe de mai multe zile, ceea ce va vulnerabiliza informația.

Cele mai puțin sigure căi de comunicare sunt:

- Apeluri telefonice, mesaje text: furnizorii țin evidența apelurilor telefonice și a mesajelor text și sunt adesea capabili să le furnizeze unor persoane terțe (în anumite condiții). Nu este dificil de monitorizat apelurile și mesajele text, utilizând tehnologia comercială disponibilă.
- E-mail-urile sunt stocate pe serverele furnizorului dvs. ceea ce le face accesibile oricui care știe parola contului dvs. de e-mail sau chiar a furnizorului însuși. Același lucru este valabil și pentru Facebook și Twitter. E-mailul necodificat este ca și cum ai trimite o carte poștală prin poștă – oricine dorește poate să o citească.

**Regula nr. 41:** Cea mai sigură aplicație civilă codificată pentru mesaje este Signal, prin intermediul căreia puteți și apela (fără apeluri de grup). Dacă utilizați Signal, este important să aveți totul activat în setările de confidențialitate – inclusiv setarea unei fraze de acces și ștergerea regulată a mesajelor (noi recomandăm intervalul de o zi). Nu recomandăm utilizarea WhatsApp sau Skype pentru informații sensibile. Pentru date semnificativ sensibile, vă recomandăm Wickr Me. Nu folosiți Viber sau Telegram. Când efectuați apeluri printr-o aplicație criptată, luați în considerare împrejurimile dvs. Nu vorbiți niciodată despre informații sensibile în transportul public, într-un automobil cu un străin sau într-o încăpere cu alte persoane. Cel mai bine este să vă plimbați afară.

**Regula nr. 42:** Cea mai sigură aplicație pentru e-mail-uri criptate este ProtonMail, cu condiția să fie utilizată de ambele părți. ProtonMail este disponibilă pentru iOS, Android și pe Internet. Se recomandă să descărcați Proton Bridge în versiune plătită, deoarece vă permite să instalați Proton Mail pentru client de e-mail în computerul dvs. Nu uitați să setați autentificarea cu doi factori. Ștergeți ProtonMail la fiecare 3 luni, ștergând toate e-mail-urile primite și trimise. Deoarece avem nevoie de un e-mail de rezervă secundar pentru ProtonMail, vă recomandăm să setați un ProtonMail separat (poate fi neplătit) cu o parolă super puternică (40 de caractere), care va fi folosită ca e-mail de rezervă pentru toate celelalte profiluri dvs. – Facebook, Twitter, LinkedIn, Instagram, conturi bancare.

## Securitatea datelor

Fiecare folder distribuit (de exemplu, pe Dropbox) este la fel de securizat ca și cel mai puțin securizat membru al echipei.

Setări recomandate pentru iPhone:

- Configurări>Notificări>parcurgeți fiecare aplicație și asigurați-vă că notificările nu pot fi accesate când ecranul este blocat
- Configurări>intimitate>servicii de localizare>
  - >distribuie locația mea – deconectați
  - Accesați fiecare aplicație și determinați dacă aveți nevoie de GPS pentru „în timp ce utilizați” sau „niciodată”. Asigurați-vă că nimic nu este

- bifat pe „întotdeauna”
- Asigurați-vă că funcția „niciodată” este selectat pentru: camera foto (sau toate fotografiile dvs. sunt imprimate cu locul în care au fost făcute); toate aplicațiile de socializare (adică twitter, Facebook, Instagram)
- >servicii de sistem – toate dezactivate cu excepția ‘SOS urgențe’ și (opțional) ‘Găsiți iPhone-ul meu’
- >locații frecvente – ‘șterge istoricul’ și schimbați pe ‘dezactivat’
- Îmbunătățirea produsului – toate ‘dezactivat’
- Configurări>intimitate>
  - Diagnosticare și utilizare – ‘nu trimite’
  - Publicitate – „Resetați identificatorul publicitar” și „Limitare urmărire publicitară” – activat

#### a. Criptarea discului

**Regula nr. 43:** Criptați discul dvs.:

- macOS: conține un program de criptare a discului numit FileVault – după ce îl porniți, va genera o cheie de recuperare (care poate fi stocată în siguranță pe serverele Apple) și apoi va cripta întregul disc. Decriptarea ulterioară este un proces de fundal, neobservabil pentru utilizator și nu încetinește sistemul.
- Windows: funcția de criptare BitLocker este inclusă numai în edițiile profesionale ale Windows. Aplicațiile precum VeraCrypt sau CipherShed reprezintă o alternativă bună pentru proprietarii edițiilor fără BitLocker.
- Telefoanele mobile și tabletele cu Android 5.0 (Lollipop) și mai noi de obicei acceptă criptarea, însă, în multe cazuri, scade performanța dispozitivului și, prin urmare, scade confortul utilizatorului. Prin urmare, vă recomandăm să păstrați criptarea dezactivată în astfel de cazuri, cu condiția ca utilizatorul să respecte următoarele sfaturi.

#### b. Criptarea și ștergerea securizată a datelor stocate pe discurile portabile

**Regula nr. 44:** Unități flash USB: pe Mac, este suficient să faceți clic dreapta pe pictograma discului din Finder și să alegeți opțiunea Cripează. Dacă apoi îl introduceți într-un alt computer, trebuie doar să introduceți parola. Dacă aveți o versiune de Windows cu BitLocker, puteți cripta discul fie în secțiunea BitLocker din Panoul de control, fie simplu făcând clic dreapta pe pictograma discului portabil. Dacă versiunea dvs. de Windows nu conține BitLocker, puteți utiliza aplicația VeraCrypt menționată mai sus, care are aceeași funcție. Nu încărcați niciodată o unitate flash USB necunoscută pe dispozitiv, chiar dacă este a prietenului dvs. – nu știți dacă el/ea are grijă de siguranța sa. Instalați programul USB Safeguard, care va deschide doar unități flash verificate. Pentru fișiere necunoscute, utilizați aplicația Sandbox.

**Regula nr. 45:** Pur și simplu ștergerea datelor de pe un disc nu le face inaccesibile – de aceea este necesar să efectuați o ștergere sigură, care poate dura mai mult timp, dar veți putea să transmiteți discul oricui:

- MacOS: puteți utiliza aplicația de sistem Utilitar disc (secțiunea Ștergere disc conține un buton pentru ștergere securizată). Folosiți aplicația Eraser.

- Windows: în prezent, Windows nu acceptă ștergerea securizată în configurația sa de bază. Cu toate acestea, chiar și versiunea gratuită a CCleaner, de exemplu, este în măsură să șteargă în siguranță datele de pe discurile portabile.

### Securitatea personală

**Regula nr. 46:** Nu plasați numele dvs. pe soneria ușii de la intrare în clădire. Dacă trebuie să fie acolo, atunci nu-l plasați pe ușa apartamentului dvs.

**Regula nr. 47:** Dacă sunteți departe de casă pentru o perioadă mai lungă de timp, nu anunțați public acest lucru și asigurați-vă că postările dvs. pe rețelele de socializare nu vă afișează locația. Alternativ, postați fotografiile din călătorie numai după întoarcerea acasă. Dacă comandați taxi sau Uber, se recomandă să nu o faceți exact în locația șederii dvs., ci la cel puțin 50 de metri distanță, și similar când părăsiți vehiculele. Datele despre locație sunt stocate în profilul dvs. și pot fi obținute relativ ușor.

**Regula nr. 48:** Stabiliți o parolă cu persoanele apropiate ca ei să vă poată trimite un text sau să vă sune atunci când se simt în pericol, iar dvs. veți apela imediat la poliție și veți merge în căutarea lor – asigurați-vă că vă vor spune și locația lor. Faceți la fel pentru familia dvs. Dacă nu puteți efectua un apel telefonic, puteți trimite un semnal de urgență.

**Regula nr. 49:** Nu intrați niciodată într-un spațiu închis singur cu o persoană necunoscută. În schimb, încetiniți, imitați un apel telefonic sau întoarceți-vă și mergeți în altă direcție. Dacă nu vă simțiți confortabil undeva, scoateți imediat telefonul și imitați un apel telefonic unei persoane apropiate, spuneți cu voce tare unde vă aflați și, de exemplu, că există o persoană ciudată, a cărei înfățișare o descrieți cu voce tare. Asta funcționează aproape întotdeauna ca factor de descurajare de succes. În mod alternativ, începeți să strigați, tare și fără ezitare. O alarmă falsă nu te costă nimic, ceea ce nu se poate spune despre opțiunea de alternativă.

**Regula nr. 50:** Pentru a putea recunoaște aproximativ cât de urgentă este o anumită amenințare, memorizați tabelul de mai jos. Regula de bază în caz de incident fizic este: fugi, ascunde-te, luptă.

## 8. CONSTATĂRI CHEIE

- Lipsa de manuale de securitate cibernetică în cadrul OSC.
- Lipsa securității operaționale de rutină/lipsa dorinței de a urma rutina.
- Lipsa resurselor umane respective (specialiști) în cadrul OSC.
- Securitatea operațională este prea tare subestimată.
- Greșelile obișnuite privind securitatea operațională, săvârșite de oficiali guvernamentali, jurnaliști și OSC, îi determină să devină ținte ușoare:
  - “Eu nu sunt atât de important.”
  - “Eu nu fac nimic ilegal.”
  - “Acest lucru nu este secret.”
- Lucrul în domeniul combaterii influenței rusești și a celei chineze te face o țintă.
- Rusia și China cu ușurință pot supraveghea mii de persoane care lucrează în acest domeniu.

## 9. REZUMAT

### Cele zece obiceiuri de securitate pe care toată lumea ar trebui să le urmeze

Regulile pe care vă recomandăm să le urmați sunt enumerate mai sus. Adesea, acești pași trebuie aplicați doar o singură dată. Dincolo de această ajustare inițială a comportamentului dvs. legat de securitate, vă recomandăm să adoptați aceste obiceiuri zilnice și să le urmați în același fel în care vă spălați în mod regulat pe dinți sau vă blocați ușa:

**Obiceiul nr. 1:** Pentru o comunicare sigură, utilizați numai aplicația Signal (pentru a trimite mesaje și pentru a suna) și ProtonMail pentru e-mail-uri criptate. Nu aveți încredere în aplicații precum WhatsApp, Facebook Messenger sau Telegram pentru conversații mai sensibile (Regulile nr. 41 - 42).

**Obiceiul nr. 2:** Ștergeți periodic datele de pe computer folosind programele Permanent Eraser sau Cleaner (Regula nr. 45).

**Obiceiul nr. 3:** Majoritatea atacurilor cibernetice vin prin phishing. Prin urmare, toate atașamentele de e-mail deschideți în Sandbox și toate linkurile primite verificați prin virustotal.com (Regula nr. 10).

**Obiceiul nr. 4:** Nu aveți încredere în nici-o unitate USB, deoarece nu este posibil să le verificați securitatea. Este mai bine ca datele să fie trimise la ProtonMail dacă este posibil. În mod alternativ, păstrați un computer separat fără conexiune la Internet unde puteți deschide unitatea USB (Regula nr. 44).

**Obiceiul nr. 5:** Stocați telefoanele mobile în siguranță în timpul întâlnirilor sensibile. În mod ideal, dispozitivele electronice ar trebui să fie plasate într-o pungă la aproximativ 7-10 metri distanță, astfel încât să fie la vedere, dar fără riscul ca dispozitivele „să audă” conversația dvs (Regula nr. 17).

**Obiceiul nr. 6:** Este recomandabil să nu utilizați dispozitive conectate fără fir (căști, imprimante). Cumpărați „prezervative USB” pentru încărcătoarele de telefon și computer (Regula nr. 16).

**Obiceiul nr. 7:** Când adăugați informații și fotografii în conturile dvs. din rețelele de socializare, adăugați doar cele pe care le-ați permite oponentilor să le vadă. Dacă postați ceva despre familie și rude sau despre viața personală, oponentii pot crea un profil psihologic și o hartă socială și pot exploata aceste informații (Regula nr. 33).

**Obiceiul nr. 8:** Utilizați întotdeauna VPN: VPN Secure Me, Proton VPN sau Avast. Urmați regula „comutatorului de ucidere” (Regula nr. 40).

**Obiceiul nr. 9:** Dacă scrieți note sensibile de mână, vă recomandăm să le prelucrați în timpul zilei, apoi să le nimiciți (sau să le rupeți în bucăți mici și să le aruncați într-un coș departe de casa sau biroul dvs.).

**Obiceiul nr. 10:** SETAȚI-VĂ UN MEMENTO ÎN CALENDAR: Schimbăm parolele la fiecare trei luni. (Regula nr. 1 - 4). Vă recomandăm să faceți în fiecare lună o copie de rezervă a documentelor personale, a conținutului calendarului electronic și a propriilor fișiere de lucru pe o unitate externă criptată (Regula nr. 19).





**UN E-MAIL CARE NU ESTE CRIPTAT ESTE ECHIVALENT CU POSTAREA MESAJELOR DVS. CĂTRE PUBLIC ÎN TIMP REAL**

**FACEȚI SĂ-I FIE MAI DIFICIL Oponentului**

- 1) Folosiți un VPN bun (Avast Secureline, Proton VPN, NordVPN,...).
- 2) Folosiți un software bun antivirus și anti-ransom (Avast, Eset, McAfee...).
- 3) Criptați datele dvs. (VeraCrypt).

**NU PUNEȚI TOATE OUĂLE ÎNTR-UN SINGUR COȘ**

- 1) Securizați toate conturile și profilurile dvs. cu autentificare pe două niveluri.
- 2) Creați mai multe e-mail-uri bine protejate pentru conturile dvs., astfel încât dacă unul este spart, nu se va lua totul.
- 3) Folosiți parole puternice, nu folosiți aceeași parolă pentru toate conturile dvs.

**ÎNTOOTDEAUNA VERIFICAȚI DE DOUĂ ORI PERSOANELE NOI CU CARE VĂ ÎNTÂLNIȚI**

- 1) Întotdeauna documentați (prin Google) istoria lor și solicitați referințe scurte de la persoane care îi cunosc.
- 2) Nu lăsați să intre străinii în oficiile dvs.

**CUNOAȘTEȚI CE INFORMAȚII DE IDENTITATE PROTEJAȚI**

Profilul dvs. pe Facebook este plin cu informații despre partenerul și copiii dvs.?

Înțelegeți că informațiile publice sunt ușor disponibile oponentilor și pot fi utilizate împotriva dvs.