Comunicații

e-Mail

5.1.1. Scopului criptării și decriptării unui email

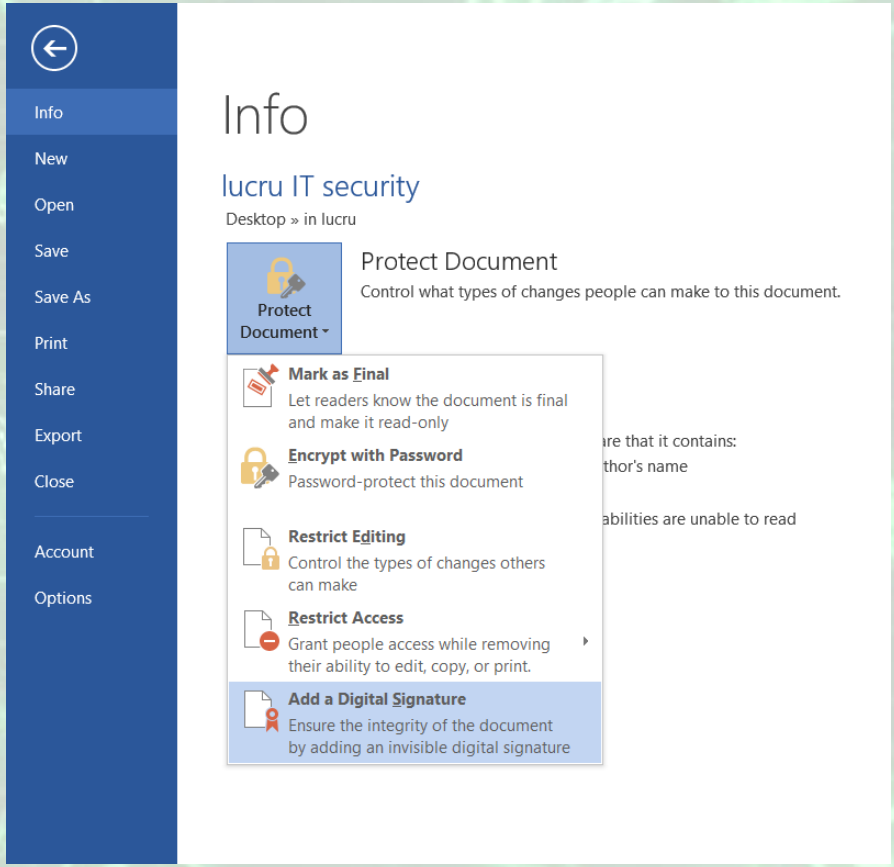
- În societatea informațională de astăzi, e-mailul este omniprezent, peste 2 milioane de e-mailuri fiind trimise în fiecare secundă pe glob. Ca urmare, riscurile scurgerilor de informații prin intermediul e-mailului sunt foarte mari atât pentru companii, cât și pentru persoane fizice. Furtul de identitate, expunerea datelor confidențiale și pierderea încrederii clienților sunt doar câteva din pericolele la care vă expuneți.
- Atunci când trimiteți un e-mail, acesta traversează mai multe computere până ajunge la destinatar. Având în vedere că nu cunoașteți unde sunt localizate aceste computere, cine sunt proprietarii lor sau cine le administrează, este recomandabil să securizați comunicarea prin email prin intermediul **criptării mesajelor**. Prin criptarea mesajelor, se reduce riscul accesului neautorizat la aceste mesaje. Astfel, e-mailul va parcurge criptat întregul canal de comunicație până la destinatar și orice interceptare a mesajului va rezulta într-un text neinteligibil. Prin decodificarea mesajului, folosind cheia de decriptare, destinatarul mesajului va transforma emailul într-o formă lizibilă.
- Avantajele criptării emailurilor sunt:
  - **Confidențialitate** - emailurile criptate nu pot fi interceptate și citite
  - **Integritate** - emailurile necriptate pot fi ușor falsificate, iar prin criptare vă asigurați că nimeni nu va schimba conținutul emailului fără alertarea destinatarului
  - **Autenticitate** - cheia de criptare/decriptare este specifică expeditorului și garantează faptul că emailul provine de la expeditor și nu de la o altă persoană.

5.1.2. Semnătura digitală

- Semnătură digitală este cel mai important instrument de securitate electronică, folosit pentru a autentifica semnatarul unui document și pentru a garanta integritatea datelor transmise.
- Semnătura digitală nu este o semnătură scanată sau o hologramă, ci reprezintă datele autentice în format electronic (un cod special, o amprentă digitală) ale unui utilizator. Anumite aplicații din suita Microsoft Office (Word, Excel, PowerPoint) oferă posibilitatea introducerii unei semnături digitale în document pentru a autentifica utilizatorul și integritatea datelor, însă nu protejează confidențialitatea datelor întrucât nu oferă opțiuni de criptare a acestora.
- Există de asemenea și semnătura digitală extinsă care, pe lângă proprietățile unei semnături digitale normale, oferă și facilități de criptare a datelor, folosind cheia criptografică a expeditorului. Aceasta face ca semnătura să fie unică atât pentru fișier cât și pentru deținătorul cheii, oferindu-se astfel atât integritate cât și autentificare. Orice modificări aduse documentului afectează semnătura.
- Semnăturile digitale utilizează criptarea asimetrică, în care se folosește o cheie pentru a crea semnătura și o altă cheie, legată de prima, pentru a o verifica.

5.1.3. Crearea și adăugarea unei semnături digitale

- Pentru adăugarea unei semnături digitale, se urmează pașii de mai jos:
  - Executați click pe butonul **File** (Fișier) și alegeți opțiunea Info (Informații).
  - Apăsați butonul Protect Document (Protejare document) și alegeți opțiunea **Add a Digital Signature** (Adăugare semnătură digitală).



5.1.4. Conștientizarea posibilității de a primi mesaje frauduloase și nesolicitate

- Datorită costului redus și transmiterii rapide a mesajelor, multe firme își fac reclamă prin intermediul poștei electronice. De aceea, este recomandat să nu faceți cunoscută adresa dumneavoastră de mail decât persoanelor de încredere deoarece, în caz contrar, puteți primi diferite mesaje fără a cunoaște cine este expeditorul acestora.
- Aceste mesaje pot conține link-uri virusate sau frauduloase, fișiere atașate virusate, ce în aparență sunt inofensive (documente, prezentări powerpoint etc). De preferat este să ștergeți aceste mesaje imediat cum le primiți sau să scanați împotriva virușilor fișierele atașate. În caz contrar există pericolul infectării calculatorului cu viruși, acest lucru determinând funcționarea necorespunzătoare a aplicațiilor și a sistemului de operare sau chiar pierderea datelor existente în calculator.

5.1.6. Înțelegerea termenului phishing. Identificarea caracteristicilor specifice phishing-ului: utilizarea numelor unor persoane sau companii legitime, linkuri web false

- Phishing-ul (derivat din termenul din limba engleză pentru "pescuit") se referă Ia o formă de activitate frauduloasă care constă în obținerea unor date confidențiale, cum ar fi datele folosite în aplicații bancare (online banking), aplicații de comerț electronic sau informații referitoare la cardurile de credit, folosind tehnici de manipulare a datelor datelor identității unei persoane sau unei instituții.
- Un atac de tip phishing constă în trimiterea de către atacator a unui mesaj electronic în care utilizatorul este sfătuit să divulge date confidențiale pentru a câștiga anumite premii sau este informat că, datorită unor defecțiuni tehnice ce au dus la pierderea datelor originale, este necesară retransmiterea acestor date confidențiale.
- Informațiile cerute sunt de obicei:
  - Numărul cardului de credit/ debit;
  - Codul PIN pentru ATM;
  - Informații despre contul bancar;
  - Codul numeric personal/ contul de asigurare;
  - Conturi de e-mail, parole etc.
- In mesajul electronic primit, utilizatorul este direcționat spre un site clonă (un site ce pare identic cu site-ul unei instituției bancare, licitații online etc) unde este invitat să completeze un formular cu datele confidențiale. Trebuie să ținești cont de faptul că organizațiile oficiale nu trimit niciodată astfel de mesaje, care solicită informații personale.

5.1.6. Conștientizarea pericolului de infectare a computerului cu viruși la deschiderea unui fișier atașat unui email, ce conține un macro sau un fișier executabil

- Mesajele electronice pot conține atașamente ce conțin viruși, destinați infectării computerului dvs. cu diverse tipuri de malware.
- Unul dintre tipurile de viruși des utilizat în cadrul fișierelor atașate este **virusul macro**. Acesta se va folosi de funcționalitățile Visual Basic for Applications (VBA) oferite de unele programe (cum ar fi Microsoft Office) de a crea macrocomenzi. Dacă utilizatorul va folosi facilitățile oferite prin crearea de macrocomenzi pentru automatizarea anumitor activități, virusul va folosi această facilitate pentru a se răspândi și a-și îndeplini scopul distructiv. Virușii de macro infectează fișierele de tip document și se răspândesc cu ajutorul documentelor transmise între utilizatori. În momentul când deschideți fișiere de tip Word, Excel, Powerpoint etc ce conțin macrocomenzi, sistemul de operare va afișa pe ecran un mesaj de avertizare prin care sunteți întrebat dacă permiteți sau nu rularea macrocomenzilor.
- Dacă fișierul provine dintr-o sursă de încredere, atunci puteți rula fără probleme macrocomenzile. Dacă fișierul provine de la o persoană necunoscută, este recomandabil să dezactivați rularea macrocomenzilor pentru a evita virusarea computerului. Dezactivarea unei macrocomenzi înseamnă nerularea ei, însă este posibil să nu puteți utiliza toate opțiunile din cadrul fișierului.

5.1.6. Conștientizarea pericolului de infectare a computerului cu viruși la deschiderea unui fișier atașat unui email, ce conține un macro sau un fișier executabil

- Un alt tip de virus este cel al **fișierelor executabile**. Acesta se atașează de fișierele de .**exe** sau .**com**. Acești viruși caută în mod special programe asociate sistemului de operare, se atașează de acestea astfel încât, la fiecare pornire a calculatorului ei să se poată replica și propaga. Din acest motiv, majoritatea serverelor resping fișierele de tip .exe întrucât le consideră potențiali viruși.