Securitatea cibernetică

GHID DE BUNE PRACTICI

I.P. Serviciul Tehnologia Informației și Securitate Cibernetică
www.stisc.gov.md

Backup: copii de siguranță a datelor

Efectuați backup-uri periodice pentru a vă asigura că informația este recentă și în siguranță. Aceasta este o prioritate în activitatea fecărei instituții. În acest sens vă asigurați activitatea față de pierderea de date, șantaj și alte posibile atacuri cibernetice!

Sfat 1: Identificați datele de care aveți nevoie pentru a crea copii de rezervă

Primul pas este identificarea acelor date fără de care instituția dvs. nu ar putea funcționa ca atare. În mod normal, informația dată va cuprinde documente, fotografii, e-mailuri, contacte și calendare, cele mai multe dintre ele fiind păstrate în doar câteva mape comune pe computer, telefon, tabletă sau rețea.

Sfat 2: Păstrați backupul separat de computer

Indiferent că păstrați informația pe un stick USB, pe o unitate separată sau pe un computer separat, accesul la copiile de rezervă ar trebui restricționat astfel încât:

• să nu fie accesibil de către personal;
• să nu fie conectat permanent la un dispozitiv ce deține copia originală;

Ransomware (și alte tipuri de programe malware) se pot deplasa automat la spațiul de stocare atașat în mod automat, ceea ce înseamnă că orice astfel de copie de rezervă ar putea fi de asemenea, infectată, lăsându-vă fără posibilitatea de a face backup. Pentru o rezistență mai mare, ar trebui să vă gândiți să stocați copiile de rezervă într-o altă locație, astfel încât furtul nu va duce la pierderea ambelor copii.

Sfat 3: Luați în considerare spațiul de stocare

Probabil ați folosit de nenumărate ori spațiul de stocare în timpul activităților, fără să știți că dacă nu vă difuzați propriul server de e-mail, e-mailurile dvs. vor fi deja stocate în cloud. Folosind spațiul de stocare în cloud (unde un furnizor de servicii vă stochează datele pe infrastructura lui) înseamnă că datele dvs. sunt fizic separate de locația dvs. Veți beneficia, de asemenea, de un nivel ridicat de disponibilitate. Furnizorii de servicii pot furniza instituției dvs. servicii de stocare a datelor și servicii web fără a fi nevoie de prea multe investiții. Majoritatea furnizorilor oferă o limită cantitativă de spațiu de depozitare și o capacitate de stocare mare la costuri minime pentru instituții mici.

Sfat 4: Creați copii de siguranță a datelor

Copierea datelor de rezervă nu este un lucru tocmai interesant de făcut sau mai ales prioritar atunci când există alte sarcini mult mai importante, însă majoritatea soluțiilor de stocare în rețea sau Cloud, vă permite acum să faceți backup-ul automat. Folosirea backup-urilor automate nu doar că vă economisește timpul, dar de asemenea veți deține și cea mai recentă versiune a fișierelor dvs. în caz că veți avea nevoie de ele. Multe soluții de rezervă sunt accesibile și ușor de configurat, ele fiind considerate drept protecție critică pentru instituția dvs. Atunci când alegeți o soluție, va trebui să luați în considerare pentru câte date aveți nevoie să creați copii de siguranță și cât de repede să le puteți accesa în caz de un eventual incident.

Protejați instituția de programele malware

Software-ul rău intenționat cunoscut și sub numele de "Malware" este un software sau un conținut web care vă poate afecta instituția. Cea mai cunoscută formă de malware sunt virușii și programele de auto-copiere care infectează software-ul legitim. Această secțiune conține 5 sfaturi simple și ușor de implementat, care vă pot ajuta în prevenirea malware-ului .

Sfat 1: Instalați și porniți software-ul antivirus

Software-ul antivirus, care este adesea inclus gratuit în sistemele de operare populare ar trebui să fie instalat în toate computerele și laptopurile. Software-ul antivirus este folosit în general pentru prevenirea și eliminarea virușilor de computer. De asemenea, poate detecta și elimina adware, spyware și malware.

Sfat 2: Interziceți personalului să descarce aplicații rău intenționate

Ar trebui să descărcați aplicații doar pentru telefoane mobile și tablete de la magazine aprobate de producător (cum ar fi Google Play sau Apple App Store). Aceste aplicații sunt verificate pentru a oferi un anumit nivel de protecție împotriva malware-ului care ar putea avea efect dăunător. Ar trebui să împiedicați personalul să descarce aplicații terțe de la furnizori / surse necunoscute, deoarece acestea nu sunt
verificate. Conturile personale ar trebui să fie accesibile doar pentru a-și îndeplini rolul, cu permisiuni suplimentare (adică pentru administratori) acordate doar celor care au nevoie de ele. La crearea conturilor administrative, acestea trebuie să fie folosite doar pentru realizarea sarcinilor specifice, având cont de utilizator standard folosit pentru munca generală.

Sfat 3: Actualizați-vă echipamentele informaționale
Este necesar să vă asigurați echipamentele IT (tablete, smartphone-uri, laptopuri și PC-uri) cu cele mai recente versiuni ale dezvoltatorilor de software și furnizorilor de hardware. Aplicarea acestor actualizări, un proces cunoscut sub numele de patching, este unul dintre cele mai importante lucruri pe care le puteți face pentru a îmbunătăți securitatea.
Sistemele de operare, programele, telefoanele și aplicațiile trebuie să fie setate în așa mod încât acestea să se actualizeze automat. La un moment dat, aceste actualizări nu vor mai fi disponibile deoarece produsul ajunge la sfârșitul duratei de viață, moment în care ar trebui să luați în considerare înlocuirea acestuia cu o alternativă modernă.

Sfat 4: Controlați modul în care pot fi utilizate unitățile USB și cardurile de memorie
Unitățile USB sau cardurile de memorie sunt din ce în ce mai folosite în transferurile de fișiere între insituții și persoanele fizice. Cert e că pericolul de a introduce în mod accidental un stick infectat (cum ar fi un drive USB care conține malware) de către un utilizator și de a devasta întreaga instituție, este mare. Atunci când unitățile și cardurile sunt partajate în mod deschis, devine greu să urmăriți conținutul acestora, unde au fost și cine le-a folosit. Puteți însă reduce probabilitatea de infectare prin:
• blocarea accesului la porturile fizice pentru majoritatea utilizatorilor;
• utilizarea instrumentelor antivirus;
• limitarea utilizării instrumentelor USB și a cardurilor de memorie doar în cadrul organizației dvs.

Aceste reguli trebuie să fie parte a politicii de securitate aprobate în cadrul instituției. De asemenea, puteți solicita personalului să transfere fișiere utilizând mijloace alternative, adică prin e-mail sau prin stocarea în Cloud.

Sfat 5: Porniți paravanul de protecție
Firewall-urile creează o "zonă amortizată" între rețeaua proprie și rețelele externe (cum ar fi Internetul). Cele mai populare sisteme de operare includ acum un firewall, așadar aceasta poate fi pur și simplu un caz de pornire.

Siguranța gadgeturilor

Tehnologia mobilă este în prezent o parte esențială a organizațiilor și instituțiilor moderne. Și asta pentru că tot mai multe dintre datele noastre sunt stocate pe tablete și smartphone-uri, dispozitive ce sunt la fel de puternice ca și computerele tradiționale. Cert este că aceste dispozitive au nevoie de o protecție mai mare decât echipamentele de tip "desktop".

Sfat 1: Activarea protecției prin parolă

Utilizați parole impredictibile, complexe dar ușor memorabile și încercați să păstrați confidențialitatea lor. Multe dispozitive includ acum recunoașterea amprentelor digitale de blocare a dispozitivelor, fără a avea nevoie de o parolă. Însă, aceste funcții nu sunt întotdeauna activate și nu funcționează întotdeauna. Verificați așadar întotdeauna dacă aceste funcții au fost activate.

Sfat 2: Asigurați-vă că dispozitivele pierdute sau furate pot fi urmărite, blocate sau șterse.

Tabletele sau telefoanele au mai multe șanse de a fi pierdute sau furate. Din fericire, majoritatea dispozitivelor includ instrumente gratuite bazate pe internet, care vă ajută să le recuperați în caz de pierdere.

Aceste instrumente puteți să le utilizați pentru:
- a urmări localizarea unui dispozitiv;
- blocarea de la distanță a accesului la dispozitivul dvs;
- ștergerea de la distanță a datelor stocate pe dispozitiv;
- recuperarea unei copii de rezervă a datelor stocate pe dispozitiv.

La prima vedere, configurarea acestor instrumentele de pe toate dispozitivele poate părea dificil la început, dar utilizând software-ul de gestionare a dispozitivelor mobile, puteți configura dispozitivele dvs. la o configurație standard doar cu un singur clic.

Sfat 3: Actualizați-vă dispozitivul

Indiferent de tipul dispozitivelor utilizate în cadrul instituția dvs., este important ca acestea să fie actualizate în orice moment. Toți producătorii (Windows, Android, iOS) publică actualizări obișnuite care conțin actualizări critice de securitate pentru a păstra dispozitivul în siguranță.

Acest proces este rapid, ușor și gratuit. Dispozitivele ar trebui să fie setate în așa fel încât să se actualizeze automat.
Asigurați-vă că angajații dvs. știu cât de importante sunt aceste actualizări și explicați-le cum le pot utiliza în caz de necesitate. La un moment dat, aceste actualizări nu vor mai fi disponibile deoarece dispozitivul ajunge la sfârșitul duratei de viață, moment în care ar trebui să îl înlocuiți cu o alternativă modernă.

Sfat 4: Actualizați-vă aplicațiile

La fel ca sistemele de operare din dispozitivele instituției dvs., toate aplicațiile pe care le-ați instalat ar trebui, de asemenea, să fie actualizate în mod regulat cu ajutorul patch-urilor de la dezvoltatorii de software. Aceste actualizări nu vor adăuga doar funcții noi, dar de asemenea ele vor identifica ce orificii de securitate au fost descoperite. Asigurați-vă că personalul știe când sunt actualizate operațiunile, cunosc cum să le instaleze și cât de importantă este realizarea lor operativă.

Sfat 5: Nu vă conectați la Hotspot-uri și Wi-Fi necunoscute

Când folosiți hotspot-uri publice, Wi-Fi (de exemplu în hoteluri sau cafenele), nu există nicio modalitate de a afla cu ușurință cine controlează hotspot-ul sau să poți dovedi cine crezi că o face. Dacă vă conectați la aceste hotspot-uri, trebuie să cunoașteți că altcineva ar putea accesa:

- ceea ce lucrați în timp ce sunteți conectat;
- detaliile dvs. private de conectare pe care multe aplicații și servicii web le mențin în timp ce sunteți conectat.

Cea mai simplă modalitate de precauție este să nu vă conectați la Internet dacă nu cunoașteți cine este deținătorul hotspot-ului. În asemenea circumstanțe, de preferat este să utilizați rețeaua mobilă 3G sau 4G, pentru a avea securitate integrată. Acest lucru înseamnă că puteți utiliza și "tethering" (în cazul în care celelalte dispozitive, cum ar fi laptop-urile împărtășesc conexiunea 3G / 4G) sau un "dongle" wireless furnizat de rețeaua dvs. mobilă.
De asemenea, puteți utiliza rețelele virtuale private (VPN), o tehnică care criptează datele înainte de a le trimite pe Internet. Dacă utilizați rețele VPN ale unor părți terțe, veți avea nevoie de capacitatea tehnică de a le configura singuri și ar trebui să utilizați VPN-uri asigurate de furnizori de servicii de performanță.

Parole puternice pentru date protejate

Laptopurile, computerele, tabletele și smartphone-urile conțin o mulțime de date importante despre afacerile dumneavoastră, informații personale ale clienților dvs., precum și detalii despre conturile online pe care le accesați. Este esențial ca aceste date să fie disponibile doar pentru utilizatori autorizați. Parolele - atunci când sunt implementate corect - sunt o modalitate gratuită, ușoară și eficientă de a împiedica accesul utilizatorilor neautorizați la dispozitivele dvs.

Sfat 1: Asigurați-vă că activați protecția prin parolă

Setați o parolă de blocare, un cod PIN sau altă metodă de autentificare (cum ar fi amprenta sau deblocarea Face ID-ului). Dacă utilizați în cea mai mare parte amprenta sau deblocarea Face ID-ului, veți introduce o parolă mai rar. Deci vă recomandăm să configurați o parolă lungă, care este greu de ghicit. Prin urmare, protecția prin parolă nu este doar pentru smartphone-uri și tablete. Asigurați-vă că echipamentul dvs. de birou (de exemplu, laptopurile și calculatoarele) utilizează un produs de criptare (cum ar fi BitLocker pentru Windows). Majoritatea dispozitivelor moderne au încorporat criptarea, dar este posibil ca criptarea să fie necesară și să fie configurată. Respectiv, verificați setarea acesteia.

Sfat 2: Utilizați autentificarea cu doi factori pentru conturile importante

Dacă vi se oferă opțiunea de a utiliza autentificarea cu doi factori (cunoscută și ca 2FA) pentru oricare dintre conturile dvs., ar trebui să o faceți. Aceasta oferă o cantitate mare de securitate pentru eforturile suplimentare. 2FA necesită două metode diferite pentru a "demonstra" identitatea dvs. înainte de a putea utiliza un serviciu (o parolă plus o altă metodă). Acesta ar putea fi un cod care este trimis pe telefonul dvs. smartphone sau un cod care este generat de cititorul de carduri al unei bănci pe care trebuie să îl introduceți suplimentar parolei dvs.

Sfat 3: Evitați utilizarea parolelor previzibile

Dacă sunteți responsabil de politicile IT din cadrul instituției dvs., asigurați-vă că personalului i se oferă informațiile necesare cu privirea corectă a parolelor. Parolele ar trebui să fie ușor de reținut, dar greu de ghicit pentru altcineva. O regulă bună este "asigurați-vă că cineva care vă cunoaște bine, nu poate să ghicească parola dvs. din 20 de încercări".

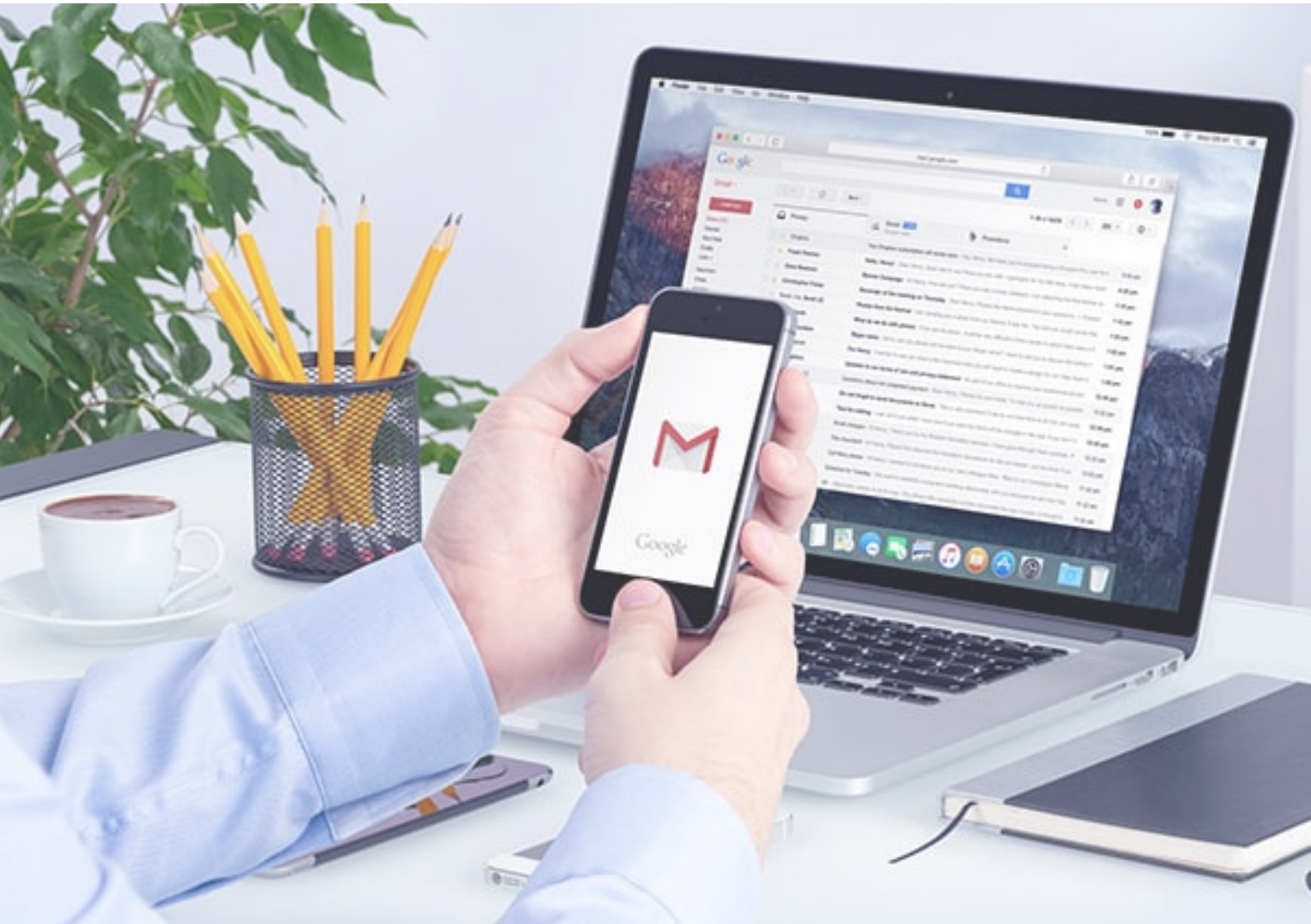
Personalul ar trebui să evite și utilizarea celor mai comune parole, pe care infractorii le pot ghici cu ușurință. Asigurați-vă că fiecare utilizator are acces personal la sistemul potrivit și că nivelul de acces oferit este întotdeauna un minim necesar pentru funcționare, minimizând expunerea inutilă la sistemele la care nu au nevoie de acces.

Sfat 4: Încurajați personalul să facă față parolelor multiple

Dacă sunteți responsabil de modul în care sunt utilizate parolele în instituția dvs., există mai multe lucruri pe care le puteți face pentru a îmbunătăți securitatea. În cazul în care utilizați parole pentru a accesa un serviciu, nu impuneți modificări frecvente ale parolei. Parolele trebuie să fie schimbate doar atunci când suspectați un compromis al acreditărilor de autentificare.
De asemenea, trebuie să furnizați un spațiu de stocare securizat, astfel încât personalul să poată scrie parolelre pentru conturi importante (cum ar fi e-mail și cont bancar) și să le păstreze în siguranță. Personalul poate să uite parolele, astfel trebuie să vă asigurați că acesta își poate reseta cu ușurință parolele pe care le dețin. Luați în considerare utilizarea managerilor de parole (instrumente care pot crea și stoca parolele dvs. pe care le accesați printr-o parolă "master"). Parola principală vă protejează toate celelalte parole. Respectiv, asigurați-vă că este una puternică, utilizând de exemplu trei cuvinte aleatorii.

Sfat 5: Schimbați toate parolele prestabilite

Una dintre cele mai frecvente greșeli este neschimbarea parolelor prestabilite ale producătorilor pe care le emit pentru telefoanele inteligente, laptopuri și alte tipuri de echipamente. Modificați toate parolele prestabilite înainte ca dispozitivele să fie distribuite personalului. De asemenea, trebuie să verificați în mod regulat dispozitivele și software-urile în mod specific pentru a detecta parolele implicite neschimbate.



Evitarea atacurilor de tip phishing

Într-un atac tipic de phishing, escrocii trimit mesaje false către mii de persoane, solicitând informații sensibile (cum ar fi detalii bancare) sau conțin link-uri către site-uri ale răufăcătorilor. Ei ar putea încerca să vă înșele pentru a vă fura informații private sau pentru a accesa informațiile instituțiile dvs. Mesajele de e-mail prin phishing se identifică din ce în ce mai greu, iar altele vor trece cu vederea chiar și de cei mai atenți utilizatori. Indiferent cât de mare sau mică este instituția dvs., puteți deveni victima atacurilor de tip phishing la un moment dat.

Sfat 1: Configurați conturile pentru a reduce impactul atacurilor de succes

Ar trebui să vă configurați conturile personale în avans folosind principiul "cel mai mic privilegiu". Aceasta înseamnă că conducerea oferă cel mai mic nivel de drepturi de utilizator necesare pentru a-și îndeplini sarcinile, astfel încât, dacă sunt victime ale unui atac de tip phishing, prejudiciul potențial este redus. Pentru a reduce în continuare pagubele care pot fi cauzate de malware sau pierderea datelor, asigurați-vă că personalul nu navighează pe web sau verifică e-mailuri dintr-un cont cu rol de administrator. Un cont de administrator este un cont de utilizator care vă permite să efectuați modificări care pot afecta și alți utilizatori.
Administratorii pot schimba setările de securitate, pot instala software și hardware și pot accesa toate fișierele de pe computer. Deci, un atacator care are acces neautorizat la un cont Administrator poate fi mult mai dăunător decât accesarea unui cont de utilizator standard. Utilizați autentificarea cu doi factori (2FA) în conturile dvs. importante, cum ar fi e-mailurile. Aceasta înseamnă că, chiar dacă un atacator știe parolele dvs., ei încă nu vor putea accesa acel cont.

Sfat 2: Verificați semnele evidente de phishing

Identificarea și ștergerea tuturor e-mailurilor de tip phishing este o solicitare imposibilă. Cu toate acestea, multe e-mailuri de phishing îmbraca formă perfectă unui atac tradițional. Așadar, căutați următoarele semne de avertizare:
• Multe escrocherii de phishing provin din străinătate și, adesea, ortografia, gramatica și punctuația sunt greșite. Alții vor încerca să creeze e-mailuri cu aspect oficial, inclusiv logo-uri și grafică;
• Este adresată dvs. prin nume sau se referă la "client cu valoare" sau "prieten" sau "coleg"? Acesta poate fi un semn că expeditorul nu te cunoaște de fapt și că face parte dintr-o înșelătorie de phishing.

Sfat 3: Gândiți-vă la modul în care operați

Asigurați-vă că personalul dvs. înțelege toate modalitățile de lucru (mai ales în ceea ce privește interacțiunea cu alte instituții), astfel încât acestea să fie pregătite mai bine decât de obicei. Printre trucurile comune se numără trimiterea unei facturi pentru un serviciu pe care nu l-ați utilizat, astfel încât atunci când atașamentul este deschis, malware-ul este instalat automat (fără știrea dvs.) în computer. Alta este de a păcăli personalul pentru a transfera bani sau informații prin trimiterea de e-mailuri care par a fi autentice. Gândiți-vă la practicile obișnuite și la modul în care aceste trucuri vă pot ajuta. De exemplu:

- Personalul știe ce să facă cu cererile neobișnuite și cum să obțină ajutor?
- Întrebați-vă dacă cineva care se prezintă sub forma unui individ important (un client sau manager) prin e-mail trebuie să fie contestat (sau să își verifice identitatea într-un alt mod) înainte de a lua măsuri.
- Înțelegeți relațiile dvs. regulate de afaceri? Înșelătorii vor trimite de multe ori e-mailuri de phishing de la mari organizații (cum ar fi băncile), în speranța că unii dintre destinatarii de e-mail vor avea o legătură cu acea companie. Dacă primiți un e-mail de la o organizație cu care nu faceți afaceri, tratați-o cu suspiciune.
- Gândiți-vă la modul în care puteți încuraja și sprijini personalul dvs. să pună la îndoială solicitări suspecte sau neobișnuite, chiar dacă acestea par a fi de la persoane importante. Având încrederea de a întreba "este autentic?" poate însemna diferența de a menține în siguranță sau de a plăti o greșeală costisitoare.

Sfat 4: Raportați toate atacurile

Asigurați-vă că personalul dvs. este încurajat să solicite ajutor dacă crede că ar fi putut fi victima unui phishing. Este important să urmații pașii indicați pentru scanarea malware-ului și să schimbați parolele cât mai curând posibil dacă bănuiți că a avut loc un atac cibernetic. Nu pedepsiți prea aspru personalul, aceast lucru descurajează oamenii să raporteze atacurile pe viitor și îi pot face atât de temători încât să petreacă foarte mult timp examinând fiecare e-mail pe care îl primesc. Ambele lucruri cauzează mai mult rău instituției dvs. . Dacă credeți că instituția dvs. a fost victima fraudei online, înșelătoriilor sau extorcărilor, ar trebui să raportați acest lucru prin intermediul site-ului stisc.gov.md.

Centrul de răspuns la incidente de securitate cibernetică din cadrul STISC, facilitează schimbul de informaţii privind incidentele TI între organizaţiile din societate şi diseminează informaţiile legate de noi probleme, care ar putea împiedica funcţionarea sistemelor TI guvernamentale. Totodată, acesta asigură informaţii şi consultanţă privind măsurile pro-active, precum compilarea şi completarea statisticilor. CERT-GOV-MD este punctul central de raportare şi coordonare privind incidentele de securitate în sistemele de comunicaţii şi informatice, aflate în administrarea Serviciului Tehnologia Informației și Securitate Cibernetică.

incidents@cert.gov.md

+373 22 820 921