



User Security Awareness

The University of Iowa
Information Security Day
December 2005

[Topics]

- Confidential Information
- Accounts and Passwords
- Workstation Security
- “Malware”
- University Security Policy

What is Confidential Information?

Examples of Confidential Information

- **Student** Records: grades, transcripts
- **Health** Records: employee or patient health/leave, medical research data
- **Financial** Records: credit cards/info, financial aid, student loans
- **Administrative** Records: payroll, budget, grants, General Ledger

[Confidential Information]

- Federal Regulations:
 - FERPA – Family Educational Rights and Privacy Act
 - Protection of education records
 - HIPAA – Health Insurance Portability and Accountability Act
 - Protection of health records
 - GLBA – Gramm Leach Bliley Act
 - Protection of financial records

[Confidential Information]

- Your Responsibilities
 - Access is based on “need to know”
 - Secondary use, secondary copies
 - Authorization required for additional purposes
 - Proper disposal is important
 - Shred printed reports containing CI
 - Delete data files when no longer needed
 - Data Classifications
 - Public, Internal, and Restricted
 - See Institutional Data Access policy

Questions

- What is the best way to dispose of confidential information in an office?
 1. Place it in the office recycle bin
 2. Tear it up and throw it away
 3. Shred it and then recycle

Questions

- What is the best way to dispose of confidential information in an office?
 1. Place it in the office recycle bin
 2. Tear it up and throw it away
 3. **Shred it and then recycle**

[Questions]

Who is responsible for protecting confidential information?

1. Management personnel
2. Security personnel
3. Server Administrators
4. All employees

[Questions]

- Who is responsible for protecting confidential information?
 1. Management personnel
 2. Security personnel
 3. Server Administrators
 4. **All employees**

[Accounts and Passwords]

- Protect your Account and Password
 - Don't share it with ANYONE
 - Don't store password in an accessible place
 - Emergency disclosure **requires** an immediate change
 - You are responsible for all use of your hawkid and password

[Accounts and Passwords]

- Change your password frequently
 - Change at Windows login or <http://hawkid.uiowa.edu>
 - Change as often as you wish, but **must** change every 90-180 days
 - If you suspect someone knows it, change it
 - Report requests for your password
 - Tell your supervisor or call the IT Security Office

[Accounts and Passwords]

- Choose a “strong” password
 - At least 8 characters long
 - 2 numbers and 2 letters required
 - *Should* use mixed case and special characters
 - Don’t use words found in dictionaries
 - Don’t use your name, account, etc
 - Don’t use HawkID password on non-University systems

Accounts and Passwords

- Ideas for choosing a password...
 - Personal events?
 - “My daughter Anne turns 9 June 12!”
 - Mdat9j12!
 - “Went to a party at Jack’s May 5”
 - wtaPaJ’s55
 - Song Lyrics?
 - “It’s been a hard days night”
 - l5bahd8n.
 - Book Titles, Movies, Famous Quotes, ...
 - “The Lord of the Rings, Fellowship of the Ring”
 - tl0R,f0tR
- OR ... use a “Pass Phrase” (sentence)
 - Any of the above (event, lyrics, title, quote)

[Questions]

- Which of the following is an acceptable password?
 1. G0Hawk5
 2. Susan89
 3. Pa55w0rd
 4. Mdi17j29

Questions

- Which of the following is an acceptable password?
 1. G0Hawk5
 2. Susan89
 3. Pa55w0rd
 4. **Mdi17j29**

[Questions]

- What is the best way to remember your password?
 1. Write it down and hide it in your drawer
 2. Use personal information such as your birthday, address, or kid's name
 3. Tell it to your secretary
 4. Use a "pass phrase"

Questions

- What is the best way to remember your password?
 1. Write it down and hide it in your drawer
 2. Use personal information such as your birthday, address, or kid's name
 3. Tell it to your secretary
 4. **Use a “pass phrase”**

Questions

- If you receive a call from someone claiming to need your password, what should you do?
 1. Refuse and report it to your supervisor
 2. Tell them your password and then change it the next day
 3. Send it to them in an e-mail message

Questions

- If you receive a call from someone claiming to need your password, what should you do?
 1. **Refuse and report it to your supervisor**
 2. Tell them your password and then change it the next day
 3. Send it to them in an e-mail message

[Questions]

- You go to a website and it asks if you want to save your password in your browser. You
 1. Click “yes” and save your password
 2. Click “no” and don’t save your password
 3. Click “X” to close the box

[Questions]

- You go to a website and it asks if you want to save your password in your browser. You
 1. Click “yes” and save your password
 2. **Click “no” and don’t save your password**
 3. Click “X” to close the box

[Workstation Security]

- An unlocked, unattended workstation is a security risk!
 - Programs open, logged in can be used with your identity and access rights
 - Files in mapped network drives are accessible
- Use a screen saver with password protection
- Use the “Lock Computer” function
 - On Windows, press CNTL-ALT-DEL and then press Enter; press CNTL-ALT-DEL and enter your password again to unlock it

[Workstation Security]

- It is YOUR responsibility to work with local IT staff to ensure:
 - All important files are backed up
 - All computer software is regularly patched and updated
 - A firewall is turned on (either locally or in front of you on the network)
- Laptops are a special case!
- If you don't know who this is, **FIND OUT**

[Questions]

- What is the best way to protect your computer when you go to lunch?
 1. Turn off the monitor
 2. Lock your computer
 3. Close all your programs

[Questions]

- What is the best way to protect your computer when you go to lunch?
 1. Turn off the monitor
 2. **Lock your computer**
 3. Close all your programs

[Questions]

- If someone uses your computer after you've logged in, whose privileges will they have?
 1. Their own
 2. Yours
 3. Guest privileges

[Questions]

- If someone uses your computer after you've logged in, whose privileges will they have?
 1. Their own
 2. **Yours**
 3. Guest privileges

Questions

- If someone sends President Skorton a message using the e-mail program on your machine, who will he see the message is from?
 1. The person who sent it
 2. An anonymous person
 3. His secretary
 4. You

Questions

- If someone sends President Skorton a message using the e-mail program on your machine, who will he see the message is from?
 1. The person who sent it
 2. An anonymous person
 3. His secretary
 4. **You**

[“Malware”]

- Malicious Software = Malware
 - Viruses, trojans, worms, spyware and “bots” (robots – package of evil)

[“Malware”]

- How might my computer get Malware?
 - Popups
 - Phishing e-mail
 - Used to be attachments, now its primarily malicious links
 - Instant Messenger
 - Poorly managed computer (not patched)

[“Malware”]

- Non-Windows computers aren't immune
- Alternative browsers (other than IE) are not immune

[Preventing Malware]

- Never click links in doubtful e-mails
- Use Symantec Antivirus program
- Use Malware scanners
 - Spybot, MS AntiSpyware (beta)
- Don't interrupt scans
- Always reboot when prompted after updates

[Questions]

- You receive an e-mail saying you need to verify your account information. You should
 1. Click on the link and answer the questions
 2. Reply to the message saying “no”
 3. Delete it

[Questions]

- You receive an e-mail saying you need to verify your account information. You should
 1. Click on the link and answer the questions
 2. Reply to the message saying “no”
 3. **Delete it**

[Questions]

- E-mail messages with attachments are safe because the University blocks the harmful ones.
 1. True
 2. False

[Questions]

- E-mail messages with attachments are safe because the University blocks the harmful ones.
 1. True
 2. **False**

[Questions]

- My computer can't get a virus because it has the Symantec Anti-Virus program installed on it.
 1. True
 2. False

[Questions]

- My computer can't get a virus because it has the Symantec Anti-Virus program installed on it.
 1. True
 2. **False**

University Security Policy

- You must report all computer security incidents
 - To your supervisor or DEO
 - OR -
 - To the IT Security Office
 - Call 5-6332
 - E-mail to security@uiowa.edu
- Examples: password breach (sharing or stealing), malware, unauthorized access to information, misuse or suspicious activity, software piracy

University Security Policy

- Roles and Responsibilities for Information Security
 - User
 - Use data as authorized by business owner
 - Data Custodian
 - Technical person(s) with operational protection responsibility, typically IT staff
 - Business Owner of Data
 - Senior official accountable for managing information assets
- See <http://cio.uiowa.edu/policy/policy-roles-and-responsibilities.htm> for details

[Questions]

- A co-worker asks you to look up some confidential information because she doesn't have "enough" access. You should
 1. Look it up and give her the information
 2. Give her your password so she can get it herself
 3. Refer her to your supervisor to request the access
 4. Immediately report it to the Security Office

[Questions]

- A co-worker asks you to look up some confidential information because she doesn't have "enough" access. You should
 1. Look it up and give her the information
 2. Give her your password so she can get it herself
 3. **Refer her to your supervisor to request the access**
 4. Immediately report it to the Security Office

Questions

- An e-mail message you did not write and did not send is in your “Sent Items” folder. You should
 1. Report the problem to your supervisor and immediately change your password
 2. Delete the message
 3. Complain to your local IT support that your e-mail is broken

Questions

- An e-mail message you did not write and did not send is in your “Sent Items” folder. You should
 1. **Report the problem to your supervisor and immediately change your password**
 2. Delete the message
 3. Complain to your local IT support that your e-mail is broken

[Best Practices for you]

- Respect data confidentiality
- Never share your password
- Lock your workstation
- Report problems

[Security is everyone's job!]

- If you are unsure, ask someone!
- Information security is not only the responsibility of your local IT support