Siguranța Online a Companiei și Protecția datelor cu caracter personal

Valentina Ichim

Chișinău, 2021

Îmbunătățirea siguranței online a companiei

Reguli de igienă cibernetică pe timp de COVID-19!

Ce puteți face ca organizație?

- Asigurați accesul angajaților la documente de lucru doar prin canale de comunicare criptate (SSL VPN, IPSec VPN).
- Oferiți angajaților acces la un software sigur dedicat apelurilor video.
- Conștientizați riscurile de securitate posibile și asigurați-vă că angajații sunt constant informați.
- Asigurați-vă că există o persoană de contact, disponibilă să ofere suport de la distanță angajaților, în cazul în care apar erori tehnice sau de securitate.
- Verificați regulat datele publicate pe pagina oficială a instituției și restricționați accesul la date importante.
- Asigurați-vă că angajații respectă prevederile cadrului legal privind cerințele minime de securitate.
- Asigurați-vă că angajații respectă legislația referitoare la protecția datelor cu caracter personal.

Ce puteți face ca angajat?

- Folosiți preferabil dispozitive și conexiuni furnizate de organizație (laptop și telefon de serviciu, conexiune privată protejată prin parolă, etc.)
- Nu partajați adresele URL a conferințelor video online pe diverse canale de social media pentru a evita accesul unor părți terțe neautorizate.
- Folosiți parole puternice și unice pentru fiecare cont (minim 8 caractere) de litere mari și minuscule, numere și caractere speciale.
- Faceți cu regularitate copii ale fișierelor și salvați-le pe suporturi sigure.
- Asigurați confidențialitatea strictă a datelor cu caracter personal(ale colegilor sau clienților).
- Nu lăsați dispozitivele spre a fi utilizate de către copii sau alți membri ai familiei.
- Nu lăsați laptopul deschis (unlocked) la părăsirea spațiului de lucru. Puteți bloca ecranul dispozitivului prin apăsarea combinației de taste (Windows+L).

SEMNE DE ALARMĂ!

În perioada pandemiei de COVID-19, fiți precauți și respectați regulile de igienă cibernetică pentru a evita escrocherii și fraude în mediul online!

- Mesaje suspecte, care creează o imagine de urgență sau prin care se solicită lucruri neobișnuite, uneori aparent transmise de la persoane cunoscute.
- Atașamente din email, care au extensii neobișnuite (ex. ".pif", ".exe", ".liliac", ".vbs"). Nu le deschideți niciodată.
- e-mail-urile nesolicitate, cu atașamente sau link-uri către pagini ce conțin prea multe greșeli gramaticale și neconcordanțe de informații.

REȚINEȚI!
Infractorii cibernetici profită de anxietatea și panica oamenilor în mod special pe perioada pandemiei. Fiți atenți și urmăriți doar surse oficiale și credibile pentru informații actualizate.

I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"
022 820 911
www.stisc.gov.md
stisc@stisc.gov.md
info@cert.gov.md

Atenție la pagini web false!

- Atenție la bara de adrese. Dacă un site web folosește http: // (fără S), atunci fiți atenți și nu introduceți informații personale.
- Verificați numele de domeniu și greșelile de ortografie. De multe ori, escrocii emit adresele web a unor companii mari cu renume, cum ar fi Yah00.com sau Amaz0n.net.
- Țineți cont că atacatorii imită perfect logoul și designul mesajelor expediate, iar de foarte multe ori, utilizează un limbaj care sugerează urgență.
- Folosiți doar opțiuni de plată sigure, cercetând în prealabil pagina web (analiza recenziilor).
- Folosiți instrumente de securitate. Instalați program antivirus și utilizați plugin-uri pentru browsere, care vă pot avertiza dacă încercați să accesați site-uri web potențial periculoase.

- Cumpărați exclusiv de la magazine cunoscute și citiți atent recenziile.
- Folosiți cartea de credit pentru cumpărături online.
- Nu vă grăbiți să acceptați orice ofertă! Dacă promoția este una prea bună pentru a fi reală, atunci cel mai probabil este o încercare falsă.
- Păstrează întotdeauna documentele referitoare la plățile pe care le-ai efectuat online.
- Nu trimite niciodată numărul de card, PIN-ul sau alte date ale cardului prin email
- Verificați periodic tranzacțiile din cont, pentru a identifica din timp orice activitate suspicioasă.
- Dacă produsul comandat nu sosește la timp, contactați imediat vânzătorul. Dacă nu răspunde, contactați banca.

Sfaturi pentru cumpărături sigure în regim online!

REȚINEȚI!
Pentru a evita escrocheriile online mai ales atunci când doriți să procurați diverse produse, fiți vigilenți și precauți. Nu uitați, infractorii cibernetici profită de panica și disperarea populației.

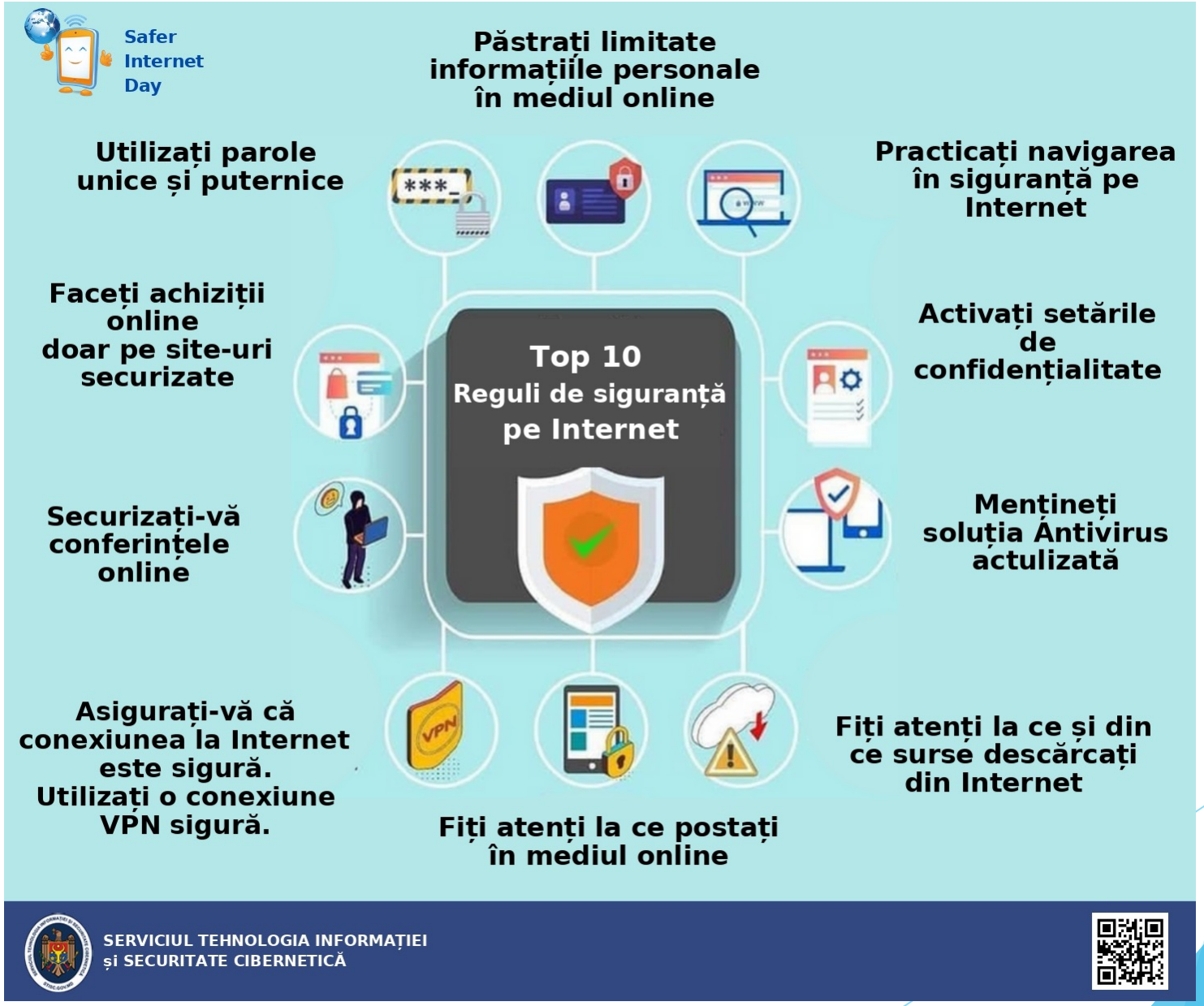
I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"
022 820 911
www.stisc.gov.md
stisc@stisc.gov.md
info@cert.gov.md

Îmbunătățirea siguranței online a companiei

Rețineți!

Infractorii cibernetici profită de anxietatea și panica oamenilor, în mod special în perioada pandemiei.
Respectați setul minim de reguli!
Fiți vigilenți și accesați doar surse oficiale, credibile și verificabile pentru informații veridice și actuale!

Îmbunătățirea siguranței online a companiei



Verificarea setărilor de confidenlialitate Si securitate

Protejați-vă computerul:

- Menţineţi sistemul de operare actualizat la zi.
- Folosiți un program antivirus.
- Folosiți un firewall.
- Faceți copii de siguranță ale fișierelor importante.
- Aveți grijă la ceea ce descărcați.

Protejați-vă online:

- Aveți grijă când dați datele personale.
- Gândiți-vă la cine este persoana cu care discutați.
- Țineți minte că nu totul este de încredere și nu toată lumea este cinstită online.

Respectați următoarele reguli :

- Trebuie să respectați legile, chiar și atunci când vă aflați pe Internet.
- Țineți minte să aveți grijă de ceilalți și de voi când sunteți online.

Verificarea setărilor de confidenlialitate și securitate

Atenție la setările privind confidențialitatea!

- Selectați atent aplicațiile sau site-urile pe care le folosiți. Citiți termenii și condițiile/permisiunile de care au nevoie aplicațiile pe care le instalăm (geolocalizare, microfon, cameră, fotografii, agenda telefonică).
- Nu puneți excesiv de multe informații despre dvs. pe Internet
- Folosiți unelte care respectă viața privată – pentru browser, pe mobil sau pentru calculator
- Cînd postați informații sau comentarii pe Internet e ca și cum ați striga în gura mare în piață ca să vă audă toată lumea. Internetul este spațiu public. Rețelele de socializare sunt un spațiu public.

Securitatea tranzacțiilor în comerțul electronic

- Îmbinarea de cuvinte „securitatea tranzacțiilor electronice”

Rețelele informatice pot intermedia acțiunile ce țin de tranzacțiile electronice doar în măsura în care este vorba de operarea cu informațiile aferente.

De aici și sarcinile ce revin „securizării tranzacțiilor electronice” – securizarea informațiilor ce țin de tranzacțiile în cauză între părțile implicate. Mai mult ca atât, disponibilitatea informațiilor necesită ca și resursele rețelelor informatice implicate să fie disponibile în stare funcțională, extinzând astfel considerabil gama de activități necesare cu securizarea tranzacțiilor electronice.

Deci, orice **tranzacție electronică** presupune transferul și procesarea de informații folosind resursele rețelelor informatice (mijloacelor informatice). De aceea mai reușit ar fi denumirea acestora „tranzacții informatice”, iar prescurtat – „i-tranzacții”.

Securitatea tranzacțiilor în comerțul electronic

- Securitatea i-tranzacțiior acoperă:
- securitatea accesului la servicii;
- identificarea corectă și autentificarea participanților (pentru a le furniza serviciile pe care le-au subscris);
- integritatea schimburilor de informații;
- dacă este necesar, confidențialitatea informațiilor;
- poate fi necesară păstrarea probelor pentru soluționarea disputelor și litigiilor. Toate aceste măsuri de protecție pot asigura așteptările utilizatorilor privind securitatea tranzacțiilor.

Protectia datelor cu caracter personal

Cerințe legale

- HG Nr. 811 din 29.10.2015 cu privire la Programul național de securitate cibernetică a RM pentru anii 2016-2020
- Legea privind semnătura electronică și documentul electronic nr. 91 din 29.05.2014
- Legea cu privire la reutilizarea informațiilor din sectorul public nr. 305 din 26.12.2012
- Legea din privind protecția datelor cu caracter personal nr. 133 din 08.07.2011
- Legea privind prevenirea și combaterea criminalității informatice nr. 20-XVI din 03.02.2009

- Date cu caracter personal (categoria obișnuită)

1) numele și prenumele;
2) sexul;
3) data și locul nașterii;
4) cetățenia;
5) IDNP;
6) imaginea;
7) vocea;
8) situația familială;
9) situația militară;
10) datele de geolocalizare/datele de trafic;
11) porecla/pseudonimul;
12) datele personale ale membrilor de familie;
13) datele din permisul de conducere;
14) datele din certificatul de înmatriculare;
15) situația economică și financiară;

16) datele privind bunurile deţinute;

17) datele bancare;

18) semnătura;

19) datele din actele de stare civilă;

20) numărul dosarului de pensie;

21) codul personal de asigurării sociale (CPAS);

22) codul asigurării medicale (CPAM);

23) numărul de telefon/fax;

24) numărul de telefon mobil;

25) adresa (domiciliului/reşedinţei);

26) adresa e-mail;

27) datele genetice;

28) datele biometrice şi antropometrice;

29) datele dactiloscopice;

30) profesia şi/sau locul de muncă;

31) formarea profesională – diplome – studii;

32) obişnuinţele/preferinţele/comportamentul;

33) caracteristicile fizice.

Date cu caracter personal (categoria specială)

Informaţia care dezvăluie:

- originea rasială sau etnică,
- convingerile politice,
- religioase,
- privind starea de sănătate
- viaţa intimă
- condamnările penale ale unei persoane fizice.

Gestionarea eficientă a profilelor din social media

- **Social media marketing** este un mijloc de comunicare puternic, disponibil întreprinderilor și organizațiilor de toate dimensiunile pentru a se conecta regulat cu clienții sau potențialii clienți/utilizatori.
- Așadar, Marketerii si profesionistii in digital marketing creează pagini de Facebook corporative și conturi pe Twitter, Instagram, Pinterest și alte rețele de socializare majore cu acest scop.
- **Social media marketing** sau SMM (de asemenea, cunoscut sub numele de rețea socială de marketing și social marketing web) *este o formă de internet marketing care folosește capacitatea canalelor de mass-media sociale și aplicații web (Apps) pentru a genera interacțiune (engagement) și distribuire (social shearing) pentru a crește vizibilitatea și conștientizarea unui brand.*
- Beneficiile **Social media marketing:**
- Imbunatațirea customer satisfaction (cerințele clienților)
- Creșterea loialității clienților (brand loyalty)
- Imbunatațirea customer service
- Mărește numarul potențialilor clienți
- Creșterea traficului web pe site-ul sau blogul activității
- Imbunatațirea ranking-ului site-ului pe motoarele de căutare
- Creșterea gradului de conștientizare a mărcii (brand awareness)
- Conectarea și dezvoltarea relațiilor interactive cu publicul țintă
- Dezvoltarea unei reputații ca expert sau lider în domeniul de activitate (brand authority)

Cum sa face Social Media Marketing ? *Regulile unei strategii de success*

- Etapa 1 : Realizare unui Audit
- Etapa 2: Definirea obiectivelor
- Etapa 3: Identificarea publicului țintă
- Etapa 4: Crearea unei social media content strategy
- Etapa 5: Acordare atenție celor care fac Influencer
- Etapa 6: Alegerea platformelor de social media marketing
- Etapa 7: Masurare si testare