Anexa 1

Pentru a preveni infectarea calculatorului dumneavoastră, este necesar să respectaţi următoarele recomandări:

1. În timpul utilizării poştei electronice:

- Nu accesaţi imaginile sau link-urile din e-mailurile dubioase. Un e-mail poate conţine o imagine sau link, care la accesare va aduce utilizatorul pe un site maliţios.
- Setaţi e-mailul dvs. în aşa fel, încât acesta să vă afişeze e-mailurile în format de text simplu, şi nu în format HTML, astfel veţi diminua riscul să fiţi trucaţi cu substituirea link-ului pe altul decât acel afişat în email.
- Asiguraţi-vă că email-urile partenerului dvs. sunt semnate digital, în scopul de a preveni falsificarea acestora;
- Aveţi în vedere că este periculos să deschideţi orice ataşament, chiar şi documentele Microsoft Word şi PDF pot conţine viruşi, nu doar acele care au la sfârşit extensia de".exe".
- În cazul în care dvs. totuşi doriţi să deschideţi documentul PDF sau Word:

a) Dacă este posibil contactaţi expeditorul email-lui prin telefon sau în oricare alt mod.
b) Asiguraţi-vă că Sistemul de operare al calculatorului dvs. şi baza de date a antivirusului este actualizată. Iar pentru verificarea unui fişier suspect încărcaţi acesta pe site-ul online de verificare https://www.virustotal.com/
c) De asemenea pentru a evita orice risc, dvs. puteţi utiliza un soft destinat convertirii PDF-ului într-un format inofensiv ".html", spre exemplu "pdftohtml", sau puteţi recurge la Google Drive, pentru online vizualizarea securizată a documentului .

2.În timpul utilizării browser-ului:

- Verificaţi în mod regulat actualizările pentru web-browser, „Flash adobe” şi „Java”.
- Asiguraţi-vă că folosiţi un antivirus cu posibilităţi de "antiphishing" şi "web-antivirus".
- Nu uitaţi că mesajele Popup (*Ferestrele popup*) care cer actualizarea softului "Adobe Flash Player", "Java" sau a altor softuri, pot fi false. Din acest considerent, este important întotdeauna să închideţi aceste ferestre, iar toate actualizările necesare trebuie instalate manual de pe site-urile oficiale ale producătorilor.
- Niciodată nu salvaţi parolele conturilor dvs. în browser-ele web.
- Utilizaţi modul „Privat” de navigare al browser-ului dvs. în reţeaua internet.
- În cazul în care, nu sunteţi siguri în securitatea unui link, e mai bine să nu îl accesaţi.

3. În timpul utilizării sistemului de operare:

- Verificaţi sistematic actualizările pentru sistemul de operare al web-browser-ului şi al antivirusului folosit.
- Nu utilizaţi contul de administrator în mod regulat când lucraţi la calculator, astfel se va împiedica extinderea virusului în sistemul de operare în cazul infectării.
- Configuraţi sistemul Windows să vă arate extensiile tuturor fişierelor. În cazul în care un fişier este numit "image.jpg.exe", majoritatea calculatoarelor Windows îl vor afişa ca "image.jpg". O bună parte din utilizatori, prin urmare, se vor gândi că acesta este o imagine inofensivă, chiar dacă în realitate fişierul este un program executabil.

- Mai mult decât atât, atunci când executaţi programul, cel mai probabil chiar veţi vedea o imagine în timp ce virusul infectează PC-ul dvs.

4. În timpul activităţii de lucru zilnice:

- fiţi precauţi referitor la apelurile telefonice nesolicitate, vizite, sau emailuri de la persoane care solicită informaţii despre angajaţi sau companie. În cazul în care o persoană necunoscută pretinde a fi de la o organizaţie legitimă, încercaţi să verificaţi identitatea acestuia, în raport cu organizaţia respectivă;
- nu oferiţi informaţii personale sau informaţii despre organizaţia dvs, inclusiv structura reţelei sale, dacă nu sunteţi sigur de autoritatea persoanei care solicită informaţiile;
- nu dezvăluiţi informaţii personale sau financiare prin e-mail;
- utilizaţi funcţii anti-phishing oferite de clientul de e-mail şi browser.

5. **Generarea parolelor:** Generarea parolelor securizate şi utilizarea lor constituie una dintre cele mai importante şi de bază metode a securizării informaţiei.

Nu se recomandă:

- Utilizarea parolelor mai scurte de 6 caractere;
- Utilizarea numelui de familie sau prenumelui ca parolă sau diferite combinaţii ale lor;
- Utilizarea doar a literelor minuscule sau doar a cifrelor (de ex. data naşterii).

Se recomandă:

- Parole de tip 1, formate din registru mic [a-z] sau din cifre [0-9], lungimea minimă 20 caractere;
- Parole mixte, de tip 2, formate din registru mare mic [a-z][A-Z], lungimea minimă 14 caractere;
- Parole mixte, de tip 3, formate registru mic mare + cifre [a-z][A-Z][0-9], lungimea minimă 10 caractere;
- Parole mixte, de tip 4, formate din registru mic mare cifre + semne [a-z][A-Z][0-9][!@$.-_], lungimea minimă de 8 caractere;
- Modificarea parolei cel puţin o dată la 3-6 luni.

Cum se creează o parolă de tip 4:

Sa presupunem ca avem un cuvânt preferat “ACADEMICA”, transformat ar fi “Ac@d3m!ca.”

6. **Browsere, Antivirusuri, Clienţi poştali:**

- Browserele recomandate sunt Mozilla Firefox şi Google Chrome, se recomandă utilizarea lor în modul incognito, astfel nu se salvează parole, care pot fi utilizate de atacatori.
- Se recomandă utilizarea Add-on-urilor de tip NoScript pentru Firefox care blochează banerele şi publicitatea nedorită pe saitul vizitat, plus opreşte executarea scripturilor malefice.
- Utilizarea antivirusului este obligatorie.
- Antivirusuri recomandate: **Kaspersky**, **Avast**. Avast propune şi variantă gratuită pentru cei ce nu dispun de resurse pentru procurarea licenţei.
- Nu se recomandă utilizarea clienţilor poştali nelicentiaţi (cracked), prin utilizarea lor vă expuneţi informaţia confidenţială (parole, documente, scrisori confidenţiale). Mozilla Thunderbird este un client poştal gratuit cu toate opţiunile asemenea celor cu plată.