SERVICIUL TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

GHID
de securitate cibernetică
pentru funcționarii publici

Elaborat de: Centrul de răspuns la incidente cibernetice CERT-GOV-MD
din cadrul I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”

2018

SERVICIUL TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

CUPRINS

1. INTRODUCERE

1.1 Context

Mediul virtual, generat de infrastructurile cibernetice, este deja o parte integrantă a vieții personale și profesionale. Noile tehnologii implică însă noi riscuri care pot afecta grav individul sau organizația, însă securitatea cibernetica este un element luat în calcul mult prea rar.

Este important ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rândul angajaților, înțelegerea tipologiei amenințărilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

Efectuarea controalelor interne care să asigure un grad corespunzător de securitate activelor informaționale ale unei instituții presupune o planificare riguroasă și identificarea exactă a obiectivelor respectivei instituții. Pentru a fi însă eficiente aceste controale trebuie să vizeze toți angajații și nu doar pe cei din compartimentul IT sau care au legătură directă cu acest domeniu.

Totuși, asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, o contribuție importantă revenind factorului uman calificat și pregătit. Majoritatea incidentelor de securitate sunt generate de o gestiune și organizare necorespunzătoare, și mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Dat fiind faptul că majoritatea datelor prelucrate și stocate de către instituțiile de stat reprezintă informații confidențiale, angajații din domeniul public sunt responsabili să asigure gestionarea datelor și informațiilor sensibile în conformitate cu **Cerințele minime obligatorii de securitate cibernetică**, inclusiv alte prevederi legislative în vigoare.

Datorită utilizării extensive în prezent a dispozitivelor mobile, atât pentru uz personal cât și pentru desfășurarea activităților specifice locului de muncă, angajații trebuie să se asigure de faptul că acest proces se desfășoară în concordanță cu politicile și liniile directoare ale instituției angajatoare.

1.2 Scop

Scopul acestui ghid este de a familiariza funcționarii publici cu modul în care ar trebui implementate și folosite tehnicile, instrumentele și mecanismele de securitate astfel încât să fie respectate normele de securitate în rândul angajaților care asigurată securitatea informației în cadrul instituției.

Acest ghid își propune să sintetizeze o serie de informații cu privire la riscurile existente și prezintă câteva metode utile pentru a determina reflexe simple pentru folosirea în siguranță a sistemelor

informatice, pentru a veni în întâmpinarea nevoilor tale de cunoaştere, atât în calitate de cetăţean, utilizator al tehnologiei moderne, cât şi în calitate de funcţionar (public sau nu) care utilizează infrastructura cibernetică a unei organizații, din moment ce, în ambele ipostaze, suntem toți dependenţi de resurse informatice şi de comunicaţii.

1.3 Obiective

Ghidul de securitate informatică pentru funcționarul public își propune următoarele obiective:

- Creșterea confidențialității, integrității și disponibilității datelor și informațiilor vehiculate în cadrul sistemelor informatice și de comunicații utilizate de funcționarii publici;
- Oferirea mijloacelor de ghidare și susținere a activității referitoare la securitatea informației în cadrul instituțiilor, prin definirea de controale și măsuri ce vizează identificarea și reducerea riscurilor și vulnerabilităților de securitate manifestate în cadrul acestora.

2. AMENINȚĂRI PRIVIND SECURITATEA INFORMAȚIILOR

Cele mai întâlnite tipuri de amenințări cibernetice sunt:

- **PHISHING**. Phishing-ul este o formă de înșelăciune în mediul online care constă în folosirea unor tehnici de manipulare a identității unor persoane/organizații pentru obținerea unor avantaje materiale sau informații confidențiale. Atacatorii folosesc diverse tehnici de social engineering pentru a determina victimele să dezvăluie date de autentificare. Țintele cele mai întâlnite sunt site-urile instituțiilor financiare, precum băncile. Alte ținte sunt reprezentate de serviciile de plată online, rețelele de socializare, furnizorii de servicii de internet, organizațiile non-profit, servicii de coletărie sau site-urile unor sectoare guvernamentale
- **SPAM**: mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase, folosite de industria emarketingului și de proprietarii de site-uri cu un conținut indecent. Mesajele spam sunt trimise cu ajutorul unor calculatoare infectate cu troieni, care fac parte dintr-un botnet (o rețea de calculatoare compromise utilizate pentru trimiterea de spam sau atacuri asupra unor site-uri pe internet, fără știrea posesorilor calculatoarelor respective). Mesajele spam, deși nu sunt un program malițios în sine, pot include atașamente care conțin astfel de programe, sau trimit utilizatorii către pagini de internet periculoase pentru siguranța sistemului.
- **VIRUȘI**: virușii informatici sunt programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componente ale sistemului de operare sau alte programe informatice.
- **VIERMI**: programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii pe alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, pe când virușii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.
- **TROIENI**: aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat.
- **SPYWARE**: o categorie de software malițios, atașate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de video chat etc.), care captează pe ascuns date de marketing (prin analiza site-urilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ș.a.m.d.) și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare, dar nesolicitate.

- **ADWARE**: orice program care afișează reclame la rularea acestuia, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up (care deschide ferestre noi cu reclame, deasupra tuturor ferestrelor). Unele programe adware pot fi considerate o formă de spyware care nu colectează date de marketing, ci doar transmit reclame.
- **ROOTKIT**: un rootkit este o colecție de utilitare proiectate să mențină controlul sau accesul la calculator. După instalare, rootkit-ul utilizează funcții ale sistemului de operare pentru a se "ascunde" astfel încât să rămână nedetectat. Rootkit-urile au fost utilizate mai întâi în Unix, dar sunt folosite în prezent și în Linux, Windows și alte sisteme de operare. Acestea pot fi folosite în scopuri legale, dar sunt cunoscute în general pentru utilizarea lor în scopuri malițioase.
- **HACKER**: o persoană care pătrunde în calculatoare (fără acordul proprietarului), de obicei prin accesarea controalelor administrative.

3. CADRUL DE MANAGEMENT AL SECURITĂȚII CIBERNETICE

3.1 De unde se începe?

Controalele interne pot fi considerate principiile care stau la baza implementării unui sistem de management al securității. Chiar dacă sursele unor astfel de măsuri pot fi destul de variate, punctul de plecare într-un astfel de demers îl reprezintă legislația aplicabilă. Este foarte important ca cel care se ocupă de implementarea unui sistem de management al securității să dețină cunoștințe despre actualele cerințe legislative.

Pe lângă legislația internă trebuie considerate și standardele internaționale (ex.: ISO/IEC 27001:2013), care răspund necesităților organizațiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securității informațiilor.

Selectarea controalelor trebuie să țină cont de specificul organizației. Nu toate recomandările pot fi aplicate, cum nu toate sunt justificate din punct de vedere al costurilor. Eficacitatea sistemului de securitate depinde de:

- Stabilirea unor obiective de securitate care să reflecte cerințele organizației;
- Sprijinul conducerii;
- Existența abilităților necesare realizării analizei riscurilor, a vulnerabilităților și a analizei de impact;
- Instruirea angajaților;
- Monitorizată controalelor implementate.

3.2 Politica de securitate

Obiectivul politicii de securitate este să ofere managementului instituției sprijinul necesar asigurării securității informațiilor din cadrul organizației.

Conducerea oricărei instituții trebuie să ofere suportul necesar prin elaborarea unui document întitulat Politică de Securitate, document care trebuie adus la cunoștința tuturor angajaților.

Fără un astfel de document există riscul ca rolurile și responsabilitățile relative la asigurarea securității informaționale să fie greșit înțelese. Nedezvoltarea unui astfel de document și neaducerea la cunoștința angajaților a politicii de securitate a companiei induce de cele mai multe ori o stare de superficialitate în tratarea acestor aspecte. Existența unei viziuni clare a conducerii și o comunicare efectivă a acesteia către angajați este fundamentală pentru asigurarea eficienței oricăror proceduri și măsuri de securitate specifice.

3.3 Organizarea securității

Organizarea securității are ca obiectiv asigurarea unei administrări unitare în cadrul organizației.

Fiecare utilizator al sistemului informațional este responsabil cu asigurarea securității datelor pe care le manipulează. Existența unei structuri organizatorice unitare care să inițieze și să controleze implementarea mecanismelor de securitate în cadrul organizației, presupune un punct central de coordonare – responsabil cu securitatea.

Rolul și atribuțiile persoanei care ocupă poziția de responsabil cu securitatea informațiilor se referă la coordonarea și urmărirea respectării procedurilor și politicilor de securitate.

Organizarea securității nu se limitează doar la personalul intern, trebuie avute în vedere și riscurile induse de terți sau subcontractori care au acces la sistemul informațional. Acest risc nu este deloc de neglijat, ultimele tendințe ale pieței globale ne arată o reconsiderare a poziției companiilor fată de externalizarea funcțiilor IT, tocmai datorită riscului mare indus de subcontractarea acestora.

Obiectivul organizării securității, documentat în standard, este menținerea securității tuturor facilităților IT și activelor informaționale accesate de către terțe persoane, fiind recomandată stabilirea unui proces prin care accesul terților să fie controlat.

3.4 Clasificarea şi controlul activelor

Măsurile de protecție sunt proiectate în funcție de gradul de sensibilitate, și de semnificația economică a resurselor vizate. Perimetrele în care sunt amplasate echipamentele de procesare, vor fi protejate cu bariere de acces suplimentar. La fel și telecomunicațiile cu un nivel ridicat de confidențialitate ar trebui criptate. Pentru a avea totuși o abordare coerentă asupra măsurilor specifice de protecție, în funcție de gradul de sensibilitatea al fiecărei resurse în parte se practică o clasificare a informațiilor.

Clasificarea informațiilor este necesară atât pentru a permite alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potențiale care pot să apară ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Obiectivul clasificării este crearea premiselor necesare asigurării unei protecții corespunzătoare valorii activelor instituției. Toate activele organizației trebuie să fie asociate unui proprietar. Politica de securitate trebuie să identifice angajații cu rol de proprietar, custode, client, utilizator.

3.5 Securitatea personalului

Cele mai multe incidente de securitate sunt generate de personal din interiorul organizației, prin acțiuni rău intenționate sau chiar erori sau neglijență în utilizarea resurselor informaționale.

Standardul ISO/IEC 27001:2013 tratează riscurile de natură umană ce pot fi induse din interiorul organizației prin măsuri specifice precum includerea responsabilităților legate de securitatea informațiilor în descrierea și sarcinile de serviciu ale postului, implementarea unor politici de verificare a angajaților, încheierea unor acorduri de confidențialitate și prin clauze specifice în contractele de muncă.

Securitatea informațiilor este un aspect ce trebuie avut în vedere încă din etapa de selecție a angajaților. Angajații trebuie monitorizați pe întreaga perioadă de valabilitate a contractului de muncă și trebuie să ia cunoștința cu prevederile politicilor de securitate. Clauzele de confidențialitate, definirea conflictelor de interese, distribuirea și divulgarea informațiilor trebuie luate în considerație pentru fiecare post în parte.

Pentru a evita neglijența sau greșelile de operare, utilizatorii ar trebui informați cu privire la amenințările la care sunt supuse informațiile manipulate. Instruirea ar trebui să ofere cunoștințele necesare asigurării securității acestora în timpul programului normal de lucru.

Utilizatorii trebuie instruiți cu privire la procedurile de securitate ce trebuie urmate și utilizarea facilităților IT în conformitate cu politica organizației.

Ar trebui să existe un program coerent de instruire a angajaților pe diverse niveluri de interes, pe lângă o instruire generală în gestiunea securității fiind necesare și specializări pentru administratorii sistemului informatic în tehnologii de securitate specifice.

Chiar dacă securitatea unei anumite zone IT, cum ar fi securitatea rețelei revine unei entități externe, este o practică bună ca și în interiorul organizației să existe competențele și abilitatea de a evalua cum sunt satisfăcute cerințele de securitate.

Instruirea este necesară și pentru a crea abilitatea de reacție la apariția unor incidente de securitate. Raportarea incidentelor de securitate are ca obiectiv minimizarea efectelor negative sau a incorectei funcționări echipamentelor. Monitorizarea unor astfel de incidente permite determinarea performanței sistemelor de securitate și îmbunătățirea continuă.

Politicile și procedurile de securitate trebuie implementate astfel încât să asigure un răspuns consistent la astfel de incidente.

3.6 Securitatea fizică

Delimitarea zonelor securizate are ca obiectiv prevenirea accesului neautorizat sau afectarea facilităților oferite de sistemul informațional. Această secțiune vizează mecanismele prin care se asigură securitatea fizică a imobilului în care organizația își desfășoară activitatea.

Alt aspect important al securității fizice este cel legat de protecția echipamentelor, prin prevenirea pierderii, distrugerii sau compromiterii funcționării echipamentelor care pot afecta funcționarea organizației.

Echipamentele de calcul trebuie să fie protejate fizic împotriva amenințărilor intenționate sau accidentale. În acest sens trebuie dezvoltate standarde și proceduri pentru securizarea atât a serverelor, cât și a stațiilor de lucru ale utilizatorilor.

Măsurile de control al accesului, implementate la nivelul aplicației, bazelor de date sau rețelei pot deveni inutile dacă există și o protecție fizică corespunzătoare.

3.7 Politica de securitate

Confidențialitatea vizează protejarea informațiilor împotriva oricărui acces neautorizat. Uneori este interpretat în mod greșit că această cerință este specifică domeniului militar și serviciilor de informații care trebuie să-și protejeze planurile de luptă, amplasamentul depozitelor de muniție sau al rachetelor strategice, notele informative. Este însă la fel de importantă pentru o organizație care dorește să-și apere proprietatea intelectuală, rețetele de producție, datele despre personalul angajat, etc. Pentru o instituție publică, datorită caracterului informației pe care o gestionează este important să asigure în primul rând integritatea și disponibilitatea datelor.

Controlul accesului începe cu stabilirea cerințelor de acordare a drepturilor de utilizare a informațiilor.

Accesul la facilitățile și serviciile oferite de sistemul informațional trebuie controlat în funcție de specificul și cerințele mediului în care își desfășoară activitatea organizația.

Pentru a răspunde acestor cerințe sunt în general definite o serie de reguli de acces corelate cu atribuțiile fiecărui utilizator al sistemului informatic.

Menținerea acestor reguli în linie cu cerințele organizației implică un proces de gestiune a accesului utilizatorilor sistemului. Obiectivul acestui proces este să prevină utilizarea neautorizată a calculatoarelor.

Trebuie să existe proceduri formale prin care să se controleze alocarea drepturilor de acces la serviciile și resursele IT.

4. REGULI DE UTILIZARE ACCEPTABILE

4.1 Reguli privind utilizarea stațiilor de lucru

Pentru a asigura integritatea calculatorului și a datelor personale, vă recomandăm respectarea următoarelor reguli:

- Indiferent de sistemul de operare pe care îl folosiți, este de a activa mecanismele automate de actualizare (update) ale sistemului de operare;
- Instalați o soluție de securitate ce oferă cel puțin protecție de tip antivirus, antimalware, antispam și antiphishing. O soluție completă de securitate trebuie să ofere și capabilități de tip firewall și IPS (Intrusion prevention systems), de prevenire a atacurilor și de navigare securizată. Aceste servicii, utilizate împreună, pot oferi o apărare stratificată împotriva celor mai frecvente amenințări. Multe dintre aceste soluții oferă și un serviciu care verifică site-urile pe care le accesați, având un istoric al reputației domeniilor web care au avut vreodată un rol în răspândire a malware;
- Nu uitați să activați orice serviciu de actualizare automată a acestor softuri de securitate pentru a vă asigura că folosiți ultimele versiuni de semnături ale programelor antimalware;
- Evitați pe cât posibil folosirea contului de administrator al sistemului de operare. Este necesară crearea unui cont de utilizator care să nu dețină toate privilegiile specifice contului de

administrator. Acest cont va fi folosit pentru activitățile uzuale, cum ar fi web-browsing, crearea sau editarea de documente, accesul la e-mail etc. Contul de administrator ar trebui folosit numai atunci când se fac actualizări de software sau când este necesară reconfigurarea sistemului. Navigarea pe web sau accesul la e-mail folosind contul de administrator este riscantă, oferind ocazia atacatorilor să preia controlul asupra sistemului;

- Folosiți versiuni ale aplicațiilor de tip Office cât mai recente. În versiunile mai recente, formatul de stocare al documentelor este XML, un format care nu permite executarea de cod la deschiderea unor documente, astfel protejând utilizatorii de malware-ul ce folosește ca mod de propagare astfel de documente. Unele din versiunile cele mai recente oferă o facilitate de tip "protected view", deschizând documentele în modul "read-only", astfel eliminând o serie de riscuri generate de un fișier infectat;
- Actualizați-vă software! Majoritatea utilizatorilor nu au timpul sau răbdarea de a verifica dacă aplicațiile instalate pe computer sunt actualizate. De vreme ce există multe aplicații ce nu au capabilități de auto-actualizare, atacatorii vizează astfel de aplicații ca mijloace de a prelua controlul asupra sistemului;
- Utilizați parole complexe. Ca o regulă generală, toate parolele asociate cu orice cont de utilizator ar trebui să posede cel puțin 10 caractere și să fie complexe, în sensul de a include caractere speciale, cifre, litere mici și litere mari;
- Nu instalați software-ul dorit din locații despre care nu sunteți sigur, mai ales software care pare să fie de tip codec (program sau o bibliotecă de software, eventual chiar și un aparat hardware corespunzător, care asigură codarea și decodarea unei informații). În schimb, accesați pagina producătorului pentru a descărca acest tip de program.
- Fiți precauți referitor la apelurile telefonice nesolicitate, vizite, sau e-mailuri de la persoane care solicită informații despre angajați sau companie. În cazul în care o persoană necunoscută pretinde a fi de la o organizație legitimă, încercați să verificați identitatea acestuia, în raport cu organizația respectivă. Nu oferiți informații personale sau informații despre organizația dvs., inclusiv structura sau rețelele sale, dacă nu sunteți sigur de autoritatea unei persoane de a avea informațiile.

4.2 Reguli privind securizarea conturilor de e-mail

Conturile de e-mail, atât cele web-based, cât și cele locale, sunt ținte vizate de atacatori. Următoarele recomandări se pot dovedi utile pentru a reduce riscurile legate de acest serviciu:

- Nu accesați imaginile sau link-urile din e-mailurile dubioase. Un e-mail poate conține o imagine sau link, care la accesare va aduce utilizatorul pe un site malițios. Dacă identitatea celui care a trimis respectivul e-mail nu poate fi verificată, sfatul este de a șterge acel e-mail fără a-l

deschide pentru a-i vedea conținutul. Nu răspundeți la e-mailuri care vă solicită date cu caracter personal.

- Setați e-mailul dvs. în așa fel, încât acesta să vă afișeze e-mailurile în format de text simplu, și nu în format HTML, astfel veți diminua riscul să fiți trucați cu substituirea link-ului pe altul decât acel afișat în email.
- Asigurați-vă că email-urile partenerului dvs. sunt semnate digital, în scopul de a preveni falsificarea acestora;
- Aveți în vedere că este periculos să deschideți orice atașament, chiar și documentele Microsoft Word și PDF pot conține viruși, nu doar acele care au la sfârșit extensia de".exe".
- În cazul în care dvs. totuși doriți să deschideți documentul PDF sau Word:
    a) Dacă este posibil contactați expeditorul email-lui prin telefon sau în oricare alt mod.
    b) Asigurați-vă că Sistemul de operare al calculatorului dvs. și baza de date a antivirusului este actualizată.
    c) De asemenea pentru a evita orice risc, dvs. puteți utiliza un soft destinat convertirii PDF-ului într-un format inofensiv ".html", spre exemplu "pdftohtml", sau puteți recurge la Google Drive, pentru online vizualizarea securizată a documentului .
- Setarea unor mesaje de genul “out-of-office” pentru contul personal de e-mail nu este recomandată, fiind o sursă prețioasă de informații pentru spammeri și confirmând faptul că este o adresă de e-mail validă;
- Folosiți întotdeauna protocoale securizate atunci când accesați e-mailul (IMAPS, POP3S, HTTPS), mai ales atunci când folosiți o rețea wireless. Majoritatea clienților de email suportă aceste protocoale, prevenind astfel o interceptare a emailului atunci când este în tranzit între computerul dumneavoastră și serverul de e-mail;
- Nu vă lăsați amăgiți de probleme privind cardul de credit, sau invitații diverse care provin din partea unor surse necunoscute. Atunci când găsiți astfel de mesaje în Inbox, luați legătura cu banca (sau mergeți personal la bancă) pentru a vă asigura ca totul este în regulă referitor la contul dumneavoastră;
- Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin atașamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informații;
- Este greu de imaginat că o agenție guvernamentală v-ar contacta prin Internet pentru a colecta o amendă, așadar, tratați astfel de mesaje cu suspiciune, și sub nici o formă nu accesați link-urile sau atașamentele conținute de mesajul respectiv. În această situație, chiar și existența unei soluții de securitate eficiente, factorul uman joacă un rol decisiv. Ingineria socială poate ajuta un hacker sau un program să stabilească o conexiune cu utilizatorul, și convingerea acestuia în a oferi date critice sau bani. De asemenea, încercați să contactați un reprezentant al instituției, care să vă ofere cât mai multe informații posibil.

4.3 Reguli pentru navigare sigură pe Internet

Browserele sunt programele folosite pentru navigarea pe internet. Ele permit accesarea și vizualizarea site-urilor, navigarea prin link-uri, descărcarea de fișiere de pe internet etc. Pentru a reduce riscurile legate de navigarea pe internet, ar trebui respectate următoarele recomandări:

- Evitați să accesați link-uri care sunt marcate drept periculoase de către soluția de securitate instalată pe sistem, sau de către browser-ul de internet. Dacă primiți orice mesaj de atenționare în timpul navigării pe o pagină, ieșiți imediat de pe respectiva pagină de internet;
- Dezactivați executarea scripturilor în browsere. Dacă folosiți anumite browsere, puteți folosi opțiunea / NotScript sau plugin-uri pentru a nu permite execuția de scripturi ce provin de pe site-uri necunoscute. Dezactivarea execuției de scripturi poate cauza probleme de folosire facilă a browserului, dar este o tehnică foarte eficientă pentru a elimina o serie de riscuri legate de execuția acestor scripturi;
- Verificați în mod regulat actualizările pentru web-browser, „Flash Adobe” și „Java”.
- Asigurați-vă că folosiți un antivirus cu posibilități de "antiphishing" și "web-antivirus".
- Nu uitați că mesajele Popup care cer actualizarea softului "Adobe Flash Player", "Java" sau a altor softuri, pot fi false. Din acest considerent, este important întotdeauna să închideți aceste ferestre, iar toate actualizările necesare trebuie instalate manual de pe site-urile oficiale ale producătorilor.
- Niciodată nu salvați parolele conturilor dvs. în browser-ele web.
- Utilizați modul „Privat” de navigare al browser-ului dvs. în rețeaua internet.
- În cazul în care, nu sunteți siguri în securitatea unui link, e mai bine să nu îl accesați.

4.4 Reguli privind utilizarea echipamentelor portabile de tip laptop

Regulile de utilizare a echipamentelor portabile de tip laptop sunt similare cu cele privind utilizarea stațiilor de lucru. Suplimentar, având în vedere caracterul mobil al acestor dispozitive, ar trebui respectate următoarele recomandări:

- Este recomandat să aveţi tot timpul controlul asupra laptop-urilor deoarece acestea pot fi ţinta unui atac dacă un atacator ar avea acces la ele. Dacă sunteţi nevoit să lăsaţi, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit şi să aibă discurile criptate. Sistemele de operare recente oferă nativ capabilitatea de criptare a discurilor prin mecanisme proprii. Pentru versiuni mai vechi, dar și pentru celelalte există produse care implementează acest serviciu. Astfel, puteţi evita accesul neautorizat la informaţii confidenţiale, în caz că laptop-ul este pierdut sau furat;

În diverse locuri (cafenele, hoteluri, aeroporturi etc.) se găsesc hotspot-uri wireless sau chioşcuri care oferă servicii internet clienţilor. Având în vedere că infrastructura ce deserveşte aceste reţele este una necunoscută şi că adeseori, securitatea nu e o preocupare în aceste locuri, există o serie de riscuri pentru a le contracara, iată câteva recomandări:

- Dispozitivele mobile ar trebui să fie conectate la internet folosind reţelele celulare (mobile Wi-Fi, 3G sau 4G), această modalitate fiind de preferat în locul hotspot-urilor;
- Dacă se foloseşte un hotspot Wi-Fi pentru accesul la internet, indiferent de reţeaua folosită, utilizatorii pot seta un tunel VPN către un furnizor de încredere pentru acest gen de servicii, protejând astfel tot traficul de date efectuat şi prevenind activităţi răuvoitoare cum ar fi interceptarea traficului;
- Dezactivați funcția ”Network Share” înainte de a vă conecta la un hotspot public;
- Utilizați o aplicație firewall care să filtreze accesul din exterior;
- Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa internetul, este recomandat să vă rezumaţi doar la navigarea pe web şi să evitaţi să accesaţi servicii unde trebuie să vă autentificaţi, deci să furnizaţi date de genul user/parolă;
- Evitați să faceți shopping online atunci când sunteți conectați la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri.

  - De obicei, informațiile schimbate între dumneavoastră și magazinul online, nu sunt criptate, și pot fi interceptate ușor de către un atacator; -Nu folosiți niciodată calculatoare publice pentru a efectua tranzacții bancare, sau pentru alte tipuri de achiziții online. Aceste calculatoare ar putea conține programe care înregistrează datele personale, precum troienii bancari.

4.5 Reguli privind utilizarea echipamentelor portabile de tip tabletă şi a telefoanelor inteligente

În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite și necesită o abordare specială. Principalele probleme care pot apărea, sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, furtul informații sensibile și direcționarea utilizatorilor către site-uri și documente compromise. Următoarele reguli vor contribui la reducerea riscurilor:

- Actualizați-vă sistemele de operare pentru dispozitivele mobile. Este recomandat să faceți acest lucru atunci când apar versiuni noi și să verificați acest lucru periodic.
- Sunteți mult mai vulnerabili atunci când utilizați dispozitivele mobile (telefon, tabletă etc.) în timpul unor călătorii, deoarece amenințările, sunt probabil mai prezente în rețelele publice din aeroporturi, gări, obiective turistice etc.

- Protejați-vă telefonul/tableta cu parole și opțiuni de criptare. În cazul în care cineva vă fură sau vă găsește telefonul/tableta, îngreunați-i accesul la informațiile stocate
- Folosiți o soluție de securitate care să aibă un modul antifurt, în mod special dacă folosiți un echipament care rulează Android. În cazul în care pierdeți echipamentul sau vă este furat, modulul antifurt vă poate ajuta să identificați și să îl recuperați. De asemenea acesta poate fi utilizat pentru a bloca echipamentul sau pentru a șterge informațiile de pe el de la distanță. În cazul telefonului aceste operații pot fi efectuate chiar dacă acesta nu are acces la internet, un simplu SMS putând fi utilizat pentru blocarea acestuia sau pentru ștergerea informațiilor personale;
- Sincronizați-vă telefonul/tableta cu un calculator personal. În cazul în care pierdeți aceste echipamente sau vă sunt furate, veți avea o copie de siguranță a contactelor, mesajelor, imaginilor și documentelor stocate pe acestea;
- Accesați doar hotspot-uri sigure. Asigurați-vă că opțiunile de conexiune prin infraroșu, Wi-Fi și Bluetooth-ul sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil;
- Fiți atenți ce aplicații descărcați și de unde. Să fie descărcate numai din magazinele oficiale ale operatorilor și producătorilor precum Google Play, Apple App Store sau Microsoft Store. Soft-urile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta și pot trimite mai departe, unor terțe părți informații private. În zone necunoscute, ați putea fi tentați să descărcați aplicații care să vă ajute să găsiți diferite locații precum restaurante, hoteluri sau muzee. Aveți însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea din greșeală a aplicațiilor nesigure, verificați configurația terminalului accesând SETĂRI, SECURITATE și asigurându-vă că opțiunea SURSE NECUNOSCUTE este nebifată.
- Fiți atenți la ofertele prea bune pentru a fi reale. Dacă primiți dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la prețuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignorați-le. Un click pe linkurile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completați formulare cu informații personale. Nu uitați de asemenea că telefonul/tableta dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website;
- Când folosiți rețelele sociale, asigurați-vă că fotografiile făcute cu smartphone-ul și pe care doriți să le încărcați pentru a le partaja cu prietenii, nu conțin informații legate de poziția dumneavoastră actuală. Partajarea locației e ideală pentru întâlnirile cu amicii în locuri publice, dar în același timp, permit persoanelor rău-intenționate să vă monitorizeze obiceiurile și rutina zilnică facilitând tentativele de hărțuire.

4.6 Reguli de folosire a propriilor dispozitive la muncă

Majoritatea instituțiilor permit angajaților introducerea propriilor dispozitive mobile în sediu și folosirea acestora în desfășurarea activității. Pentru securitatea dumneavoastră și a rețelei instituției în care lucrați, vă sfătuim să urmați aceste reguli:

- Informați departamentul IT de faptul că aveți un dispozitiv personal pe care doriți să-l folosiți la serviciu. Echipa IT vă va introduce dispozitivul în rețeaua instituției și vă va informa asupra regulilor de utilizare și întreținere a echipamentului în interiorul instituției;
- Anunțați de urgență pierderea unui dispozitiv mobil pe care aveți date care aparțin instituției. Acest lucru este esențial pentru limitarea accesului unei persoane neautorizate la aceste informații. În cazul pierderii, echipa IT vă va ghida cum să vă ștergeți de la distanță conținutul telefonului;
- Nu uitați că un smartphone e și un dispozitiv de stocare portabil. Scanați conținutul memoriei interne și externe a telefonului la fiecare introducere în calculatorul de serviciu cât și în cel de acasă. In acest fel, nu veți transfera viruși de la serviciu, acasă și viceversa;
- Din același motiv, nu introduceți nici un dispozitiv de stocare găsit (de exemplu, USB stick, CD/DVD-ROM, card SD) în calculatoarele instituției. Majoritatea atacurilor asupra rețelei instituțiilor încep cu un astfel de dispozitiv "uitat" de atacator în lift, în parcare sau în locuri din instituție în care e permis accesul personalului de întreținere sau a publicului (recepții, spații de aprovizionare etc).

4.7 Protecţia datelor pe durata călătoriilor (deplasărilor de serviciu)

Utilizarea dispozitivelor mobile (laptop, smartphone, tabletă) este importantă în cazul călătoriilor profesionale, simplificând transportul și schimbul de date. Există totuși o serie de riscuri în condițiile în care datele vehiculate sunt sensibile - date a căror pierdere sau furt pot genera consecințe importante asupra activităților organizației.

Pentru a vă proteja datele, vă recomandăm să respectați următoarele reguli, înaintea de plecarea în delegație:

- Nu folosiţi decât echipamente dedicate delegației (laptop, telefon, suporți de memorie) și care conțin doar strictul necesar de date;
- Realizaţi un back-up al datelor pentru a le putea restaura în caz de pierdere;

- Dacă trebuie să lucraţi în timpul călătoriei, folosiţi un filtru de protecție pentru ecran și o conexiune securizată pentru accesarea resurselor companiei de la distanță;
- Aplicaţi un semn distinctiv dispozitivelor Dvs., pentru a fi siguri că nu a avut loc o substituire;
- Nu permiteţi salvarea parolelor;
- Ștergeți istoricul conexiunilor de pe tabletă / telefon; acestea ajută un potențial agresor să identifice o serie de date despre tine (locații, obiceiuri, cerc relațional etc.)

Pe perioada aflării în delegație este important să:

- Păstraţi dispozitivele (echipamentele și suporții de memorie) permanent asupra Dvs;
- Dezactivaţi funcțiile Wi-Fi și Bluetooth;
- Îndepărtaţi cartela SIM și bateria dacă trebuie să lasaţi telefonul nesupravegheat;
- Informaţi reprezentanții organizației pe care o reprezentați în caz de inspecție a bagajelor sau de confiscare a dispozitivelor de către autorități străine;
- Nu folosiți echipamente primite cadou dacă nu le puteți verifica înainte;
- Evitaţi conectarea echipamentelor persoanle la cele ale altor entități. Dacă trebuie să extrageţi fișiere (prezentări etc.) din laptop, folosiţi un stick USB dedicat, pe care îl veţi formata ulterior cu un software specializat;
- Nu permiteţi conectarea altor echipamente (smartphone, stick USB, MP3 player, cameră foto etc.) la cele cu care călătoriţi;
- Este recomandat să utilizaţi modemuri mobile, provenite de la operatori de telefonie mobilă;
- Implementaţi mecanismele software de dezactivare de la distanţă a dispozitivului mobil şi de protejare a informațiilor stocate împotriva intruziunii, în cazul unei pierderi sau al unui furt.

La întoarcerea din delegație, recomandabil este să:

- Ștergeți istoricul apelurilor și al navigației GPS;
- Schimbaţi parolele folosite pe durata delegației;
- Predaţi echipamentele la verificare, dacă este posibil;
- Nu folosi/scana/verifica stick-uri de memorie/telefoane/laptop-uri/tablete/cd-uri cu prezentări/servicii VPN/VPS care v-au fost oferite pe durata delegației deoarece ar putea conține software malițios.

5. MĂSURILE DE SECURITATE

5.1 Spyware

Utilizatorii sunt sfătuiți să raporteze cazurile de activitate suspicioasă pe stațiile de lucru, cum ar fi, apariția excesivă a ferestrelor de tip pop-up, performanța extrem de slabă a computer-ului sau un browser de Internet extrem de lent, care ar putea fi redirectat către site-uri nelegitime sau nedorite, precum cele pornografice sau cele de pariuri online. În astfel de cazuri trebuie să vă adresați pentru asistență Departamentului IT, și să raportați suspiciunea că stația dvs. a fost infectată cu spyware.

Programele de tip spyware sunt scrise cu scopuri malițioase. Ele se pot afișa extrem de simplu, ca niște ferestre de tip pop-up extrem de enervante, care au menirea să îți distragă atenția sau să te atragă către site-uri malițioase. Totodată, pot fi software-uri care înregistrează obiceiurile din browser-ul pe care îl folosești pentru navigarea pe Internet sau chiar intrările de la tastatură (keylogger), cu intenția de a capta credențiale de acces sau parole.

Cum vă protejați de spyware

- Încercați să evitați accesarea site-urilor necunoscute și să le frecventați pe cele de încredere.
- Nu descărcați niciodată deliberat, software de pe Internet pe stația de lucru, indiferent cât de productiv sau interesant pare. Chiar și inofensivele bare de instrumente sau utilități pot conține spyware. Atenție sporită la programe de tip file-sharing, pe care oricum nu ar trebui să le utilizați la birou;
- Stați departe de orice site-uri dubioase, inclusiv pornografie, jocuri de noroc, hacking sau alte site-uri suspicioase/ne-convenționale. În orice caz, nu ar trebui să vizitați astfel de site-uri în desfășurarea atribuțiilor de serviciu;
- Oricând apare o fereastră pop-up nedorită sau neașteptată, închideți-o imediat apăsând pe semnul X din partea dreapta sus a ferestrei. Niciodată nu dați click pe orice buton afișat, chiar dacă afișează mesajul “CANCEL” sau “CLOSE” pe fereastra în sine. Aceste butoane pot avea în spate o comandă pentru descărcare nedorită de spyware;
- Fiți suspicioși în momentul în care numeroase ferestre pop-up încep să se afișeze pe ecranul computer-ului, sau dacă performanța sistemului este sesizabil afectată. Din acel moment puteți presupune că ați fost infectat cu spyware și va trebui să vă adresați departamentului IT;
- Dacă folosiți Internet Explorer ca browser, schimbați setările pentru a bloca Active X. Mergeți la TOOLS > Internet Options > Security > Custom Level. În această fereastră există o secțiune în partea de sus, dedicată controalelor Active X. Aici vă sfătuim să dezactivați descărcarea de Active X cu sau fără semnătură, precum și cele marcate ca ‘’unsafe’’. Unele obiecte Active X sunt spyware. Aceste setări le vor bloca.

5.2 Farse pe e-mail, Scam și Spam

Multe din incidentele de tip Scam vin sub forma unui avertisment despre un virus care poate să 'șteargă hard disk-ul' sau un mesaj similar. Mesajul îți va cere să contactezi toate persoanele din agenda dvs. pentru a-i avertiza. Aceste farse sunt extrem de comune, astfel că furnizorii de software antivirus au creat pagini web care raportează și urmăresc ultimele astfel de încercări.

Una dintre escrocheriile cele mai cunoscute și propagate via e-mail (SCAM) este cea care folosește mesajul 'You can be a millionaire' (Poți deveni milionar). Prin retransmiterea acestor e-mail-uri altor persoane, utilizatorul este convins că va primi o anumită sumă de bani pentru fiecare mesaj transmis. Au existat foarte multe persoane care au căzut pradă acestei scheme.

Autorii acestui tip de e-mail caută adesea notorietate prin transmiterea mesajului lor, la cât mai mulți utilizatori.

O modalitate simplă de a sesiza o farsă sau înșelătorie este includerea unui atașament. La fel cum site-uri de încredere nu vor cere informații cu caracter personal prin e-mail, persoane de încredere sau instituții nu vă vor transmite printr-un atașament care trebuie folosit 'pentru eliminarea fișierelor infectate. Așadar, este foarte important să nu deschideți niciodată un atașament de la un expeditor necunoscut sau un atașament pe care nu îl așteptați.

Țineți minte: În cazul în care mesajul sună prea frumos pentru a fi adevărat, atunci probabil că așa este. În cazul în care în corpul e-mail-ului se specifică faptul că urmărește numărul destinatarilor mesajului pe care ar trebui să îl transmiți mai departe, atunci este vorba de o înșelătorie. E-mail-urile nu pot fi urmărite în acest mod. Cel mai bun mod de a opri acest tip de farse și escrocherii, este de a te informa despre modul cum acestea operează. Informarea este cheia succesului în cazul eliminării campaniilor dăunătoare de pe Internet.

Spam-ul este varianta electronică a junk mail-ului, termen referitor la mesaje nesolicitate și adesea nedorite de către destinatar. Tendința este ca și spam-ul să conțină un atașament sau link malițios.

Cu toate că nu vei putea niciodată elimina complet primirea unor astfel de mesaje, există totuși modalități de a reduce cantitatea de mesaje de tip spam primită.

Există câțiva pași pe care puteți să-i faceți pentru a reduce semnificativ cantitatea de spam pe care o primiți:

- Nu oferiți adresa de e-mail în mod arbitrar – adresele de e-mail au devenit așa de comune, încât au alocat un spațiu special pe aproape orice formular. Uneori aceste liste sunt vândute sau partajate cu alte companii, astfel că din acel moment este posibil să primiți mesaje nesolicitate;

- Raportați mesajele ca spam – Majoritatea clienților de e-mail (Thunderbird, Outlook etc.) oferă o opțiune de a raporta un mesaj ca spam sau junk. Dacă aveți această opțiune puteți profita de funcționalitatea ei. Raportând mesajele de tip spam sau junk folosind această funcționalitate, ajută la filtrarea corectă a mesajelor astfel încât email-urile nedorite să nu mai fie afișate în Inbox această filtrare fiind automatizată , este de dorit să verificați frecvent directoarele de tip SPAM sau JUNK pentru eventualitatea în care mesaje legitime pot ajunge la rândul lor în acest spațiu;
- Mesajele nedorite care oferă o opțiune de dezabonare sunt deosebit de tentante, dar acest lucru este de multe ori o metodă de colectare a adreselor valide care sunt apoi folosite pentru a trimite alte mesaje de tip spam;
- Dezactivați descărcarea automată a graficii în e-mail-uri HTML – Mulți dintre cei care trimit mesaje de tip SPAM trimit mesaje HTML cu un fișier grafic atașat.

5.3 Phishing

Phishing-ul este o metodă online folosită de către atacatori pentru a sustrage bani, credențiale de acces la conturi online, parole sau alte informații personale și/sau importante. De obicei, un atac de tip phishing reprezintă un e-mail deghizat ca un mesaj de la o sursă de încredere (bancă, companii de credit, comercianți online etc.). Nu este un fapt neobișnuit ca funcționarii publici să primească e-mail-uri de tip phishing care par să vină din partea colegilor de birou sau din partea altor angajați din spațiul public. Aceste conturi au fost de cele mai multe ori compromise în prealabil și ulterior făcute să trimită e-mailuri de tip phishing către toate contactele înregistrate în lista lui de contacte.

Spear-phishing este o formă mai concentrată și vizează un anumit membru al unei instituții, care solicită accesul neautorizat la date confidențiale. Ca și în cazul mesajelor folosite în cazul campaniilor de tip phishing normale, mesajele de spear-phishing par că sunt expediate de la o sursă cunoscută și de încredere. În cazul spear-phishing-ului însă, sursa aparentă a emailului este cel mai probabil un individ din interiorul instituției recipientului sau dintr-o rețea de contacte de încredere, de regulă aflați într-o poziție de autoritate.

Mesajul primit vă cere de regulă să verificați imediat datele contului dvs., amenințând de regulă cu luarea unor măsuri negative împotriva dvs. în cazul în care nu vă conformați. Utilizatorii sunt astfel adesea păcăliți în a furniza informațiile cerute cu caracter personal sau confidențial, cum ar fi numere de cont bancar sau de card de credit, codul numeric personal, parole, etc. Astfel de e-mail-uri pot conține imagini, logo-uri texte și link-uri către site-uri web ce par a fi legitime. De asemenea, este comun pentru astfel de e-mail-uri să includă atașamente și link-uri pentru documente false, care vă solicită să introduceți numele de utilizator și parola. Este foarte importantă verificarea legitimității

oricăror atașamente venite din partea colegilor de muncă, angajați din spațiul public, sau din alte surse, înainte de a deschide documentul sau de a accesa link-ul transmis.

E-mail-urile legitime venite din partea instituțiilor financiare, angajați din domeniul public sau orice alt tip de organizație, nu îți vor solicita NICIODATĂ informații personale.

Cum puteți sesiza diferența dintre o înșelătorie de tip phishing și un e-mail sau site legitim?

Din nefericire, incidentele de tip phishing sunt din ce în ce mai răspândite și utilizate, dezvoltându-se și fiind din ce în ce mai greu de identificat. Cu toate acestea, există multiple strategii pe care le puteți utiliza pentru a recunoaște acest tip de escrocherii.

- Fiți sceptic! Din moment ce realizați faptul că astfel de escrocherii de tip phishing există în lumea virtuală, fiți sceptici cu privire la conținutul fiecărui email pe care îl primiți. A fost oare contul dvs. cu adevărat compromis? Aveți cu adevărat nevoie să vă actualizați informațiile contului? Majoritatea companiilor nu așteaptă până în ultimul moment să notifice clienții despre o situație de urgență. Aceștia de regulă trimit mai multe notificări, de regulă prin intermediul serviciului poștal sau vă contactează prin telefon pentru a vă avertiza asupra potențialelor încălcări ale securității. Dacă primiți astfel de email-uri, verificați conținutul pentru indicii care să demonstreze că acel mesaj este un fals;
- Verificați atent adresa web și adresa de email deopotrivă. Este o modalitate foarte bună de a descoperi o înșelătorie. Spre exemplu, în cazul în care o adresă web este afișată sub această formă (http://172.168.15.100/ebay/account/), atunci fiți sigur că site-ul pe care urma să îl accesați nu este unul legitim. Chiar dacă Ebay este parte a adresei afișate, după cum puteți observa, prima parte conține caractere numerice aranjate sub forma unei adrese IP. Acesta este un indiciu clar că ceva nu este în regulă;
- Uitați-vă după semne clare de securitate. Site-urile corporațiilor, de regulă sunt atent securizate și folosesc pagini web criptate de fiecare dată când clienților li se cere să trimită informații cu caracter personal. În bara de navigare a browserului utilizat, verificați dacă adresa pe care doriți să o accesați începe cu 'https://'. Litera 's' reprezintă unul din semnele că această conexiune este securizată și vine din engleză de la termenul de 'security/secure'. Totodată, uitați-vă după o pictogramă cu un lacăt închis în partea de sus a ferestrei browserului. Dacă nu identificați aceste semne, atunci este posibil ca site-ul să fie unul fals;
- Atenție la detaliile dubioase! Majoritatea email-urilor sau website-urilor venite din partea corporațiilor au un aspect profesional. Phishing-urile încearcă să te păcălească, copiind aspectul acestora. Pentru a detecta diferențele, căutați în text greșeli gramaticale, de ortografie sau chiar greșeli de design cu privire la aspectul site-ului.
- Dacă instinctul îți transmite că e ceva dubios, atunci cel mai probabil ai dreptate. După cum am mai afirmat, escrocheriile de tip phishing devin din ce în ce mai complexe pe zi ce trece, astfel

că parcurgerea pașilor propuși nu este o modalitate 100% sigură de detectare a unui phishing, dar este un punct de început;

- Folosiți telefonul pentru a vă asigura de legitimitatea conținutului. Sunați compania expeditoare a mesajului sau persoana în cauză, dar nu folosiți numărul de telefon afișat în corpul e-mail-ului. Contactați o persoană care ar putea cu adevărat să vă ajute să verificați legitimitatea mesajului primit.
- Dacă simțiți că ați fi putut primi un e-mail de tip phishing, nu faceți click pe orice link-uri pentru a deschide atașamentele și nu transmiteți e-mailul mai departe.

6. CONSIDERAŢII FINALE

“Gidul de securitate cibernetică pentru funcționarii publici”, elaborat de Centrul pentru răspuns la incidente cibernetice CERT-GOV-MD, nu reprezintă un ghid absolut împotriva amenințărilor cibernetice şi respectiv nu oferă garanții pentru o protecție sigură. Ghidul însă contribuie la dezvoltarea unei culturi şi crearea unor reflexe în ceea ce privește securitatea informației şi respectarea cerințelor minime obligatorii de securitate cibernetică, într-un mediu digital caracterizat printr-o continuă transformare şi dezvoltare.

Pentru creșterea nivelului de securitate cibernetică a unei organizații sunt importante:

- Crearea unei viziuni şi a unor principii ce ar trebui translatate într-o politică a securității informației;
- Implementarea acestei politici în cadrul organizației şi definirea clară a rolurilor şi responsabilităților;
- Dezvoltarea unei culturi şi a unei stări de spirit adecvate, prin implementarea corectă a principiilor ce privesc securitatea informației.

Utilizatorul reprezintă primul zid de apărare împotriva amenințărilor din spatele monitorului, primul şi uneori ultimul senzor în identificarea pericolelor şi, în funcţie de caz, semnalarea acestora responsabilului IT al instituţiei. Utilizatorul este, totodată, cel care poate preveni crearea unor prejudicii substanţiale atât pentru sine, cât şi pentru instituţia în care activează.

CE PRESUPUNE CULTURA ÎN SECURITATEA INFORMAȚIEI?

- **Comunicare sigură şi responsabilă;**
- **Utilizarea înţeleaptă a reţelelor de socializare;**
- **Transferul conţinutului digital într-o manieră sigură;**
- **Utilizarea adecvată a parolelor;**
- **Evitarea pierderii informațiilor importante;**
- **Asigurarea că doar anumite persoane au acces la informaţii;**
- **Protecția împotriva virușilor sau a altor aplicații malware.**