

Curs 6.

SECURITATEA ȘI

CONFIDENȚIALITATEA DATELOR

SECURIZAREA DOCUMENTELOR SUITEI MICROSOFT OFFICE. SECURITATEA MESAJELOR E-MAIL.

Aspecte privind securitatea documentelor în Microsoft Word

- Protecția documentelor prin parolă la deschidere (*Encrypt with Password*)
- Protecția documentelor la modificare:
 - prin parolă (*Password to modify*) - documentul va putea fi deschis, însă va putea fi salvat doar dacă se cunoaște parola de modificare, în caz contrar va putea fi salvat cu alt nume
 - deschidere doar în citire (*Read-only recommended*) - avertizarea de deschidere a documentului "doar în citire" pentru a se evita suprascrierea conținutului inițial (avertizarea se poate ignora)
 - restricții de editare privind modificări ale formatului (*Styles*) sau ale conținutului documentului (comentarii - *Comments*, formulare - *Forms*), pentru toți utilizatorii sau doar pentru anumiți utilizatori
 - marcare ca variantă finală (*Mark as Final*) și salvarea ca document *read-only*
 - restricționarea drepturilor de acces și editare, copiere sau tipărire prin conectarea la un server de management al drepturilor digitale (*Rights Management Server*)
 - adăugarea unei semnături digitale

Aspecte privind securitatea documentelor în Microsoft Word

Protecția documentelor prin parolă la deschidere (*Encrypt with Password*):

- pierderea parolei nu va mai permite accesul la conținutul documentului

Parole puternice:

- combinație de litere mari, mici, cifre și simboluri;
- lungime de 14 caractere sau mai mult, când este posibil;
- varietate cât mai mare a simbolurilor utilizate;
- parole diferite pentru servicii diferite;
- păstrarea parolelor într-un loc sigur;
- nu folosiți:
 - înșiruiți de litere ce pot fi "ghicite" (cuvinte existente în orice limbă; scrise invers citirii normale; abrevieri);
 - secvențe repetitive de caractere;
 - caractere adiacente pe tastatură (*qwerty*) sau în alfabet;
 - cifre consecutive;
 - informații personale (nume, data nașterii, număr card bancar etc.).
- Testarea complexității unei parole: www.passwordmeter.com

Aspecte privind securitatea documentelor în Microsoft Word

Marcare ca variantă finală (*Mark as Final*) și salvarea ca document *read-only*

- indică faptul că editarea este completă și că acea variantă este versiunea finală
- se setează proprietatea “document read-only” pentru a interzice modificarea
- apăsarea butonului Edit Anyway va permite totuși editarea documentului și eliminarea status-ului *read-only*

Certificatul digital

- este o informație atașată unui document, proiect de macro-comenzi sau mesaj de poștă electronică prin care:
 - se garantează **autenticitatea** acestuia (faptul că provine de la cel care se declară autorul său);
 - se asigură **criptarea securizată** (cu chei publice);
 - se furnizează o **semnătură electronică** verificabilă.
- poate fi emis de:
 - **autorități de certificare recunoscute la nivel mondial** - furnizori comerciali de certificate digitale (*Certification Authority*) - CertPlus, Entrust, GeoTrust, GlobalSign, Thawte, Verisign etc.
 - **un grup intern dintr-o companie sau organizație**, care acționează ca autoritate de certificare locală
 - **autorul însuși, prin auto-semnare** ("self-signed") - acest tip de certificat nu verifică și nu garantează identitatea semnatarului, ci doar faptul că informația este nealterată (nemodificată) de la ultima semnare digitală

Certificatul digital

1. Crearea și verificarea unui certificat digital autosemnat – Selfcert.exe
2. Vizualizarea proprietăților unui certificat digital
3. Aplicarea unui certificat digital (semnarea digitală a unui document)

Aspecte privind confidențialitatea datelor în Microsoft Word

Înainte ca documentul să devină public este recomandabilă **eliminarea** unor meta-date salvate odată cu documentul:

- proprietățile documentului (autor, cuvinte cheie, companie, manager);
- comentarii, revizii, versiuni.

Niveluri de securitate în Microsoft Office

Trust Center - ansamblu de opțiuni, informații și recomandări privind securitatea și confidențialitatea datelor:

- liste cu dezvoltatorii, folderele și fișierele considerate "de încredere" (*trusted*)
- opțiuni privind executarea modulelor adăugate (*add-ins*) și a controalelor ActiveX
- opțiuni privind executarea macro-comenzilor (secvențe de cod scrise în VBA)
- avertizări la deschiderea documentelor din surse nesigure (Internet, e-mail sau foldere potențial nesigure - ex. Temporary Internet Files)
- restricții privind deschiderea sau salvarea anumitor formate de fișiere

Aspecte privind securitatea foilor de calcul în Microsoft Excel

Protecția registrelor de lucru la deschidere: prin parolă la deschidere (*Encrypt with Password*)

Protecția registrelor de lucru la modificare:

- prin parolă (*Password to modify*) - registrul de lucru va putea fi deschis, însă va putea fi salvat doar dacă se cunoaște parola de modificare, în caz contrar va putea fi salvat cu alt nume
- deschidere doar în citire (*Read-only recommended*) - avertizarea de deschidere a registrului de lucru "doar în citire" pentru a se evita suprascrierea conținutului inițial (avertizarea se poate ignora)
- marcarea ca variantă finală (*Mark as Final*) și salvarea ca registru de lucru *read-only*
- restricții de editare privind o foaie de calcul Excel (*Protect Sheet*)
 - blocarea celulelor unei foi de calcul Excel (*Locked*)
 - ascunderea formulei dintr-o celulă Excel (*Hidden*)
 - setarea unei parole pentru o celulă Excel
- protejarea structurii unui registru de lucru Excel (*Protect Workbook*)
- restricționarea drepturilor de acces și editare, copiere sau tipărire prin conectarea la un server de management al drepturilor digitale (*Rights Management Server*)
- adăugarea unei semnături digitale

Aspecte privind securitatea foilor de calcul în Microsoft Excel

Marcare ca variantă finală (*Mark as Final*) și salvarea ca document *read-only*

- indică faptul că editarea este completă și că acea variantă este versiunea finală
- se setează proprietatea “document read-only” pentru a interzice modificarea
- apăsarea butonului Edit Anyway va permite totuși editarea documentului și eliminarea status-ului *read-only*

Aspecte privind securitatea foilor de calcul în Microsoft Excel

Restricții de editare privind o foaie de calcul Excel (*Protect Sheet*)

Pas 1: se setează proprietățile dorite (Format Cells -> Protection)

- blocarea (interzicerea modificării) celulelor unei foi de calcul Excel (*Locked*)
- ascunderea formulei dintr-o celulă Excel (*Hidden*)

Pas 2: se protejează foaia de lucru (Review -> Protect Sheet) privind:

- posibilitatea de selectare a celulelor blocate/neblocate
 - formatarea celulelor
 - inserarea/ștergerea rândurilor/coloanelor
 - utilizarea altor instrumente (sortare, filtrare, tabele pivot etc.)
-
- posibilitatea setării unei parole
 - pasul 2 este necesar pentru aplicarea proprietăților de la pas 1

Aspecte privind securitatea foilor de calcul în Microsoft Excel

Restricții de editare privind o foaie de calcul Excel (*Protect Sheet*)

- pentru anumiți utilizatori și pe baza unei parole opționale, se poate permite editarea unei zone de celule (*Allow Users to Edit Ranges*)

Protejarea structurii unui registru de lucru Excel (*Protect Workbook*)

- se dezactivează posibilitatea de modificare a structurii curente a registrului de lucru (adăugare/ștergere/mutare/redenumire/ascundere foi de calcul)
- posibilitatea setării unei parole

Aspecte privind confidențialitatea datelor în Microsoft Excel

Înainte ca registrul de lucru să devină public este recomandabilă **eliminarea** unor meta-date salvate odată cu documentul:

- proprietățile documentului (autor, cuvinte cheie, companie, manager);
- comentarii, revizii, versiuni;
- foi de lucru ascunse, conținut invizibil etc.

Aspecte privind securitatea prezentărilor în Microsoft Powerpoint

Protecția prezentărilor la deschidere: prin parolă la deschidere (*Encrypt with Password*)

Protecția prezentărilor la modificare:

- prin parolă (*Password to modify*) - prezentarea va putea fi deschisă, însă va putea fi salvată doar dacă se cunoaște parola de modificare, în caz contrar va putea fi salvată cu alt nume
- deschidere doar în citire (*Read-only recommended*) - avertizarea de deschidere a prezentării "doar în citire" pentru a se evita suprascrierea conținutului inițial (avertizarea se poate ignora)
- marcarea ca variantă finală (*Mark as Final*) și salvarea ca prezentare *read-only*
- restricționarea drepturilor de acces și editare, copiere sau tipărire prin conectarea la un server de management al drepturilor digitale (*Rights Management Server*)
- adăugarea unei semnături digitale

Aspecte privind securitatea prezentărilor în Microsoft Powerpoint

Marcare ca variantă finală (*Mark as Final*) și salvarea ca prezentare *read-only*

- indică faptul că editarea este completă și că acea variantă este versiunea finală
- se setează proprietatea “document read-only” pentru a interzice modificarea
- apăsarea butonului Edit Anyway va permite totuși editarea prezentării și eliminarea status-ului *read-only*

Aspecte privind confidențialitatea datelor în Microsoft Powerpoint

Înainte ca prezentarea să devină publică este recomandabilă **eliminarea** unor meta-date salvate odată cu prezentarea:

- proprietățile prezentării (autor, cuvinte cheie, companie, manager);
- comentarii, revizii, versiuni;
- foi de lucru ascunse, conținut invizibil etc.

Aspecte privind securitatea datelor în Microsoft Outlook

- parolă pe fișierul de date Outlook
- debifarea opțiunii “Remember password” în setările contului e-mail
- restricții asupra mesajului (de exemplu să nu permită Forward) prin conectarea la un server pentru managementul drepturilor digitale (*Rights Management Server*)

Aspecte privind securitatea datelor în Microsoft Outlook

Filtru anti-spam

- marcarea mesajelor nedorite ca *Junk E-mail* în urma unei analize complexe a unor factori: numele sau adresa expeditorului, titlul mesajului, conținutul sau cuvinte cheie din corpul mesajului
- mai multe niveluri de protecție
- mesajele spam sunt mutate automat în folderul *Junk E-Mail*
- posibilitatea definirii unor liste cu:
 - expeditori siguri (adrese e-mail sau nume de domenii), inclusiv adresele din agenda personală (*Address Book*) - ex: nume@companie.com
 - destinatari siguri - ex: @companie.com
 - expeditori blocați - ex: nume@domeniu.com
 - nume de domenii web (TLD) blocate - ex: .cn
 - codări ale textului blocate - ex: Cyrillic

Aspecte privind securitatea datelor în Microsoft Outlook

Trust Center:

- securizarea unui mesaj e-mail folosind un certificat digital:
 - criptarea conținutului și a fișierelor atașate
 - semnarea digitală a mesajului
 - importul/exportul certificatelor digitale instalate în sistem
- blocarea previzualizării fișierelor atașate mesajelor e-mail
- blocarea afișării automate a imaginilor inserate într-un mesaj e-mail
- vizualizarea tuturor mesajelor e-mail ca text simplu, indiferent de formatul lor nativ