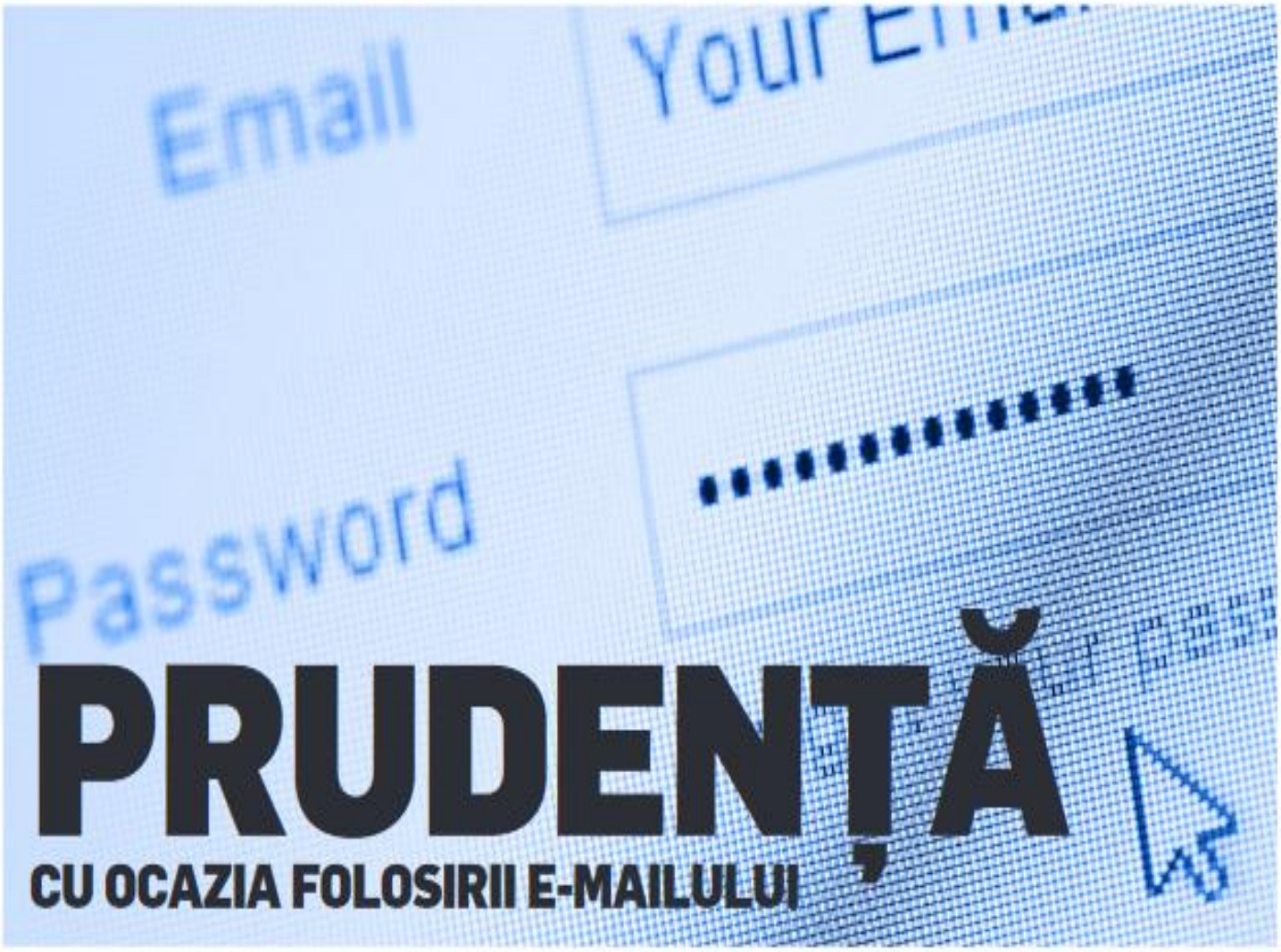

PRUDENȚĂ

CU OCAZIA FOLOSIRII E-MAILULUI

E-mailurile și atașamentele acestora au un rol foarte important în facilitarea atacurilor informatice.

Rețelele de criminalitate informatică, prin acțiuni de manipulare a persoanelor (inginerie socială), distribuie către mai mulți utilizatori mesaje electronice nesolicitate (spam), cu caracter aparent comercial, de publicitate pentru produse și servicii, cu scopul de a infecta utilizatorii.

SECURITATEA E-MAILULUI:

- evită transmiterea sau recepționarea de informații sensibile prin e-mail;
- evită încercările de inginerie socială sau phishing (tehnică utilizată de infractorii cibernetici pentru a obține informații sensibile care implică de regulă existența unui link malițios în cadrul mesajului; odată accesat, acesta trimite utilizatorul spre un site web de unde se va descărca automat un malware);
- orientează-te spre un provider de e-mail ce oferă o filtrare puternică anti-spam;
- nu răspunde la spam și evită e-mailurile în cascadă sau piramidale;
- configurează corect clientul de e-mail;
- nu folosi același nume pentru contul de e-mail personal și pentru cel de serviciu; utilizarea

de nume distincte pentru aceste conturi diminuează riscul ca acestea sa fie ținta unui atac informatic;

- evită stocarea informațiilor critice în conturile personale de e-mail sau în alte rețele din afara instituției/ companiei în care îți desfășori activitatea.

În momentul în care primești un e-mail, acordă atenție următoarelor:

- identitatea expeditorului nu este garantată: verifică relația dintre expeditor și conținutul mesajului;
- nu deschide atașamente provenind de la persoane necunoscute sau asociate unor conturi legitime, dar având mesaje cu subiect și conținut suspect. Acestea pot conține software malițios (malicious software sau malware, cum ar fi viermi, troieni, spyware, forme de adware etc.);
- dacă este absolut necesară deschiderea unui atașament, chiar și din e-mailuri legitime, acesta trebuie, în prealabil, descărcat și scanat cu soluția antivirus instalată și, ulterior, deschis cu aplicația asociată;
- în cazul e-mailurilor care conțin link-uri, nu accesa direct acel link din corpul mesajului; eventual, poate fi copiat acel link și deschis din altă filă (tab) a browser-ului;
- nu răspunde e-mailurilor conținând solicitări de date personale sau confidențiale (de exemplu codul PIN și numărul cardului bancar).

PROTEJEAZĂ-ȚI INFORMAȚIILE:

Pe piață sunt accesibile diferite tipuri de criptare a datelor, ce și-au dovedit eficiența în numeroase situații: criptarea mediilor de stocare sau a mesajelor expediate prin poșta electronică (în locul transmiterii prin e-mail a unor date sensibile în format text, conținutul poate fi criptat cu una dintre soluțiile existente pe piață, de exemplu „pgp").

DE UNDE ȘTII CĂ E-MAILUL TĂU A FOST „ACCESAT" DE PERSOANE NECUNOSCUTE?

- contactele tale spun că au primit e-mailuri spam de la tine;
- primești multe e-mailuri cu erori;
- apar mesaje în dosarul „trimise" fără ca tu să le trimiți;
- istoricul localizării contului în operația de login nu corespunde cu activitatea ta curentă.

CUM SECURIZĂM CONTUL DE E-MAIL CARE A FOST „ACCESAT" DE PERSOANE NECUNOSCUTE?

- recuperarea contului și schimbarea parolei;
- schimbarea parolelor de securitate, setarea verificării prin utilizarea telefonului;
- verificarea conturilor de acces la bănci sau plăți online și notificarea acestora cu privire la spargerea contului de e-mail;
- notificarea contactelor din e-mail că ar putea exista un risc de securitate și că e-mailul (contul) a fost accesat de persoane necunoscute;
- efectuarea operației de back-up la fișierele importante.

Sursa: "Ghid de bune practici pentru securitate cibernetica"

https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf