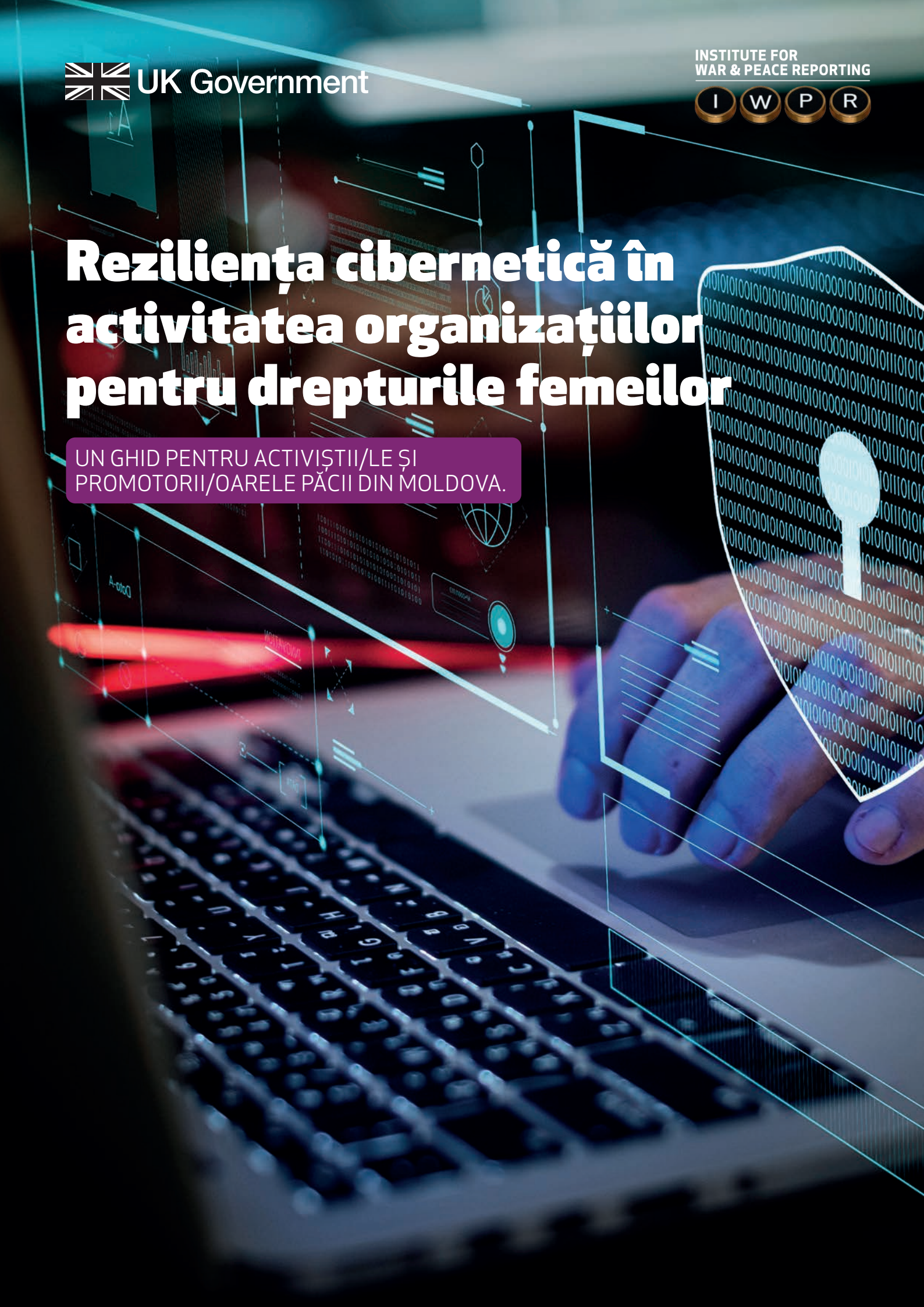
UK Government

INSTITUTE FOR WAR & PEACE REPORTING

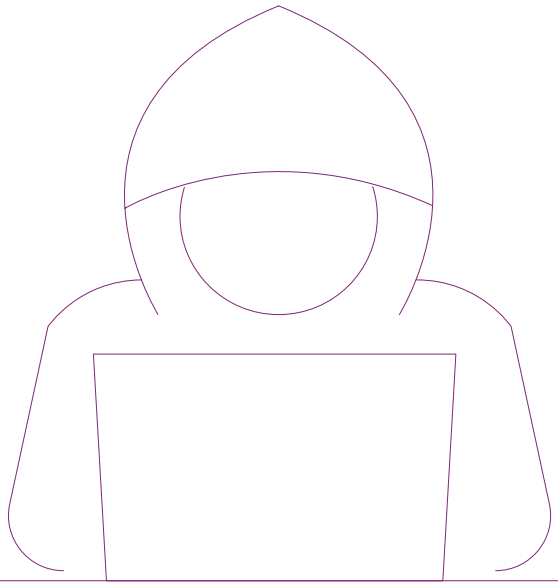
IWPR

Reziliența cibernetică în activitatea organizațiilor pentru drepturile femeilor

UN GHID PENTRU ACTIVIȘTII/LE ȘI PROMOTORII/OARELE PĂCII DIN MOLDOVA.



CUPRINS



INRODUCERE	3
PEISAJUL SECURITĂȚII CIBERNETICE DIN MOLDOVA: O ANALIZĂ DE GEN	4
SUNT CU ADEVĂRAT O ȚINTĂ?	6
NAVIGAREA ÎN SIGURANȚĂ PE INTERNET: AI MERGE PE O STRADĂ AGLOMERATĂ CU GEANTA DESCHISĂ?	11
WIFI-UL PUBLIC: O COMOARĂ PENTRU HACKERI	15
CE AU ÎN COMUN CHEILE DE LA CASĂ ȘI PAROLELE?	18
MALWARE: UN VIRUS CARE SLĂBEȘTE SISTEMUL IMUNITAR AL COMPUTERULUI	21
PROTEJEAZĂ-ȚI DISPOZITIVELE, ORGANIZAȚIA ȘI BENEFICIARII	24
CÂTEVA CUVINTE DE FINAL	27
RĂSPUNSURILE TALE CIBERNETICE	28
RESURSE	29

Scris de: **Jennifer Kanaan**
Editat de: **Daniella Peled**
Tradus în limba română de: **Svetlana Morarenco**
Proiectat de : **Humble Bee Design**
Modelele adaptate în limba română de:
Ecaterina Șalaru

Reziliența cibernetică pentru organizațiile pentru drepturile femeilor

UN GHID PENTRU ACTIVIȘTII/LE ȘI PROMOTORII/OARELE PĂCII DIN MOLDOVA.

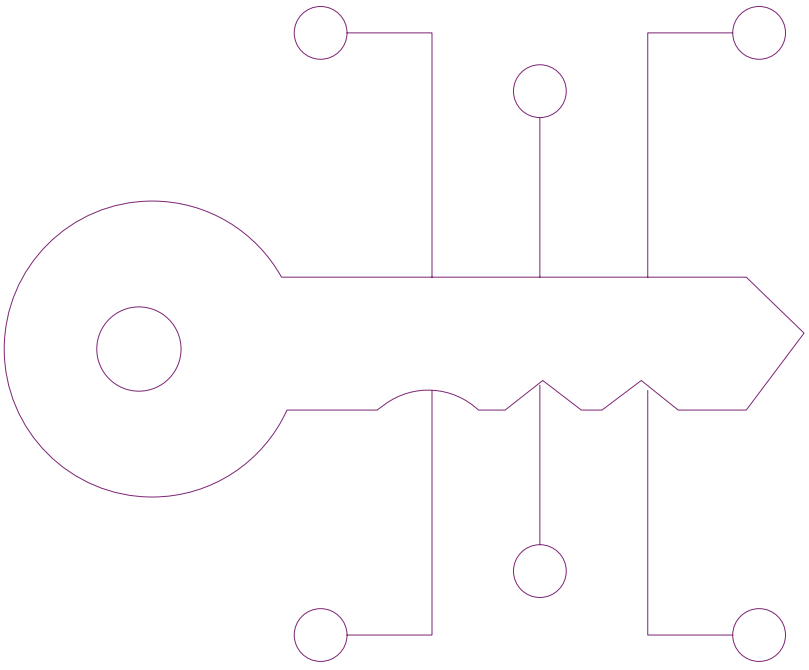
Această publicație a fost elaborată în cadrul proiectului "Consolidarea rezilienței în vecinătatea estică" (BREN), implementat cu sprijinul Biroului pentru afaceri externe, comunitate și dezvoltare al Regatului Unit (FCDO). Opiniile, constatările și concluziile prezentate în acest document aparțin autorilor și nu reflectă în mod necesar pe cele ale Guvernului Britanic.

Desfășurat în parteneriat cu Rețeaua globală a femeilor care promovează pacea (GNWP), BREN este conceput pentru a consolida capacitatea de rezistență a organizațiilor societății civile și pentru a promova securitatea umană, pacea și stabilitatea în Caucazul de Sud și în Moldova, în special pentru femei și comunități marginalizate.

Institute for War & Peace Reporting (IWPR) oferă posibilitatea ca vocile locale să impulsioneze schimbarea în țările aflate în conflict, criză și tranziție. Acolo unde discursul instigator la ură și propaganda se intensifică, iar jurnaliștii și activiștii civici sunt atacați, IWPR promovează informații fiabile și dezbateri publice care fac diferența.

Informațiile furnizate în acest ghid nu constituie și nu sunt menite să constituie o consiliere în materie de securitate cibernetică; în schimb, acestea sunt destinate exclusiv unor scopuri informative generale.

Este esențial ca organizațiile să angajeze un consilier, un consultant în domeniul securității cibernetice sau, cel puțin, un expert IT care să le sprijine în consolidarea mediului cibernetic. Acești experți pot oferi asistență, îndrumare și răspunsuri rapide în cazul unui atac cibernetic sau al altor probleme.



INSTITUTE FOR WAR & PEACE REPORTING

IWPR

Biografie Jennifer Kanaan:
Jennifer Kanaan este manageră regională de comunicare pentru programul "Consolidarea capacității de reziliență în Vecinătatea din Est" (BREN) din cadrul Institute for War & Peace Reporting (IWPR). Expertă în comunicare digitală și advocacy, Jennifer lucrează la IWPR din 2016, contribuind la diverse proiecte. Printre acestea se numără proiectul de pionierat "Cyber Arabs", un site web cuprinzător de resurse de securitate cibernetică în limba arabă al IWPR și un manual digital de advocacy pentru Etihad, un proiect care sprijină organizațiile LGBTQI din regiunea MENA.

Biografie Daniella Peled:
Daniella Peled este redactor-șef al IWPR, supervizând tot conținutul și producția editorială. Jurnalistă și editor cu peste 20 de ani de experiență în domeniul relațiilor externe, a conceput și implementat cursuri de formare în jurnalism în multe dintre zonele de activitate ale IWPR, inclusiv în Afganistan, Irak și Turcia.

Mulțumiri: Toro & Gnwp
Experți în domeniul cibernetic: Samvel Martirosyan, Artur Papyan, Davit Ghonghadze și Vlad Mazureac

gnwp Global Network of Women Peacebuilders

Peisajul securității cibernetice din Republica Moldova: o analiză de gen

Republica Moldova, o fostă republică sovietică din Europa de Est, se confruntă cu un peisaj politic modelat de sentimente divergente pro-europene și pro-ruse. Această dezbinare ideologică influențează în mod semnificativ guvernarea și formularea politicilor.

Populația este împărțită între cei care pledează pentru legături mai strânse cu Europa și cei care favorizează alinierea cu Rusia(1). Având rădăcini istorice, culturale și geopolitice, această dezbinare creează o polarizare politică. În 2023, 31,6 la sută dintre moldoveni nu susțineau integrarea europeană, iar 52 la sută aveau cunoștințe limitate despre UE, ceea ce arată profunzimea acestei divergențe(2).

Aceste sentimente opuse reprezintă o provocare în formarea unor guverne stabile. Partidele politice adesea se aliniază pe linii pro-europene sau pro-ruse, ceea ce împiedică consensul și duce la schimbări frecvente în dinamica politică(3).

Războiul intensificat al Rusiei împotriva Ucrainei a îndemnat Moldova să solicite aderarea la UE. Această decizie reflectă o reevaluare mai amplă a strategiilor politice și de securitate, punând accentul pe legături mai strânse cu UE(4).

Războiul din Ucraina a provocat un șoc economic major în Moldova. Dependența economică de Rusia, împreună cu întreruperea exporturilor, a contribuit la acest declin. Dependența Moldovei de importurile de gaze rusești a stârnit îngrijorări pe fondul conflictului, având un impact asupra tranzitului de gaze prin Ucraina. În plus, impactul global asupra prețurilor la alimente și energie a exacerbat provocările existente ale Moldovei în materie de inflație(5).

Aceste vulnerabilități, combinate cu proximitatea geografică față de părțile beligerante, amplifică impactul asupra economiei Moldovei(6).

Războiul a dus, de asemenea, la strămutări substanțiale, creând o situație umanitară complexă. Atenția acordată nevoilor celor afectați de conflict este crucială în interiorul granițelor Moldovei și în regiunile învecinate.(7, 8).

Peisajul securității cibernetice

Recunoscând provocările reprezentate de instabilitatea regională, Republica Moldova și-a consolidat pro-activ rezistența cibernetică, dezvăluind două instituții esențiale în februarie 2024.

Agenția Națională pentru Securitate Cibernetică: Această agenție, aliniată la cele mai bune practici europene, acordă prioritate infrastructurilor critice și sectoarelor publice. Dincolo de protejarea acestor domenii, agenția se angajează să sporească gradul de conștientizare și educație a cetățenilor în domeniul securității cibernetice(9).

Institutul Național de Inovații în Securitate Cibernetică (Cybercor): Acest institut este un centru de cultivare a viitoarelor talente în domeniul securității cibernetice prin programe educaționale de ultimă generație. Acesta joacă un rol esențial în dotarea studenților și a funcționarilor publici cu competențe esențiale pentru a naviga în peisajul cibernetic în continuă evoluție(10).

Mai mult decât atât, UE sprijină în mod activ îmbunătățirea pregătirii Republicii Moldova în domeniul securității cibernetice. Prin intermediul unei formări adaptate, UE sprijină funcționarii guvernamentali și furnizorii de servicii esențiale, consolidând apărarea digitală a statului (11).

Republica Moldova se confruntă cu o creștere a amenințărilor cibernetice(12), care se manifestă sub diverse forme:

-Atacuri cibernetice asupra entităților guvernamentale: Incidentele s-au triplat în 2022, vizând sistemele guvernului, reprezentând o provocare semnificativă pentru securitatea națională(13).

-Atac DDoS: Originând în Rusia, atacul din septembrie 2023 a afectat aeroportul din Chișinău, Agenția Națională de Reglementare în Energetică și Ministerul Afacerilor Externe și Integrării Europene (MAEIE) (14).

-Atacurile cibernetice rusești: Exacerbate de tensiunile regionale, cum ar fi războiul din Ucraina, aceste atacuri se concentrează cu precădere asupra Serviciului de Tehnologie a Informației și Securitate Cibernetică din Moldova(15).

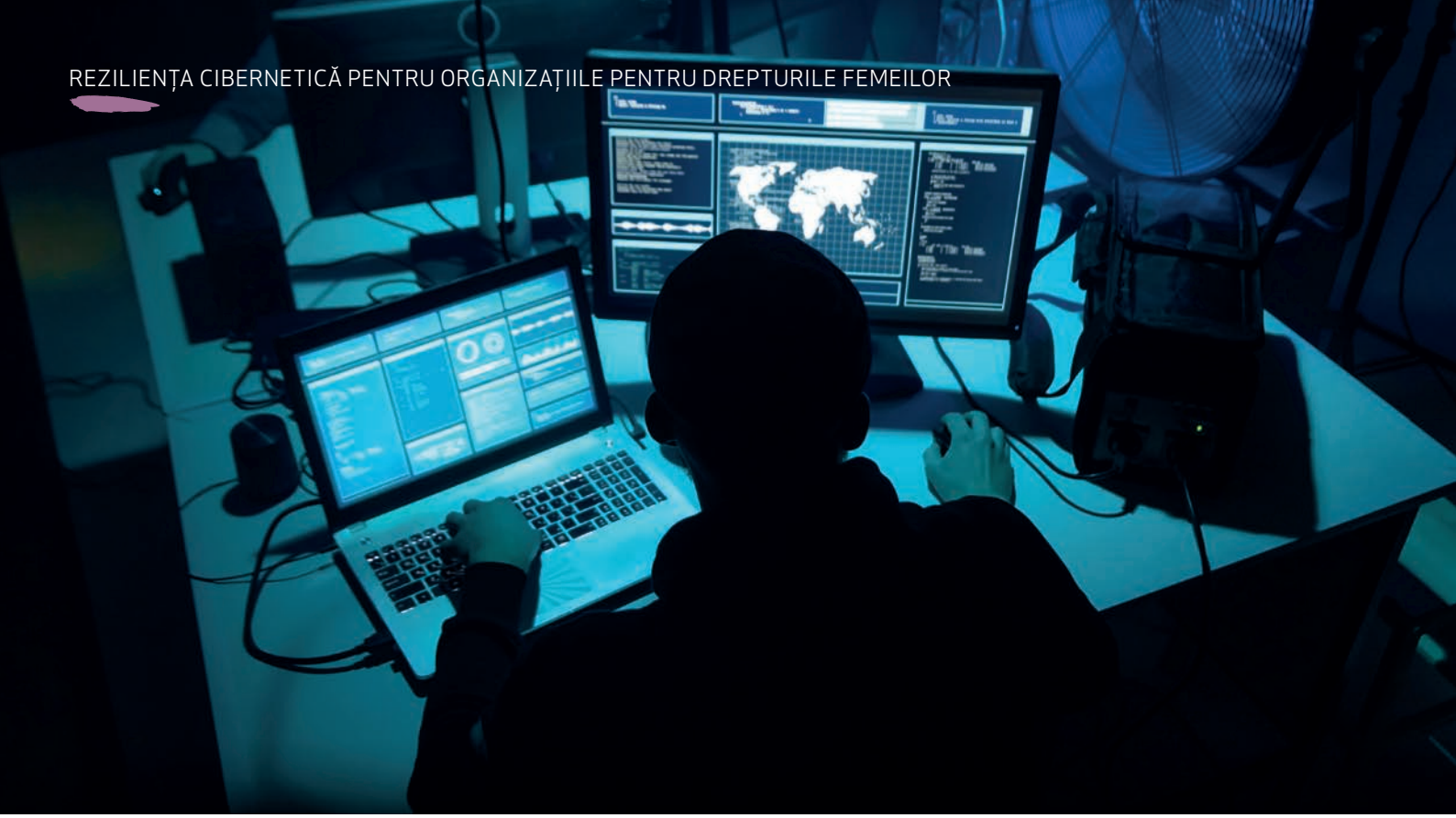
-Exploatarea e-mailurilor: Hackerii au exploatat o vulnerabilitate a produsului de e-mail Zimbra pentru a viza instituțiile guvernului în vara anului 2023, subliniind vulnerabilitatea sistemelor de comunicare(16).

-Amenințări cibernetice de ordin general: Moldova își consolidează în mod activ apărarea digitală împotriva unei game diverse de amenințări cibernetice, obținând sprijin internațional pentru îmbunătățiri securității cibernetice naționale (17, 18).

Societatea civilă și amenințările cibernetice

Societatea civilă din Moldova se confruntă cu aceleași amenințări ca și ceilalți utilizatori de internet din țară. Cu toate acestea, natura activității lor amplifică aceste riscuri, ceea ce duce la repercusiuni potențial mai mari pentru organizații și pentru beneficiarii acestora. Cercetarea Justice for Journalists (JIJ) a documentat 56 de atacuri asupra lucrătorilor din mass-media în 2022, incluzând atât amenințări fizice, cât și cibernetice (19). Din 2017, aceste atacuri au fost în mod constant principala metodă de presiune asupra profesioniștilor din mass-media din Moldova, afectând în mod semnificativ libertatea de exprimare și activismul civic.

Evoluțiile recente evidențiază diverse amenințări cibernetice cu care se confruntă societatea civilă din Moldova:



-Hacking și perturbare cu țintă precisă: Actorii societății civile sunt vulnerabili la spargerea, distrugerea, întreruperea sau confiscarea intenționată a dispozitivelor, conturilor online, datelor sau serviciilor. Aceste amenințări vizează în mod special subminarea activităților și a vocilor persoanelor și organizațiilor dedicate cauzelor sociale (20).

-Sprijinul Forului de coordonare a refugiaților: Forul de Coordonare a Refugiaților sprijină în mod activ organizațiile locale din Moldova, inclusiv actorii societății civile. Accentul pus pe oportunitățile de finanțare sugerează provocările financiare cu care se pot confrunta aceste entități, potențial legate de nevoile de securitate cibernetică (21).

-Peisajul global al amenințărilor cibernetice: Poziția proactivă a Republicii Moldova în ceea ce privește consolidarea apărării digitale rezultă din poziția sa geopolitică unică și peisajul global al amenințărilor cibernetice care escaladează. Actorii societății civile pot fi afectați în mod semnificativ de acest peisaj, ceea ce impune măsuri sporite de rezistență și securitate. (22).

Analiza de gen în amenințările cibernetice

Amenințările cibernetice sunt o problemă omniprezentă care afectează persoanele din întreaga lume. Din păcate, femeile sunt adesea cele mai afectate de aceste amenințări, confruntându-se cu provocări și vulnerabilități unice. În întreaga lume, violența cibernetică împotriva femeilor este o preocupare urgentă, cuprinzând forme precum hărțuirea cibernetică, pornografia din răzbunare și atacurile online violente(23 24, 25). Aceste atacuri adesea escaladează în amenințări grave, exemplificate de incidentele în care au fost vizate jurnaliste cu amenințate cu moartea în Bosnia și Herțegovina(26).

Un studiu din 2023 privind genul și drepturile omului în abordările la nivel național privind securitatea cibernetică, realizat de GNWP, subliniază importanța încorporării unei perspective de gen în elaborarea politicilor(27). Această abordare recunoaște faptul că femeile și organizațiile pentru drepturile femeilor se pot confrunta cu provocări unice care necesită analize și recomandări individualizate.

Potrivit raportului GNWP, beneficiile aplicării unei prisme de gen la securitatea cibernetică includ:

1 - Recunoașterea faptului că femeile și grupurile marginalizate utilizează internetul în mod diferit și sunt afectate în mod disproporționat de atacurile cibernetice. Nevoile lor specifice și reprezentarea lor în procesul de elaborare a politicilor de securitate cibernetică și de dezvoltare tehnologică sunt adesea ignorate.

2- Îmbunătățirea accesului femeilor și al altor grupuri marginalizate la prevederile privind securitatea cibernetică, abordând limitările în ceea ce privește răspunsul de urgență și remediile juridice din cauza structurilor societale discriminatorii preexistente.

3 - Abordarea punctelor oarbe din politica de securitate cibernetică prin încorporarea unei perspective de gen, punând accent pe o abordare centrată pe om și sensibilă la dimensiunea de gen.

Atacurile cibernetice au un impact distinct asupra femeilor din Moldova, contribuind la o serie de provocări. Violența cibernetică, așa cum a fost evidențiată într-un raport PNUD (28), dăunează femeilor prin limitarea drepturilor lor la libertatea de exprimare, știrbind din încredere și afectând stima de sine. Această formă de violență lipsește femeile și fetele de drepturi, amenințând drepturile lor fundamentale.

În plus, Moldova s-a confruntat cu amenințări cibernetice, inclusiv amenințări cu bombă și atacuri cibernetice, care au sporit temerile de destabilizare regională, după cum a raportat IWPR (29). Vulnerabilitățile unice cu care se confruntă femeile în situații de conflict sunt recunoscute de Agenda privind femeile, pacea și securitatea (30), care recunoaște impactul diferențiat și unic asupra femeilor în timpul conflictelor și amenințărilor la adresa păcii și securității internaționale.

În plus, prevalența violenței în familie în Moldova, care afectează un număr semnificativ de femei, adaugă un alt nivel la impactul diferențiat al amenințărilor cibernetice, după cum a raportat Just Access (31).

Intersecția dintre securitatea cibernetică și drepturile de gen necesită o atenție și o acțiune susținute pentru a crea un spațiu digital mai sigur pentru femei la nivel global. Cercetările și inițiativele de securitate cibernetică în curs de desfășurare axate pe gen sunt esențiale pentru a înțelege impactul specific asupra femeilor în contextul moldovenesc.

Sunt cu adevărat o țintă?

Cu siguranță ești. De fapt, toată lumea este.

Intenția aici nu este de a insufla panică sau frică. Cu toate acestea, este esențial să fim pragmatici și să obținem o înțelegere clară a amenințărilor cibernetice și a activităților infracționale. Aceste cunoștințe îți vor da posibilitatea de a trece peste aceste provocări și de a te proteja nu numai pe tine, ci și pe colegii, beneficiarii și munca ta.

Fie că ești din domeniul umanitar, activist/ă sau apărător/oare ale drepturilor femeilor din Moldova, este probabil că te concentrezi pe pledoarie pentru schimbare, pe lobby pentru perspective de gen în legislație și pe sensibilizarea comunităților tale.

Este posibil ca amenințările cibernetice să nu facă parte din considerațiile tale obișnuite și, cu siguranță, nu se poate aștepta de la tine să abordezi situațiile ca un infractor cibernetic. Cu toate acestea, la fel ca și în cazul integrării unei prisme de gen în politici și legi, este imperativ în lumea de astăzi să integrezi conștientizarea cibernetică în toate activitățile tale.

> Protejându-te pe tine, pe colegii și organizația ta, nu protejezi doar datele, ci asiguri impactul pozitiv pe care l-ai avut și vei continua să-l ai asupra societății.

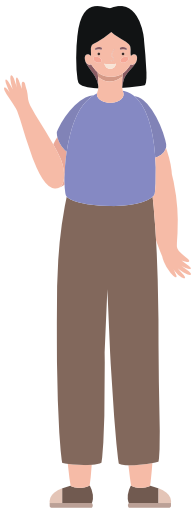
Hai să le cunoaștem pe Anastasia și pe Maria

Anastasia, o activistă pentru drepturilor femeilor, își dedică zilele pentru a îndemna la schimbări pozitive. Rutina ei include întâlniri cu organizațiile locale de femei, elaborarea de strategii pentru promovarea egalității de gen și îndrumarea tinerilor activiști/e. Își petrece multe seri în cadrul programelor de sensibilizare a comunității, unde împărtășește povești care inspiră femeile. Ziua Anastasiei este un amestec de advocacy, educație și discuții publice. .

Maria, o promotoare al păcii și o lideră dedicată al comunității, se concentrează asupra inițiativelor de la firul ierbii. Implicată activ în promovarea dialogului și a înțelegerii, Maria conduce adesea ateliere de lucru în comunitate și organizează evenimente de consolidare a păcii, promovând unitatea între diverse grupuri. Angajamentul ei se extinde, de asemenea, la discuțiidespre rezolvarea conflictelor, interacționând cu membrii comunității. Ziua ei obișnuită este plină de întâlniri, ateliere de lucru și eforturi de colaborare pentru a construi o societate pașnică și favorabilă incluziunii.

Anastasia:

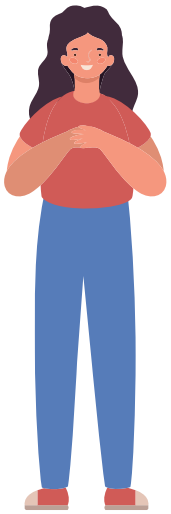
AVOCAT PENTRU DREPTURILE FEMEILOR



Istoricul activității profesionale: Anastasia este o activistă proeminentă în domeniul drepturilor femeilor din Moldova, dedicându-și cariera promovării egalității de gen și a justiției. Activitatea sa se concentrează pe emanciparea femeilor în regiunile post-conflict, contribuind astfel la o pace durabilă.
Stilul de viață: Anastasia este foarte implicată în inițiative de consolidare a comunității și în dialoguri de pace. Angajamentul său pentru incluziune și justiție socială a făcut din ea o figură respectată printre susținătorii drepturilor femeilor.

Maria:

PROMOTOARE A PĂCII ȘI LIDERĂ COMUNITARĂ



Istoricul activității profesionale: Maria este o pacificatoare dedicată, implicată activ în inițiative care abordează războiul, violența și inegalitățile sociale. Ea a co-fondat propria inițiativă de consolidare a păcii, promovând dialogul și înțelegerea.

Stilul de viață: Maria conduce ateliere de lucru în comunitate, subliniind importanța implicării femeilor în procesele de pace. Accentul pe care îl pune pe eforturile la nivel local exemplifică intersecția dintre consolidarea păcii și drepturile femeilor.

De ce să fie atacați/e cibernetic activiștii/ele, promotorii/oarele păcii și liderii/ele comunității?

Infractorii cibernetici vizează persoanele care ocupă aceste funcții datorită poziției lor influente în societate. Eforturile lor în direcția unei schimbări pozitive îi transformă în potențiale amenințări pentru cei cu interese opuse. În plus, natura muncii lor implică adesea informații sensibile, ceea ce îi face ținte atractive.

TIPURI DE ATACURI CIBERNETICE ÎN MOD SIMPLIFICAT:

Atac fără țintă:

-Cea mai frecventă formă de amenințare malițioasă.
-Nu vizează persoane sau organizații concrete. Infractorii cibernetici urmăresc să vizeze cât mai multe computere, persoane și organizații posibil.
-Programele malware, viermii sau virușii sunt trimiși la întâmplare prin e-mail la numeroase adrese.
-Atacurile cibernetice fără țintă sunt mai ușor de executat, dar sunt mai puțin distructive decât atacurile cu țintă precisă.

Atac țintit:

-Destinat unei anumite persoane sau organizații. Infractorii cibernetici acționează cu un scop specific, identificând o țintă de interes.
-Aceste atacuri durează luni de zile și pot implica inginerie socială, phishing, malware personalizat, campanii persistente și botnet-uri.
-Țintele s-au extins dincolo de organismele guvernamentale și bazele militare, incluzând organizații, mass-media, comunicații și infrastructuri critice.

Înțelegerea acestor concepte vă va permite să navigați eficient în mediul digital.

MOTIVAȚII DEZVĂLUITE: DE CE SĂ TE VIZEZE?

1. Influență și perturbare:
Rolul tău vital: În calitate de activist/ă, promotor/oare al păcii sau lider/ă comunitar/ă, misiunea ta este de a forma opinia publică și de a influența politicile publice.
Amenințarea cibernetică: Infractorii cibernetici pot pune ochii pe tine pentru a-ți perturba activitatea de impact. Prin faptul că te vizează, urmăresc să creeze haos, subminând inițiativele pozitive pe care le susții.
2. Obținerea de informații sensibile:

Manipularea datelor critice: În activitatea ta zilnică, adesea ai de-a face cu informații sensibile legate de probleme sociale.
Amenințarea cibernetică: Infractorii cibernetici ar putea încerca să fure sau să manipuleze aceste date în interes propriu. Fie că este vorba de profit personal sau de influențarea opiniei publice, informațiile tale valoroase devin o țintă.
Înțelegerea acestor motivații este primul pas pentru consolidarea rezilienței cibernetice.

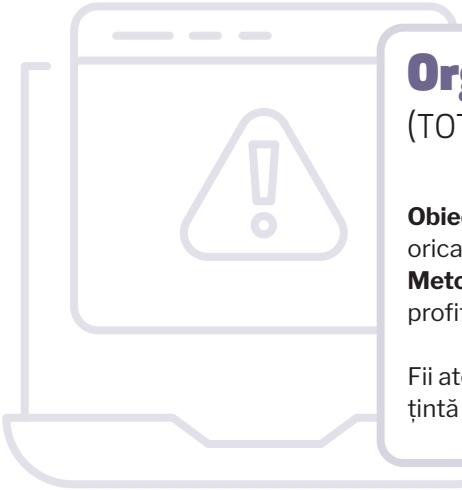
> Rolul nostru, în calitate de experți în securitate cibernetică, este de a vă proteja să nu deveniți o victimă întâmplătoare (atac fără țintă precisă). Dacă un hacker vă vizează, cel mai probabil va găsi o cale sau o vulnerabilitate, iar rolul nostru este să întârziem acest lucru cât mai mult posibil.
>
> VLAD MAZUREAC, EXPERT ÎN SECURITATE CIBERNETICĂ

Ghidul tău rapid privind tipurile de infractori cibernetici

Hacktiviștii
(DA, CHIAR EXISTĂ!)

Motivație: Motivați de cauze politice sau sociale.
Misiune: Să militeze pentru agenda lor sau să protesteze împotriva nedreptăților percepute.
Atacurile cibernetice preferate: Desfigurarea site-urilor web, scurgerea de informații sensibile sau perturbarea activităților online.

Natura activității tale ar putea într-adevăr să te transforme în țintă pentru hacktiviști. Informează-te și rămâi vigilent.



Organizații criminale
(TOTUL DESPRE BANI)

Obiectiv: Să-și extindă activitățile infracționale, oricare ar fi acestea.
Metoda: Furt de date private pentru a le vinde pentru profit.

Fii atent, deoarece datele tale valoroase ar putea fi o țintă lucrativă pentru aceste organizații.

Actori sponsorizați de stat
(STRĂINI SAU INTERNI)

Implicare: Guverne sau entități sponsorizate de stat.
Obiectiv: Suprimarea disidenței și monitorizarea activităților opoziției.
Nivelul de risc: Capacitățile avansate prezintă un risc ridicat atât pentru persoane, cât și pentru organizații.

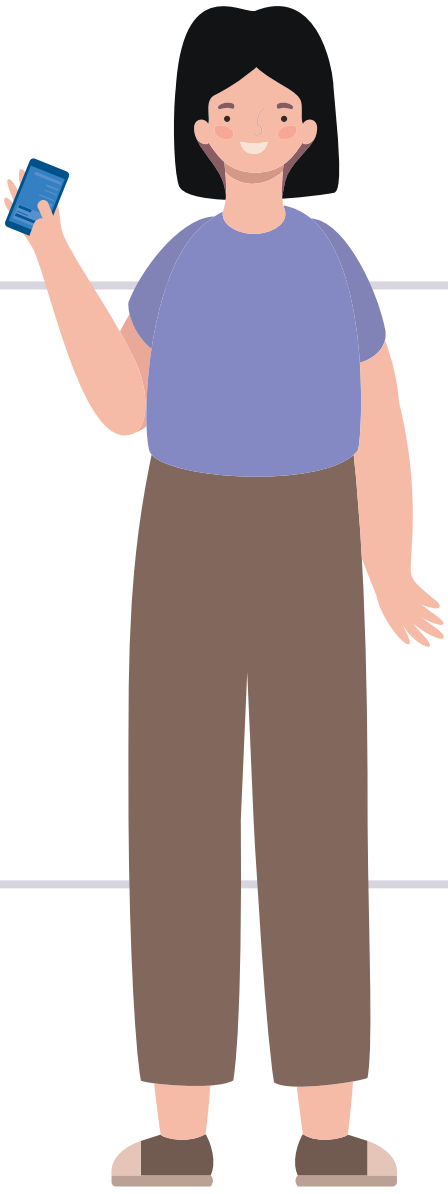
Este esențială înțelegerea motivațiilor din spatele amenințărilor cibernetice împotriva activiștilor/elor, a promotorilor/oarelor păcii și a liderilor comunității. Acest lucru îți permite să recunoști potențialele amenințări și să iei măsuri pro-active pentru a dezvolta măsuri solide de securitate cibernetică.

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

1 Vulnerabilitatea universală: Toată lumea este susceptibilă la atacuri cibernetice. Rolul tău profesional ar putea crește acest risc.
2 Atacuri țintite vs. atacuri fără țintă: Distincția principală constă în intenție. Atacurile cu țintă precisă vizează anumite persoane, în timp ce atacurile fără țintă precisă au o rază de acțiune mai largă.
3 Diverse motivații ale infractorilor cibernetici: Există diferite tipuri de infractori cibernetici, fiecare fiind condus de agende și motivații unice.
4 Protecție holistică: Acordarea de prioritate siguranței cibernetice nu te protejează doar pe tine, ci extinde protecția la colegii, beneficiarii și organizația ta.

Ia aminte că înțelegerea acestor aspecte cheie nu numai că întărește apărarea individuală, dar contribuie și la rezistența colectivă a ecosistemului tău profesional.

> Cunoaște-ți inamicul și cunoaște-te pe tine însuți și vei putea duce o sută de bătălii fără pierderi.
>
> SUN TZU



TESTEAZĂ-ȚI CUNOȘTINȚELE:

Anastasia, o activistă proeminentă, a primit un e-mail de phishing care pretindea că provine de la o organizație pentru drepturile omului cu care colabora. E-mailul o îndemna să facă clic pe un link pentru a-și actualiza acreditările din cauza unei breșe de securitate.

Victima cărui tip de atac cibernetic a fost ea?

1. Atac țintit pentru a-i fura datele
2. Atac fără țintă precisă pentru a-i fura datele
3. Atac cu țintă precisă din partea unei organizații criminale
4. Atac fără țintă precisă din partea unei organizații criminale

Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

Navigarea în siguranță pe internet: ai merge pe o stradă aglomerată cu geanta deschisă?

Cu siguranță că nu!

Imaginează-ți că mergi pe una dintre străzile pline de viață ale Chișinăului în drum spre serviciu. Să te asiguri că geanta este bine închisă, să privești în ambele sensuri înainte de a traversa strada și să fii atent/ă la ceea ce te înconjoară este ca și firesc pentru tine. Chiar și în spații aparent sigure, să rămâi conștient, prudent și să iei măsuri pro-active pentru a reduce riscul devin obiceiuri înrădăcinate...

Aceleași principii se aplică și atunci când navighezi în lumea online. Navigarea în siguranță pe internet reflectă principiile unui mers singur pe stradă, punând accentul pe conștientizare, prudență și măsuri proactive pentru a minimiza riscurile.

Responsabilizează-te să fii mai vigilent/ă în spațiul digital. Infractorii cibernetici folosesc tehnici din ce în ce mai sofisticate pentru a înșela și fura date. Deși poate fi dificil la început, adoptarea acestor practici este similară cu obiceiurile pe care le aplici atunci când te deplasezi pe străzi sau când părăsești apartamentul - acestea devin o a doua natură cu ajutorul practicii.

Aspect	Mers pe străzi în siguranță	Navigare sigură pe Internet
Vigilență și conștiență	Fii atent/ă la împrejurimi, evită zonele slab iluminate și fii atent la persoanele necunoscute.	Fii atent/ă la escrocheriile de tip phishing și la site-urile frauduloase.
Verificarea siguranței	Alege rute sigure și verifică credibilitatea cartierului în ceea ce privește siguranța fizică.	Verifică autenticitatea site-urilor web înainte de a împărtăși informații personale.
Măsuri preventive	Adoptă măsuri preventive, cum ar fi închiderea ușilor, închiderea genții și asigurarea obiectelor de valoare.	Folosește instrumente de securitate, actualizează browser-ele și folosește setări stricte de confidențialitate.
Respectarea regulilor și a instrucțiunilor	Respectă regulile de circulație și urmează indicatoarele și instrucțiunile de circulație.	Urmează cele mai bune practici de securitate cibernetică și respectă regulile online.
Verificări periodice de securitate	Efectuează verificări periodice ale lacătelor, ușilor și împrejurimilor în ceea ce privește securitatea fizică.	Actualizează în mod regulat sistemele de operare, browser-ele și programele de securitate.

SERGHEI SAVCHIUC | UNSPLASH

Ghidul tău rapid pentru identificarea site-urilor web frauduloase:

1 Verifică URL-ul: Examinează URL-ul site-ului web pentru a vedea dacă nu conține greșeli de ortografie, caractere suplimentare sau domenii neobișnuite.
-Legitim: https://www.example.com
-Phishing: https://www.exaample.com (greșeală de ortografie), https://www.example.pf (domeniu neobișnuit)

2 Caută HTTPS: Asigură-te că site-ul web utilizează HTTPS în loc de HTTP. Litera S indică o conexiune securizată cu criptare pentru transmiterea datelor.
-Legitim: https://www.securewebsite.com
-Phishing: http://www.insecurewebsite.com (lipsește litera S pentru a fi un site sigur)

3 Verifică designul site-ului web: Fii atent la site-urile web prost concepute sau la cele cu numeroase ferestre pop-up.
-Legitim: Aranjare profesionistă, branding consecvent.
-Phishing: Design slab, logo-uri nepotrivite, numeroase ferestre pop-up.

4 Verifică informațiile de contact: Site-urile legitime oferă informații de contact clare. Fii suspicios dacă nu este disponibile informații de contact sau dacă detaliile par dubioase.
-Legitim: Pagina de contact clară, cu o adresă, un număr de telefon și un e-mail valabile.
-Phishing: Nu există informații de contact sau detalii suspecte, cum ar fi o adresă de e-mail generică.

5 Treceți cu mouse-ul peste linkuri: Treceți mouse-ul peste link-uri pentru a pre-vizualiza URL-ul de destinație. Evitați să dați clic pe linkurile din e-mailuri; în schimb, introduceți direct adresa URL.
-Legitim: Dacă treceți cu mouse-ul peste un link, apare o pre-vizualizare care corespunde textului afișat.
-Phishing: Dacă se trece cu mouse-ul deasupra, se dezvăluie un URL de destinație diferit, de exemplu, http://www.trustworthy.com (afișat), dar conduce la http://www.phishingsite.com.

Site-uri web frauduloase

EXPLICATE SIMPLU

Ce sunt acestea? Site-urile web frauduloase sunt platforme online nelegitime, concepute pentru a înșela vizitatorii și a-i determina să furnizeze informații personale sau financiare.
Cum? Prin crearea de site-uri care imită entități demne de încredere, cu scopul de a păcăli utilizatorii să dezvăluie date sensibile.
Unde? Bănci, magazine de comerț electronic, site-uri de întâlniri, etc.

Ghidul tău rapid pentru identificarea escrocheriilor de tip phishing:

1 Verifică conturile în mod regulat : Un e-mail de phishing poate sugera activități suspecte în contul tău, îndemnându-te să faci clic pe un link pentru a rezolva problema.
Exemplu: "Urgent: Contul tău a fost compromis. Intră aici pentru a verifica".

2 E-mail-uri prin care se solicită acțiuni urgente: Phisherii creează un sentiment de urgență.
Exemplu: "Contul tău va fi suspendat dacă nu confirmi datele în termen de 24 de ore. Dă clic acum pentru a evita întreruperile".
Exemplu: "Acționează acum pentru a revendica recompensa înainte să expire!"

3 E-mail-uri cu gramatică proastă și ortografie neprofesionistă: Organizațiile legitime mențin o comunicare profesională.
Exemplu: "Stimate utilizator, contul tău a fost închis. Rugăm să actualizați parola pentru siguranță".
Exemplu: "Dă clic aici pentru prem1ul tău exclusiv" în loc de "Dă clic aici pentru premiul tău exclusiv".

4 Utilizarea unui domeniu public de e-mail: E-mail-urile de phishing pot utiliza domenii de e-mail generice.
Exemplu: "service@gmail.com" în loc de "service@legitimatecompany.com".

5 Verifică adresa de e-mail: Infractorii cibernetici imită adresele de e-mail legitime.
Exemplu: "support@paypa1.com" în loc de "support@paypal.com."

5 Subiect generic: E-mail-urile de phishing au adesea subiecte vagi.
Exemplu: "Informații importante", fără a preciza natura mesajului.

Escrocherii de tip phishing:

EXPLICAT SIMPLU

Ce este? Escrocheriile de tip phishing sunt încercări frauduloase de a păcăli persoanele pentru a le determina să divulge informații sensibile, cum ar fi nume de utilizator, parole sau detalii financiare, care pot fi apoi folosite în scopuri rău intenționate.
Cum? Prin a se da drept entități de încredere în e-mailuri, mesaje sau alte forme de comunicare.
Unde? E-mailuri, rețele de socializare, chat Whatsapp, etc.

CELE MAI FRECVENTE LINII DE SUBIECT ALE E-MAILURILOR DE PHISHING DIN VIAȚA REALĂ LA NIVEL GLOBAL SUNT:

Google: Ai fost menționat într-un document: "Proiectul planului strategic"
Resurse umane: Important: Modificări ale codului vestimentar
Resurse umane: Actualizarea politicii de concediu
Adobe Sign: Evaluarea performanței Dvs.Verificarea parolei este necesară imediat. Recunoașteți evaluarea Dumneavoastră
IT: Raport privind internetulPrincipalele teze ale reuniunii de astăzi
USAA: Suspendarea contului. Rambursarea cheltuielilor angajaților pentru [[email]]

Phishing-ul devine din ce în ce mai popular printre infractorii cibernetici:

Aproximativ **1,2 %** din toate e-mailurile trimise la nivel mondial sunt tentative de phishing. **81%** dintre organizațiile din întreaga lume au observat o creștere a atacurilor de phishing prin e-mail.
Escrocheriile de tip phishing contribuie la aproape **36%** din toate cazurile de încălcare a securității datelor, conform raportului Verizon 2022 Data Breach Report.

Site-uri web frauduloase v/s Escrocherii de Phishing: același lucru, dar diferit

Site-urile web frauduloase sunt platforme online nelegitime, concepute pentru a convinge vizitatorii să furnizeze informații personale sau financiare prin mijloace înșelătoare, adesea imitând entități de încredere.
Pe de altă parte, escrocheriile de tip phishing implică practici frauduloase, cum ar fi e-mailuri sau comunicări înșelătoare, în care atacatorii se dau drept surse demne de încredere pentru a păcăli persoanele să dezvăluie informații sensibile.

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

1. La fel ca în cazul obiceiurilor fizice, practicile digitale devin o a doua natură cu practica.
2. Fii atent/ă la escrocheriile de tip phishing și la site-urile frauduloase.
3. Verifică autenticitatea site-urilor web înainte de a împărtăși informații personale.
4. Folosește instrumente de securitate, actualizează browser-ele și folosește setări stricte de confidențialitate.
5. Actualizează în mod regulat sistemele de operare, browser-ele și programele de securitate.

Acum este o lume online mai sigură pentru tine și pentru toți cei din jurul tău.

TESTEAZĂ-ȚI CUNOȘTINȚELE:

Care dintre următoarele subiecte de e-mail sunt frecvent asociate cu e-mailurile de phishing? (Selectați toate variantele care se aplică):

1. Contul tău a fost compromis. Verifică îndată!
2. Urgent: Este necesară o acțiune imediată pentru actualizarea salariilor
3. Confirmarea abonării la comunicate
4. Cadou gratuit! Dă clic pentru a revendica premiul
5. Important: Revizuiește și aprobă documentul
6. Alertă de securitate: A fost detectată o activitate neobișnuită de autentificare
7. Felicitări! Ai câștigat la loterie.

Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

WiFi public: Un paradis pentru intrușii cibernetici

Sfat:

Dacă nu ești dispus/ă să strigi în gura mare informții sensibile, nu le partaja pe o rețea Wi-fi publică.

Maria se bucură de o cină plăcută cu cea mai bună prietenă a ei, Anastasia, la restaurantul lor preferat, pentru a recupera după ce nu s-au văzut de ceva vreme. Acestea se bucură de o conversație vioaie, schimbând anecdote personale și povestindu-și aventurile de vară. Conversația trece la discuții despre muncă, deoarece plănuiesc să colaboreze la un proiect comun.

În cursul conversației, Maria și Anastasia fac schimb de informații private despre locația adăposturilor pe care le-au înființat pentru a găzdui femei care au supraviețuit violenței de gen. Ele discută despre cum să-i ajute pe rezidente și își fac planuri de vizită în ziua următoare.

Acum, imaginează-ți un scenariu în care întreaga conversație devine de notorietate publică; toată lumea din restaurant le ascultă.

Deși poate părea o exagerare, acest lucru ilustrează vulnerabilitatea rețelelor WiFi publice. Fiecare utilizator din rețea are acces nelimitat la informațiile transmise.

Conectarea la un hotspot WiFi îi conferă proprietarului hotspot-ului autoritatea de a monitoriza activitățile online și, în unele cazuri, chiar de a urmări mișcările fizice.

Ia în considerare implicațiile atunci când lucrezi de la o cafenea, când folosești un computer de serviciu pentru a gestiona informații sensibile, pentru a schimba e-mailuri sau pentru a partaja detalii confidențiale. Toate aceste date devin vizibile și accesibile în rețeaua WiFi publică, transformând-o într-un potențial teren de joacă pentru hackeri.

KLARA KULIKOVA | UNSPLASH

Dacă ai nevoie să vizualizezi anumite informații sensibile sau să accesezi conturi protejate prin parolă, există câteva metode sigure:

1. Configurarea și utilizarea unui Hotspot
Atunci când se accesează informații sensibile sau conturi protejate prin parolă, configurarea unui hotspot personal poate spori securitatea. Urmează acești pași:

a. Activează Hotspot:
- Pe telefonul smartphone, accesează Setări.
- Găsește opțiunea "Hotspot" sau "Tethering".
- Pornește hotspot-ul și setează o parolă puternică.

b. Conectează dispozitivele:
- Conectează-ți computerul sau alte dispozitive la hotspot.
- Asigură-te că hotspot-ul tău este protejat cu o parolă pentru un nivel suplimentar de securitate.

c. Accesează datele sensibile:
- Odată conectat/ă, vizualizează în siguranță informații sensibile sau accesează conturi protejate prin parolă.

Notă: Acestea sunt orientări generale și pot fi diferite în funcție de dispozitiv și de sistemul de operare.

SPOTLIGHT

Lumina reflectorului: deși convenabil, Wifi-ul public prezintă multe riscuri

Infractorii cibernetici pot intercepta datele dintre dispozitivul tăi și router-ul WiFi, putând capta informații sensibile.
Lipsa de criptare înseamnă că datele transmise prin WiFi public sunt mai vulnerabile la interceptare.
Atacatorii cibernetici pot crea hotspot-uri WiFi frauduloase cu nume înșelătoare, păcălindu-i pe utilizatori să se conecteze la rețele rău intenționate.
Hackerii pot folosi instrumente de adulmecare a pachetelor pentru a captura și analiza pachetele de date, extrăgând detalii sensibile.

2. Utilizează o rețea privată virtuală (VPN)
Utilizarea unui VPN este o modalitate eficientă de a-ți securiza activitățile online, în special pe rețelele WiFi publice. Iată un ghid rapid pentru Windows și Mac:

a. Selectează un furnizor de VPN:
- Alege un serviciu VPN de renume și înregistrează-ți un cont.

b. Descarcă și instalează:
- Descarcă clientul VPN pentru sistemul tău de operare.
- Instalează software-ul urmând instrucțiunile.

c. Conectează-te la un server:
- Lansează aplicația VPN.
- Alege o locație a serverului și stabilește o conexiune securizată.

d. Accesează informațiile sensibile:
- Cu VPN-ul activ, accesează în siguranță informații sensibile în rețelele publice.

Notă: Acestea sunt orientări generale și pot fi diferite în funcție de dispozitiv și de sistemul de operare.

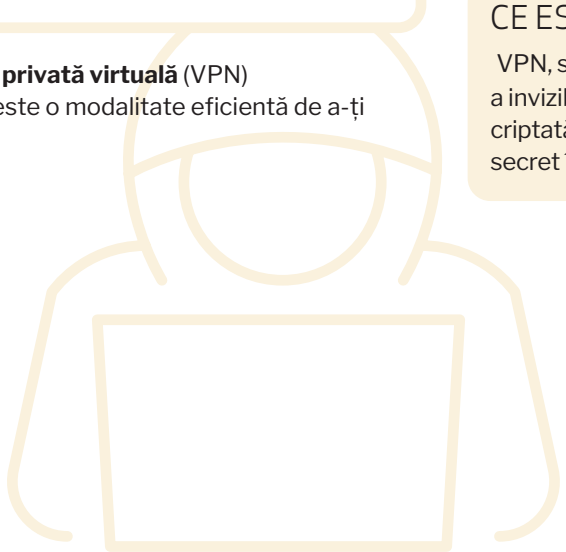
3. Așteaptă până când vei putea utiliza o rețea WiFi nepublică de încredere

Atunci când ai de-a face cu date foarte sensibile, cea mai sigură opțiune ar putea fi să aștepți până să ai acces la o rețea WiFi nepublică în care ai încredere. Evitarea totală a rețelelor publice elimină riscurile asociate cu acestea.

Ia aminte că securitatea datelor tale este esențială, iar alegerea metodei potrivite depinde de nivelul de sensibilitate și de urgență.

CE ESTE UN VPN?

VPN, sau Rețeaua privată virtuală, este mantia digitală a invizibilității. Cu VPN, datele tale poartă o deghizare criptată, ceea ce le face la fel de sigure ca un agent secret într-o misiune secretă.



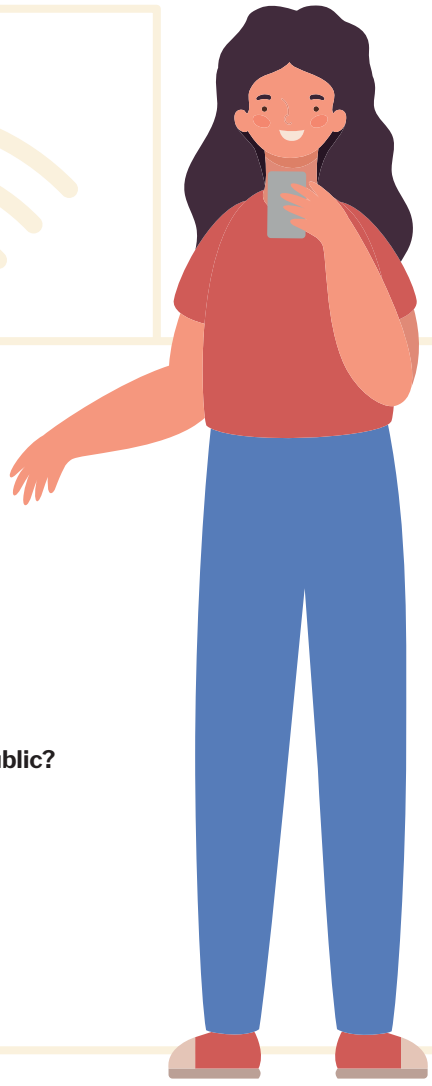
ATENȚIE:

ce trebuie luat în calcul la alegerea unui furnizor de VPN:

Caracteristici de securitate și confidențialitate: Asigură-te că VPN-ul are o criptare robustă, o politică de interzicere a înregistrărilor și protocoale de securitate avansate pentru a-ți proteja datele.
Rețeaua și locațiile serverului: O rețea de servere diversă și extinsă îți îmbunătățește experiența online. Alege un VPN cu servere amplasate strategic în întreaga lume.
Viteza de conectare: Optează pentru un VPN care oferă viteze de conectare rapide și fiabile, esențiale pentru navigare și streaming fără întreruperi.
Caracteristici și performanță: Evaluează funcțiile suplimentare oferite de VPN, cum ar fi comutatoarele kill switch, tunelarea divizată și performanța generală.
Prețuri: Deși un VPN gratuit poate părea tentant, serviciile cu plată oferă adesea o securitate și o performanță mai bune. Alege un VPN care se potrivește bugetului tău și oferă un raport calitate-preț.

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

1. Rețelele WiFi publice expun utilizatorii la potențiali intruși cibernetici, deoarece fiecare utilizator din rețea are acces nelimitat la informațiile transmise.
2. Atunci când ai de-a face cu date extrem de sensibile, cea mai sigură opțiune este să aștepți să ai acces la o rețea WiFi de încredere, nepublică.
3. Analizează opțiunea configurării și utilizării unui Hotspot sau a unui VPN.
4. Alegerea metodei de securitate potrivite depinde de nivelul de sensibilitate și de urgență.



TESTEAZĂ-ȚI CUNOȘTINȚELE:

Întrebarea 1: Ce risc potențial prezintă rețelele WiFi publice?

A) Acces limitat la informații
B) Securitate sporită
C) Expunere la intruși cibernetici
D) Urmărirea fizică a utilizatorilor

Întrebarea 2: Cum îmbunătățește VPN-ul securitatea pe WiFi-ul public?

A) Prin expunerea de informații sensibile
B) Prin limitarea activităților online
C) Prin stabilirea unei conexiuni securizate
D) Prin evitarea rețelelor publice

Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

Ce au în comun cheile de la casă și parolele?

Într-o după-amiază, în timp ce mergea pe străzile aglomerate ale Chișinăului, Anastasia se confruntă cu o criză neașteptată - își dă seama că și-a pierdut cheile. Se panichează, deoarece se teme că securitatea ei fizică ar putea fi compromisă. Pe lângă faptul că locuința sa este vulnerabilă la furt, Anastasia nu se simte în siguranță să doarmă acasă. Repede, Anastasia se întoarce pe unde a trecut și caută pe străzi, dar nu-și găsește cheile. Astfel, recunoscând gravitatea amenințării, Anastasia contactează imediat poliția, raportează lipsa cheilor, cheamă un lăcătuș pentru a schimba încuietoarea și solicită mai multe copii ale cheilor, lăsând una la o persoană de încredere.

Acum, gândește-te la următorul lucru: la fel cum cheile Anastasiei deschid ușa de la casa ei, parolele acționează ca chei ale obiectelor valoroase din punct de vedere digital - conturi bancare, e-mailuri, comunicare, informații private, date de la locul de muncă, beneficiari, comunicare personală, etc.

Amount of time to crack a password	
7 characters	.29 milliseconds
8 characters	1 – 5 hours
9 characters	11 hours – 5 days
10 characters	3 – 4 months
11 characters	1 decade
12 characters	2 centuries

Source (17) https://www.verveit.com/blog/is-your-password-strong-enough

SASHA PLESCHCO | UNSPLASH

Ghidul tău rapid pentru stabilirea de parole puternice și sigure

1 - Evită parolele comune:
Evită parolele ușor de ghicit, cum ar fi "parola123" sau cuvinte comune. Optează pentru combinații unice pentru a spori securitatea.
Un bun exemplu: Tr3ndyP@ssw0rd! (Complex și unic)
Exemplu rău: Parola123 (Simplu și utilizat în mod obișnuit)

2 - Folosește un amestec de caractere:
Încorporează o combinație de litere majuscule și minuscule, numere și caractere speciale pentru a crește complexitatea.
Un bun exemplu: F!reDraGon87# (Include o varietate de tipuri de caractere)
Exemplu prost: parola1234 (Lipsește diversitatea și complexitatea)

3 - Lungimea parolei:
Creează parole lungi, deoarece acestea sunt în general mai robuste. Încearcă să obții cel puțin 12 caractere.

Un bun exemplu: S3cur3L0ngP@ssw0rd! (Lung și complex)
Exemplu rău: ParScurt! (Prea scurt pentru a asigura o securitate puternică)

4 - Parolă unică pentru fiecare cont:
Evită folosirea aceleiași parole pentru mai multe conturi. Parolele unice pentru diferite platforme sporesc securitatea generală.

5 - Evită informațiile personale:
Evită să incluzi detalii personale, cum ar fi nume, zile de naștere sau adrese. Aceste informații sunt ușor accesibile și pot fi exploatate de atacatori.

Un bun exemplu: B3l0v3dPet#R0v3r (Încorporează elemente personale, dar nu este evident)
Exemplu rău: JohnsDog123 (în legătură directă cu informații personale)

6- Actualizează parolele cu regularitate:
Schimbă parolele periodic pentru a reduce riscul de compromitere. Setează memento-uri pentru a le actualiza la fiecare câteva luni.

7 - Configurează 2FA (autentificare cu doi factori) sau MFA (autentificare cu factori multipli):
Autentificarea cu doi factori (2FA) adaugă un nivel suplimentar dincolo de simple parole, solicitând utilizatorilor să furnizeze o a doua formă de identificare, cum ar fi un cod temporar trimis pe dispozitivul lor mobil.

Acest lucru reduce semnificativ riscul de acces neautorizat, chiar dacă parolele sunt compromise.

7 - Utilizează un manager de parole:
Dacă ai mai multe conturi și trebuie să ții evidența tuturor parolelor, folosește un manager de parole. Alege un manager de parole de încredere: iată câteva dintre cei mai siguri manageri de parole recomandați de experții cibernetici.

1Password: Cunoscut pentru designul său bogat în funcții și intuitiv.

Recomandarea experților: Considerat cel mai bun manager de parole în general, oferind un echilibru între caracteristici, folosire intuitivă și accesibilitate.

Bitwarden: Manager de parole open-source cu un accent deosebit pe securitate.

Recomandarea experților: Recunoscut pentru măsurile sale de securitate și pentru capacitatea de a fi implementat pe diferite platforme.

NordPass: Dezvoltat de creatorii NordVPN, care oferă caracteristici de securitate solide.

Recomandarea experților: Notat ca fiind una dintre alegerile de top pentru gestionarea parolelor în 2024

9 - Optează pentru utilizarea unei fraze de acces:
O frază drept parolă este un șir de cuvinte ca într-o propoziție, utilizată pentru autentificare, care este mai lungă decât o parolă tradițională, ușor de reținut și dificil de spart.

Un bun exemplu: Elefanți11PurpuriiSarSus (Frază de acces lungă și memorabilă)
Exemplu rău: ParolaMea123 (Simplu și totuși seamănă cu o parolă obișnuită)

PAROLĂ SAU FRAZĂ DE ACCES?

O parolă este, de obicei, o combinație de caractere, inclusiv litere, numere și simboluri, utilizată pentru a autentifica un utilizator. De obicei, este mai scurtă și mai complexă.

Pe de altă parte, o frază de acces este o secvență mai lungă de cuvinte sau o propoziție. Aceasta tinde să fie mai firească de reținut, dar este mai lungă.

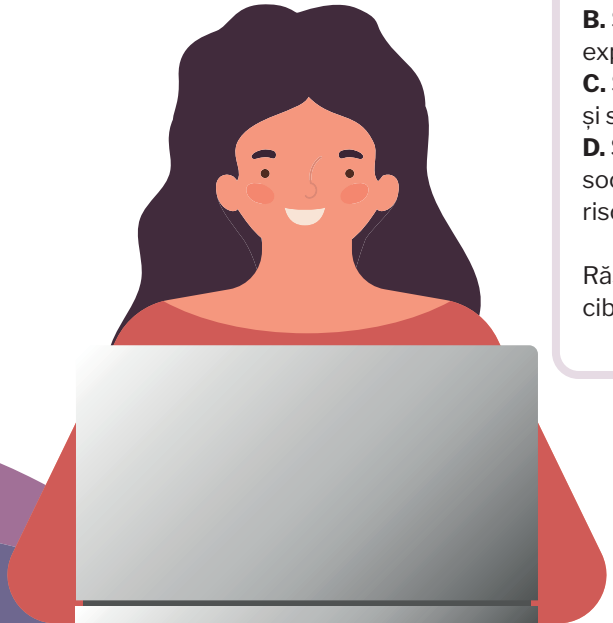
Care este mai sigură? Siguranța unei parole sau a unei fraze de acces depinde de diverși factori, inclusiv de lungime și complexitate. În general, parolele sau frazele de acces mai lungi și mai complexe sunt mai sigure. Adesea, frazele de acces oferă o securitate mai bună datorită lungimii lor și a utilizării de elemente de limbaj natural.

Number of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2 bn years	48 bn years	380 bn years
18	6 days	481k years	126 bn years	2 tn years	26 tn years

Source (18): https://tech.co/password-managers/how-long-hacker-crack-password

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

1. Atât cheile de la casă, cât și parolele sunt esențiale pentru securitate, iar compromiterile prezintă riscuri pentru siguranța fizică și digitală.
2. Folosește parole sau fraze de acces puternice pentru a-ți proteja conturile. Folosește combinații unice, un amestec de caractere și parole mai lungi (cel puțin 12 caractere) pentru a spori securitatea.
3. Implementează măsuri de securitate suplimentare, cum ar fi autentificarea cu doi factori (2FA), pentru a adăuga un nivel suplimentar de protecție, dincolo de parole.



TESTEAZĂ-ȚI CUNOȘTINȚELE:

Scenariu: Maria primește o notificare referitoare la accesul neautorizat la informații personale în cadrul unei spargeri a securității datelor. Panicată, ea își dă seama că trebuie să ia măsuri imediate pentru a rezolva situația și a proteja datele sensibile.

Întrebare de test:
Ce măsuri ar trebui să ia Maria după primirea notificării privind accesul neautorizat în cazul unei spargeri a securității datelor?

Opțiuni:
A. Să ignore notificarea; este posibil să fie o alarmă falsă.
B. Să ia legătura cu compania implicată și să ceară o explicație.
C. Să schimbe parolele asociate cu contul compromis și să activeze autentificarea cu doi factori.
D. Să împărtășească notificarea pe rețelele de socializare pentru a-i avertiza pe ceilalți cu privire la riscurile potențiale.

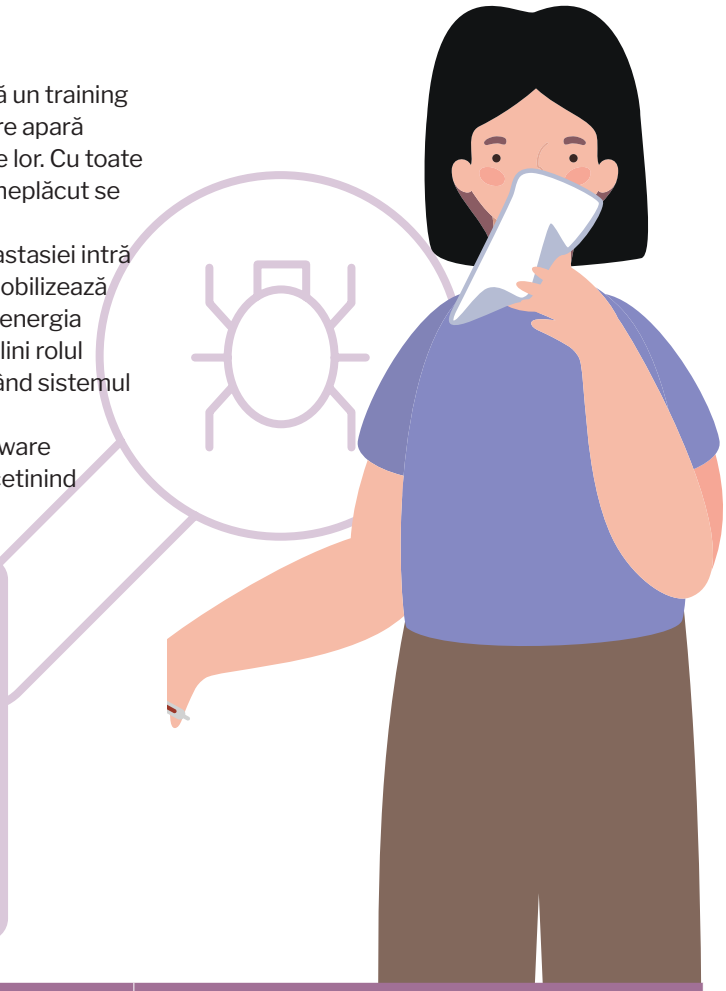
Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

Malware: un virus care slăbește sistemul imunitar al computerului.

Este luni dimineață, iar Anastasia se pregătește să conducă un training de două zile pentru tinerii activiști și activiste din Chișinău care apără drepturile femeilor pe rețelele de socializare și în comunitățile lor. Cu toate acestea, a apărut un adversar neașteptat - un virus. Un virus neplăcut se infiltrează în corpul ei, lăsând-o bolnavă, febrilă și slăbită.

Pe măsură ce virusul se instalează, sistemul imunitar al Anastasiei intră în acțiune. Celulele albe din sânge, apărătorii corpului ei, se mobilizează pentru a identifica și neutraliza amenințarea. Între timp, însă, energia Anastasiei scade rapid, afectându-i capacitatea de a-și îndeplini rolul cheie. Incapabilă să efectueze training-ul, ea îl amână până când sistemul ei imunitar reușește să neutralizeze virusul.

Ceva asemănător se întâmplă atunci când un program malware se infiltrează în computerul tău, compromițând fișierele și încetinind funcționalitatea.



CARE ESTE DIFERENȚA DINTRE MALWARE ȘI UN VIRUS?

Malware este un termen larg care cuprinde orice software rău intenționat conceput pentru a afecta un computer sau o rețea. Include diferite tipuri de viruși, troieni și ransomware. Pe de altă parte, un virus este un tip specific de malware care se reproduce și se răspândește în alte fișiere sau sisteme. În esență, toți virușii sunt programe malware, dar nu toate programele malware sunt viruși.

Aspect	Malware pe computer	Virus în corpul uman
Natura	Software rău intenționat conceput pentru a afecta sau exploata sistemele.	Agenți infecțioși care provoacă boli în organismele vii.
Forme	Diverse forme, inclusiv viruși, viermi, troieni etc.	Diferiți viruși care provoacă boli (de exemplu, gripa).
Transmitere	Se răspândesc prin intermediul fișierelor infectate, al site-urilor web sau fișierelor descărcate.	Se transmit prin contact direct, prin picături sau prin aer.
Replicare	Se replică în cadrul sistemului informatic pentru a se răspândi mai departe.	Se replică în celulele gazdei pentru a răspândi boala.
Intenție	Poate duce la furtul de date, la întreruperea sistemului sau la spionaj.	Cauzează boli, cu grade diferite de gravitate.
Detectare	Detectat de programele antivirus și de instrumentele de securitate cibernetică.	Diagnosticat prin teste și examene medicale.
Prevenire	Prevenit prin utilizarea antivirusului, a firewall-urilor și a actualizărilor.	Prevenit prin vaccinări, igienă și sănătate imunitară.
Impact asupra sistemului	Încetinește, întrerupe operațiunile sau deteriorează datele.	Cauzează simptome care variază de la boli ușoare la boli grave.
Tratament	Necesită instrumente de eliminare a programelor malware și restaurarea sistemului.	Tratament medical, medicație și îngrijire de susținere.
Evoluție	În continuă evoluție, cu noi variante și tehnici.	Evoluează prin mutații, ducând la noi tulpini de virus.
Origine	Dezvoltat de infractori cibernetici sau de entități rău intenționate.	Provine din surse naturale sau poate fi produs de om.

Malware este prescurtarea de la software malițios (rău intenționat).

(DA, AU ȘI PORECLE!)

Este un termen colectiv pentru diferite programe dăunătoare concepute pentru a afecta calculatoarele, a fura informații sau a perturba funcționarea normală.

În acest moment, probabil că te gândești de ce te-ar viza infractorii cibernetici pe tine sau organizația ta cu programe malware?

1 Spionaj politic: Hackerii se pot angaja în spionaj politic pentru a culege informații despre femeile implicate în politică și activități privind drepturile omului, exploatând datele sensibile ale organizațiilor(22).

2 Perturbarea activismului: Actorii rău intenționați pot avea ca scop întreruperea activităților grupurilor pentru drepturile femeilor prin infectarea sistemelor acestora cu programe malware. Acest lucru le poate împiedica capacitatea de a milita pentru schimbare.

3 Câștigarea unui punct de sprijin pentru atacuri mai mari: Hackerii se folosesc adesea de infecțiile inițiale cu malware pentru a obține un punct de sprijin în cadrul unei rețele. Odată intrate, acestea își pot extinde accesul și pot lansa atacuri mai ample, putând compromite întreaga infrastructură a organizației(23).

4 Agende politice sau sociale: Actorii care reprezintă o amenințare pot utiliza programe malware pentru a promova agende politice sau sociale specifice, cum ar fi răspândirea de dezinformări sau discreditarea activităților organizațiilor pentru drepturile femeilor(24).

Maria eventually went to the doctor, took the recommended treatment and recovered from the virus. She ended up giving the training a few days later and made sure to mention the importance of cyber safety for any activist, peacebuilder and advocate.

ASTA ÎNSEAMNĂ CĂ EXISTĂ ȘI ALTE TIPURI DE SOFTWARE RĂU INTENȚIONAT?
DA, DESTUL DE MULTE...

Spyware: Ca niște spioni digitali, care observă în liniște și fură informații.

Adware: Ca niște vânzători de pop-up enervanți, care te bombardează cu reclame nedorite.

Ransomware: Ca un răpitor digital, care îți blochează fișierele până când plătiți o răscumpărare.

Vierme: Ca și răspândirea infecțiilor, se auto-replică și exploatează vulnerabilitățile.

Troian: Ca și cadourile înșelătoare, care se prefac în software legitim.

Soluții antivirus, antispyware și firewall aprobate de experți cibernetici:

Bitdefender®

norton™

Câteva cifre despre diferite tipuri de malware:

La nivel global, **72,7 %** din toate organizațiile au căzut pradă unui atac ransomware în 2023, ceea ce evidențiază impactul semnificativ asupra securității cibernetice.

În 2020, **61%** dintre organizații s-au confruntat cu o activitate malware care s-a răspândit de la un angajat la altul; până în 2021, acest număr a crescut la **7%**, subliniind creșterea frecvenței incidentelor malware.

Adware a reprezentat **25,28%** din toate amenințările mobile detectate în 2022, ceea ce indică prevalența sa ca tip de amenințare proeminent.

Surse:
(19) https://www.cobalt.io/blog/cybersecurity-statistics-2024
(20) https://www.comparitech.com/antivirus/malware-statistics-facts/
(21) https://terranovasecurity.com/blog/cyber-security-statistics/

CE ESTE UN FIREWALL?

-Un firewall este ca un paznic pentru rețeaua de calculatoare.
-Monitorizează și controlează traficul care intră și iese, acționând ca o barieră de protecție.
-Lasă să intre lucrurile bune și blochează lucrurile rele, cum ar fi amenințările cibernetice.
-Firewall-urile pot fi hardware sau software și joacă un rol crucial în menținerea unui mediu online sigur.

SPOTLIGHT

Cum să-ți protejezi computerul de programele malware?

Pe lângă utilizarea unor parole puternice și evitarea clicului pe link-uri suspecte, iată câteva lucruri importante pe care ar trebui să le faci:

-Instalează programe antivirus și antispyware de încredere pentru a detecta și elimina amenințările malware.
-Păstrează software-ul actualizat: aceasta include sistemele de operare, aplicațiile și software-ul antivirus.
-Folosește un firewall pentru a monitoriza traficul de intrare și de ieșire din rețea și pentru a acționa ca o barieră suplimentară împotriva programelor malware.

TESTEAZĂ-ȚI CUNOȘTINȚELE:

Întrebarea 1: Care este scopul principal al spyware-ului?

A. Îmbunătățirea performanțelor sistemului
B. Observarea și furtul de informații
C. Blocarea fișierelor până la plata unei răscumpărări
D. Răspândirea infecțiilor și auto-replicarea

Întrebarea 2: De ce s-ar putea ca infractorii cibernetici să se angajeze în spionaj politic folosind programe malware?

A. Pentru a îmbunătăți performanța sistemului
B. Pentru a perturba activismul
C. Pentru a obține un punct de sprijin pentru atacuri mai mari
D. Pentru a promova agende politice sau sociale specifice

Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

Lupta Anastasiei împotriva unui virus reflectă impactul programelor malware asupra calculatoarelor, perturbând atât operațiunile normale, cât și încetinind funcționalitatea acestora.

Malware este un termen generic pentru diferite forme de soft-uri dăunătoare.
Infractorii cibernetici țintesc activiștii cu programe malware în scopul spionajului politic, al perturbării activismului, al promovării unor agende politice și sociale specifice și ca punct de intrare pentru atacuri mai ample.

Rămâi în siguranță prin instalarea de programe antivirus și antispyware, actualizarea permanentă a software-ului și utilizarea unui firewall.

Protejează-ți dispozitivele, organizația și beneficiarii

Drumul către siguranța cibernetică poate fi o provocare. Schimbarea obiceiurilor poate necesita timp și muncă, dar este extrem de importantă pentru a proteja informațiile sensibile, pentru a te proteja pe tine, pe colegii tăi și, cel mai important, pentru a-ți proteja beneficiarii.

Acest ghid își propune să ofere pași practici pentru securizarea dispozitivelor, promovarea conștientizării și implementarea unor măsuri solide de securitate cibernetică în cadrul organizației.

PENTRU ÎNCEPUT: SCHIMBAREA PRACTICILOR CIBERNETICE PAS CU PAS

Formarea angajaților:

-Organizează sesiuni de informare în domeniul securității cibernetice pentru a-i familiariza pe angajați despre amenințările comune, cu atacurile de phishing și despre importanța unui comportament online sigur.
-Începe cu concepte de bază înainte de a te familiariza cu practici mai complexe de securitate cibernetică.

Sesiuni regulate de perfecționare:

-Programează sesiuni periodice de perfecționare în domeniul securității cibernetice pentru a consolida cunoștințele și pentru a actualiza cunoștințele angajaților cu privire la amenințările emergente.
-Încurajează comunicarea deschisă, permițând angajaților să își împărtășească preocupările și să pună întrebări.

Punerea în aplicare pe etape:

-Introdu măsurile de securitate cibernetică în etape, pentru a evita copleșirea angajaților.
-Începe cu practici fundamentale, cum ar fi igiena parolelor și treci treptat la măsuri mai avansate.

> Pentru a fi eficientă, formarea în domeniul securității cibernetice implică o schimbare de comportament.

SCHIMBĂRI DE COMPORTAMENT PENTRU O MAI MARE SIGURANȚĂ CIBERNETICĂ

Pe lângă măsurile tehnice, promovarea schimbărilor comportamentale este vitală pentru o securitate cibernetică rezistentă:

1. Obiceiuri de navigare în siguranță

-Sfătuiește angajații să examineze cu atenție URL-urile, să evite să dea click pe link-uri suspecte și să verifice
-legitimitatea site-urilor web.
Implementează instrumente de filtrare web pentru a bloca accesul la site-uri rău intenționate.

2. Autentificarea cu doi factori (2FA)

-Promovează utilizarea 2FA pentru a adăuga un nivel suplimentar de protecție pentru conturi și sisteme.
-Încurajează adoptarea autentificării biometrice pentru o securitate sporită

3. Cultura raportării incidentelor

-Încurajează o cultură în care angajații să se simtă confortabil să raporteze prompt orice activități suspecte sau incidente de securitate.
-Stabilește un plan clar de răspuns la incidente pentru a le rezolva eficient și în timp util.

Acordând prioritate securității cibernetice, organizațiile pentru drepturile femeilor își pot consolida apărarea digitală și își pot proteja activitatea. O combinație de educație, implementare treptată și încurajarea schimbărilor de comportament va contribui la un mediu cibernetpasic rezistent și sigur

ANRAS VAS | UNSPLASH

PUNEREA ÎN APLICARE A MĂSURILOR DE SECURITATE CIBERNETICĂ LA NIVEL DE ORGANIZAȚIE

1. Instalarea software-ului antivirus
-Folosește un software antivirus de încredere pentru a detecta și elimina amenințările rău intenționate.
-Actualizează în mod regulat bazele de date antivirus pentru a fi protejat/ă împotriva celor mai recente amenințări.

2. Actualizări regulate de software și hardware
-Actualizează în mod regulat sistemele de operare și aplicațiile pentru a remedia vulnerabilitățile.
-Activează actualizările automate ori de câte ori este posibil, pentru a asigura o protecție în timp util împotriva exploatatorilor cunoscuți.
-Asigură-te că toate componentele hardware, inclusiv router-ele și dispozitivele IoT, au cele mai recente actualizări de firmware pentru a rezolva problemele de securitate.

3. Utilizarea firewall-urilor
-Activează firewall-urile atât pe dispozitivele individuale, cât și pe infrastructura de rețea. Configurează firewall-urile pentru a monitoriza
-și controla traficul de intrare și ieșire din rețea, îmbunătățind securitatea generală.

4. Configurarea permisiunilor pentru angajați
-Pune în aplicare principiul celui mai mic privilegiu, acordând angajaților doar permisiunile necesare pentru rolurile lor.
-Revizuiește și actualizează în mod regulat permisiunile pentru a le alinia la schimbările organizaționale și la rolurile angajaților.

5. Utilizarea criptării
-Încurajează utilizarea criptării pentru comunicațiile sensibile și stocarea datelor.
-Implementează criptarea end-to-end pentru platformele de mesagerie pentru a proteja conversațiile confidențiale.

6. Copii de siguranță regulate
-Subliniază importanța efectuării regulate de copii de rezervă a datelor pentru a atenua impactul atacurilor ransomware sau al pierderilor de date.
-Păstrează copiile de rezervă în condiții de siguranță, de preferință într-un mediu offline sau în cloud, și testează periodic procesele de restaurare.

TESTEAZĂ-ȚI CUNOȘTINȚELE:

Întrebare: Care este scopul principal al formării în domeniul securității cibernetice?

A) Să îmbunătățească aspectul estetic al dispozitivului
B) Să rezulte într-un comportament schimbat
C) Să ignore măsurile de securitate cibernetică
D) Să se concentreze doar pe practicile complexe

Întrebare: Care este abordarea recomandată pentru implementarea măsurilor de securitate cibernetică la nivel organizațional?

A) Implementarea imediată a măsurilor avansate
B) Introducerea de măsuri în mod aleatoriu
C) Implementarea pe etape, începând cu practicile fundamentale
D) Bazarea exclusiv pe permisiunile angajaților

Întrebare: Ce măsură de securitate cibernetică presupune acordarea angajaților doar a permisiunilor necesare pentru rolurile lor?

A) Criptare
B) Firewalls
C) Copii de siguranță regulate
D) Configurarea permisiunilor

Răspunsurile pot fi găsite în ultimul capitol: Răspunsuri cibernetice

DACĂ AR FI SĂ REȚII CÂTEVA IDEI ESENȚIALE DIN ACEASTĂ SECȚIUNE, SĂ FIE ACESTEA:

1. Lupta Anastasiei împotriva unui virus reflectă impactul programelor malware asupra calculatoarelor, perturbând atât operațiunile normale, cât și încetinind funcționalitatea acestora.
2. Malware este un termen generic pentru diferite forme de soft-uri dăunătoare.
3. Infractorii cibernetici țintesc activiștii cu programe malware în scopul spionajului politic, al perturbării activismului, al promovării unor agende politice și sociale specifice și ca punct de intrare pentru atacuri mai ample.
4. Rămâi în siguranță prin instalarea de programe antivirus și antispyware, actualizarea permanentă a software-ului și utilizarea unui firewall.

SCENARIU PENTRU EXERCIȚIU: SIMULARE DE PHISHING ȘI RĂSPUNS PRIORITAR

Simulează un atac sofisticat de phishing care vizează angajații pentru a evalua capacitatea organizației de a detecta, răspunde și prioritiza acțiunile de securitate cibernetică.

Pași de exercițiu:

1. Simulare de e-mail de phishing:
-Trimite e-mailuri de phishing realiste unor angajați selectați la întâmplare.
-Creează scenarii care imită tacticile comune de phishing, cum ar fi solicitări urgente, oferte tentante sau deghizate în comunicări interne.

2. Răspunsurile angajaților:
-Observă cum răspund angajații la e-mailurile de phishing.
-Evaluează dacă aceștia recunosc tentativa de phishing, dacă o raportează prompt sau dacă cad victime atacului.

3. Notificarea echipei de securitate:
-Anunță echipa de securitate cibernetică despre atacul simulat de phishing.
-Evaluează timpul de răspuns și eficiența echipei în ceea ce privește analiza și confirmarea tentativei de phishing.

4. Prioritatea de răspuns la incidente:
-În funcție de gravitatea atacului de phishing, atribuie priorități acțiunilor de răspuns la incidente.
-Testează capacitatea organizației de a stabili priorități și de a aloca eficient resursele.

5. Comunicare și formare:
-Comunică angajaților incidentul simulat, subliniind importanța vigilenței față de amenințările de phishing. Oferă o formare specifică privind recunoașterea și raportarea tentativelor de phishing.

6. Analiza post-exercițiu:
-Efectuează o analiză amănunțită a exercițiului, identificând domeniile care pot fi îmbunătățite.
-Evaluează eficacitatea formării în materie de securitate cibernetică a organizației și ajustează prioritățile în consecință.

Acest scenariu pentru exercițiu se concentrează pe prioritizarea răspunsurilor la atacurile de phishing, o amenințare prevalentă în materie de securitate cibernetică. Acesta ajută organizațiile să își evalueze gradul de pregătire pentru a face față provocărilor de securitate în continuă evoluție.

> În ceea ce privește securitatea cibernetică, poți avea cea mai bună protecție (antivirus, VPN etc...) și totuși nu este suficient. Oamenii sunt veriga cea mai slabă. O singură greșeală umană poate duce la defectarea sistemului de protecție.

DAVIT GHONGHADZE, EXPERT ÎN SECURITATE CIBERNETICĂ

Câteva cuvinte de final

La încheierea acestui ghid de reziliență cibernetică, adaptat pentru organizațiile pentru drepturile femeilor din Moldova, ar trebui să fie clară intersecția crucială dintre securitatea digitală și apărarea drepturilor omului. Protejarea informațiilor sensibile și a activelor digitale nu reprezintă doar o bună practică, ci și o condiție prealabilă esențială pentru exercitarea drepturilor omului.

Peisajul în evoluție al amenințărilor cibernetice subliniază urgența cu care organizațiile pentru drepturile femeilor trebuie să cultive o schimbare de paradigmă în ceea ce privește comportamentele cibernetice. Măsurile solide de securitate cibernetică, care includ monitorizarea în timp real și soluții proactive, sunt imperative pentru a fortifica infrastructura digitală împotriva potențialelor riscuri .

Într-o lume ideală, persoane ca Anastasia și Maria s-ar putea dedica în întregime apărării drepturilor femeilor, conducerii inițiativelor de la firul ierbii și formării profesionale, fără a fi preocupate de amenințările cibernetice. Cu toate acestea, realitatea lumii noastre necesită activități paralele pentru schimbări în domeniul securității cibernetice și pentru integrarea unor practici mai sigure la nivel organizațional.

Imaginează-ți-o pe Maria și Anastasia, relaxându-se la restaurantul lor preferat după o săptămână solicitantă. După ce au efectuat o evaluare cibernetică amănunțită și au beneficiat de formare cu privire la măsurile de securitate cibernetică prioritare, acestea pot acum să își protejeze echipele, precum și beneficiarii.

Acest ghid nu este menit să insufle teamă; mai degrabă, el reprezintă o resursă practică, înarmând organizațiile pentru drepturile femeilor din Moldova cu cunoștințe și instrumente esențiale pentru a naviga în siguranță în mediul digital. În acest fel, se pot concentra asupra misiunii lor esențiale de promovare a egalității de gen și a drepturilor omului.

SINCERLEY MEDIA | UNSPLASH

Răspunsurile tale cibernetice

Capitolul: Sunt cu adevărat o țintă?

Răspuns: Răspunsul corect este A: Atac țintit pentru a-i fura datele. Identificarea unei organizații cu care colaborează Anastasia și pretinderea că o reprezintă pentru a-i trimite un e-mail înseamnă că hackerii cibernetici au făcut cercetări și au vizat-o în mod special pe Anastasia. Cerându-i să își actualizeze datele de identificare, aceștia urmăreau să îi fure numele de utilizator și parola și să îi spargă conturile.

Capitolul: Navigarea în siguranță pe internet: ai merge pe o stradă aglomerată cu geanta deschisă?

Răspuns: Răspunsurile corecte sunt: 1, 2, 4, 5, 6, 7. Singurul răspuns greșit este 3. În timp ce un e-mail cu subiectul "Confirmare abonare la newsletter" poate fi titlul unui e-mail de phishing, toate celelalte subiecte de e-mail au un sentiment de urgență și folosesc frica pentru a determina o acțiune imediată. Această manipulare emoțională este o tactică obișnuită folosită de hackeri pentru a păcăli persoanele să facă click pe link-urile de e-mail de phishing.

Capitolul: WiFi public: Un paradis pentru intruși cibernetici

Răspunsul la întrebarea 1 este C: Expunerea la intruși cibernetici. Cel mai important risc pe care îl prezintă rețelele WiFi publice este acela de a te expune intrușilor cibernetici. În unele cazuri, această expunere le permite să-ți urmărească mișcările fizice.

Răspunsul la întrebarea 2 este C: Prin stabilirea unei conexiuni securizate. VPN-ul sporește securitatea pe rețelele WiFi publice prin redirecționarea conexiunii tale la internet printr-un server privat, făcând inaccesibilă adresa IP reală și ascunzându-ți activitatea online.

Capitolul: Ce au în comun cheile de la casă și parolele?

Răspunsul la întrebarea din testul de scenariu este C: Schimbă parolele asociate cu contul compromis și activează autentificarea cu doi factori. Dacă parola ei a fost compromisă și a fost dezvăluită în cadrul unei încălcări a securității datelor, înseamnă că hackerii cibernetici au acces la numele de utilizator și la parolele ei. Maria ar trebui să schimbe imediat parola contului compromis și să activeze autentificarea cu doi factori pentru un nivel suplimentar de protecție.

Capitolul: Malware: Un virus care slăbește sistemul imunitar al computerului.

Răspunsul la întrebarea 1 este B: Observarea și furtul de informații. Scopul principal al programelor spyware este similar cu cel al spionilor digitali - de a observa în liniște și de a fura informații.

Răspunsul la întrebarea 2 este B: Pentru a perturba activismul. Hackerii se pot angaja în spionaj politic pentru a culege informații despre activiști/te, promotori/oare ai păcii și organizații lor, exploatând date sensibile pentru a perturba activismul.

Capitolul: Protejează-ți dispozitivele, organizația și beneficiarii

Răspunsul la întrebarea 1 este B: Care rezultă într-o schimbare de comportament. Scopul principal al oricărei formări în domeniul securității cibernetice este de a încuraja oamenii să își schimbe comportamentul într-un mod care să contribuie la un mediu de lucru mai sigur pentru toți angajații din organizație.

Răspunsul la întrebarea 2 este C: Implementarea pe etape, începând cu practicile fundamentale. Abordarea recomandată este de a începe pas cu pas, începând cu elementele fundamentale, cum ar fi navigarea în siguranță pe internet, recunoașterea e-mailurilor de phishing. Apoi poți trece la e-mailuri criptate, firewall-uri, VPN-uri și alte subiecte mai complicate.

Răspunsul la întrebarea 3 este D: Configurarea permisiunilor.

Surse

https://carnegieendowment.org/politika/90356

https://www.epc.eu/en/publications/Moldovas-European-future-A-call-to-open-accession-talks~544e08

https://www.gisreportsonline.com/r/moldova-russia-east/

https://www.usip.org/publications/2023/07/ukraines-edge-russia-presses-hybrid-war-tiny-moldova

https://www.german-economic-team.com/en/newsletter/war-in-ukraine-moldova-to-face-severe-economic-shock/

https://www.nrc.no/resources/reports/socio-economic-impact-on-the-moldovan-economy-since-the-war-in-ukraine/

https://reliefweb.int/report/moldova/republic-moldova-impact-war-ukraine-moldovan-returnees-abroad-data-collected-february-june-2023

https://dtm.iom.int/reports/republic-moldova-impact-war-ukraine-moldovan-returnees-abroad-feb-jun-2023

https://ega.ee/news/moldova-establishes-national-cybersecurity-agency/

https://www.marketwatch.com/press-release/moldova-fortifies-digital-defenses-with-new-cybersecurity-agency-and-cybecor-institute-21787ece

https://www.eeas.europa.eu/delegations/moldova/cybersecurity-exercise-enhances-moldova%E2%80%99s-resilience-against-cyber-threats_en

https://www.researchgate.net/publication/350476430_Cybersecurity_of_the_Republic_of_Moldova_a_retrospective_for_the_period_2015-2020

https://www.csis.org/analysis/moldovas-sisyphean-security-struggle

https://newsmaker.md/rus/novosti/sayt-midei-podvergsya-moschnoy-kiberatake-chto-rasskazali-v-pravitelstve/?utm_source=substack&utm_medium=email

https://newsmaker.md/rus/novosti/sayt-midei-podvergsya-moschnoy-kiberatake-chto-rasskazali-v-pravitelstve/?utm_source=substack&utm_medium=email

https://therecord.media/hackers-target-govts-with-zimbra-zero

https://my.rusi.org/resource/battening-down-the-hatches-moldovas-cyber-defence.html

https://www.marketwatch.com/press-release/moldova-fortifies-digital-defenses-with-new-cybersecurity-agency-and-cybecor-institute-21787ece

https://jfj.fund/attacks-on-media-workers-in-moldova-in-2022/

https://www.state.gov/drl-strengthening-resilience-for-digital-security-providers-and-capacity-for-civil-society-in-ukraine-and-moldova/

https://data.unhcr.org/fr/documents/download/106557

https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf

https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights

https://iwpr.net/global-voices/moldovans-face-bomb-threats-and-cyberattacks

https://gc3b.org/cyber-impact-stories/cyber-impact-stories-women-in-cyber-fellowship/

https://just-access.de/the-issue-of-domestic-violence-in-the-republic-of-moldova/

https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations

https://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma

https://www.amnesty.org/en/latest/campaigns/2015/08/how-governments-are-using-spyware-to-attack-free-speech/

https://tech.co/password-managers/how-long-hacker-crack-password#:~:text=A%2010%2Ddigit%20password%20that,hacker%20up%20to%20two%20weeks

https://www.verveit.com/blog/is-your-password-strong-enough/

https://www.cobalt.io/blog/cybersecurity-statistics-2024

https://www.comparitech.com/antivirus/malware-statistics-facts/

https://terranovasecurity.com/blog/cyber-security-statistics/

https://www.linkedin.com/pulse/breaking-down-tactics-used-hackers-exploit-womens-rights-middle

https://www.sciencedirect.com/science/article/pii/S245195882200001X

https://www.ibm.com/topics/threat-actor

INSTITUTE FOR
WAR & PEACE REPORTING

I W P R

iwpr.net

IWPR United Kingdom
48 Gray's Inn Road,
London WC1X 8LT
Tel +44 (0)20 7831 1030

IWPR United States
1156 15th Street NW Suite 329,
Washington, DC 20005
Tel +1 202 393 5641

IWPR Netherlands
iwpr-nl@iwpr.net