SERVICIUL TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

INSTRUCȚIUNEA
PRIVIND MĂSURILE DE PREVENIRE
A INFECTĂRII SISTEMELOR INFORMAȚIONALE

Pentru a preveni infectarea sistemelor informaționale este necesar să respectați următoarele recomandări:

1. În timpul utilizării poștei electronice:
   - 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.
   - 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. Iar pentru verificarea unui fișier suspect încărcați acesta pe site-ul online de verificare https://www.virustotal.com/

     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 .

2. În timpul utilizării browser-ului:
   - 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.
3. În timpul utilizării sistemului de operare:
   - Verificați sistematic actualizările pentru sistemul de operare al web-browser-ului și al antivirusului folosit.

- Nu utilizați contul de administrator în mod regulat când lucrați la calculator, astfel se va împiedica extinderea virusului în sistemul de operare în cazul infectării.
- Folositi o parolă puternică care trebuie să conţină minim opt caractere, dintre care cel puţin două litere şi două numere sau caractere speciale. Cînd schimbaţi parola nu alegeţi o parolă pe care aţi utilizat anterior. Nu folosi cuvinte din alte limbi, nume, date, numere de telefon, care este usor de identificat.
- Configurați sistemul Windows să vă arate extensiile tuturor fișierelor. În cazul în care un fișier este numit "image.jpg.exe", majoritatea calculatoarelor Windows îl vor afișa ca "image.jpg". O bună parte din utilizatori, prin urmare, se vor gândi că acesta este o imagine inofensivă, chiar dacă în realitate fișierul este un program executabil. Mai mult decât atât, atunci când executați programul, cel mai probabil chiar veți vedea o imagine… în timp ce virusul infectează PC-ul dvs.

4. În timpul activităţii de lucru zilnice:
   - 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.
   - Nu dezvăluiți informații personale sau financiare prin e-mail.
   - Utilizați funcții anti-phishing oferite de clientul de e-mail și browser.