IT Security Awareness

United States District Court – District of Maryland

1

The Goal of IT Security Awareness

About IT Security Awareness Training

- The security of the information we store on our computers, as well as the hardware needed to access it is instrumental to our jobs and to the court.
- Our computers once connected to the internet are being attacked at least a few hundred times every hour.
- Sometimes threats can be let in by accident.
- Unfortunately, other times some individuals exploit the Internet through criminal behavior and other harmful acts.
- For these reasons employees, contractors, and temporary employees are required to complete computer security training.
- Completion of this course will provide participants with the capabilities needed to access and use the court's Information Technology assets.

3

Some Recommendations

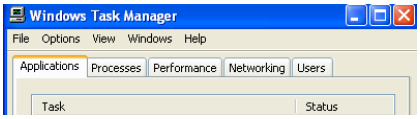
- Utilize automatic updates for your operating system and applications
- Keep your browser up-to-date – Go to **Help**> **About** for the browser version

- You can easily upload any file (up to 20MB) to VirusTotal.com and have it scanned by a 35 different antivirus engines, including ones from Kaspersky, McAfee, and Symantec

4

Avoid Clicking on Pop-ups

- Select **Ctrl+Alt+Del** >> click **Task List** >> under the Applications tab highlight the application >> click **End Task**
- Never click "Yes," "Accept" or even "Cancel", because it could be a trick that installs software on your PC



5

Turn on Personal Firewall

- It monitors traffic entering and leaving your computer
- Checks for suspicious patterns indicating the presence of malware or other malicious activity

6

Antivirus for Judiciary Users

- Court employees are entitled to use Symantec EndPoint Antivirus for their home PCs for as long as they are employed with the Judiciary:
  - Symantec EndPoint Protection for Workstations
  - Norton Antivirus for the Mac

7

What if My Computer Still Becomes Infected?

- Antivirus protection software does not provide a 100% security guarantee

8

Free Malware Tools

MALWARE BYTES

http://www.malwarebytes.org/

SPYBOT SEARCH & DESTROY

http://www.safer-networking.org/en/download/index.html

9

Sensitive Information - Printing

- Don't leave important, sensitive, or confidential material lying around the office.
- Common printing areas are frequented by people coming and going. Often you will be in line to pick up your documents and others may handle them before you do. This leads to unnecessary information disclosures.

- Always use the closest print station, or a dedicated printer for confidential information, and go get it right away!

10

Sensitive Information Physical Security

- When faxing documents containing sensitive information, promptly retrieve the original from the sending fax machine and alert the recipient to promptly retrieve the copy from the receiving fax machine.

- When expecting a faxed document containing sensitive information, watch the fax machine closely and retrieve the fax as soon as it arrives.
- Do not leave this information in an unattended or unlocked copy or conference room.

11

2

Passwords & Unauthorized Access

Why Simple Passwords
Are Easy To Crack

- Many people put leading or trailing digits on dictionary words – e.g., buddy123
- Crack programs usually try such combinations first
- On the other hand, bu1d2d3y will be harder to crack because crack programs don't have the computing power to try all the combinations for permutations of buddy123 that include embedded digits or special characters

13

Check Your Password Strength
Using Microsoft's Password Checker

Weak Password

Strong Password

https://www.microsoft.com/protect/fraud/passwords/checker.aspx?WT.mc_id=Site_Link

14

Password Habits To Avoid

2. Don't use:
   a. User ID
   b. Names of family members or pets
   c. SS#, DOB, phone numbers
   d. Information about you that could be readily learned or guessed
   e. Don't post them where it can be viewed by others
   f. Also, avoid dictionary words

15

Tips for Creating… and Remembering Strong Passwords

- Use the first letters of a sentence or phrase that is meaningful to you.
- Make some of the letters uppercase, include numbers and special characters for increased strength.
- Example: **E**very **G**ood **B**oy **D**eserves **F**udge → **Eg18bdF!**
- Example: **I**s **E**con **2**20 **B**eing **O**ffered **T**his **S**emester? → **IE2bots?**

16

Passwords – Can I Write Them Down?

Insecure Password Location

Secure Password Location

If you have to write down your password keep it in a secure location
- E.g. **BlackBerry Password Keeper** (be sure to keep an additional copy)
- **Password Safe:** http://passwordsafe.sourceforge.net/
- **Password Vault:** http://www.pvault.com/

17

Preventing Unauthorized Access

- Press **Ctrl+Alt+Del > Lock Workstation,** or **<Windows Logo> + L** when stepping away from your PC
- If leaving your PC unattended for an extended period of time > log off the network
- Add screen saver that will automatically lock your workstation – e.g. lock after 20 minutes of inactivity

18

3 Internet-Posted Content, Mobile Devices

Traveling and Mobile Devices

- If you have to travel with court-assigned mobile devices, do not travel with sensitive information that you will not need.
- Never place your mobile device in your checked luggage. For greater security turn your device off and keep a close view of them when going through airport security/customs screening.

20

Traveling and Mobile Devices, Cont'd

- If you are attending a conference or trade show, be especially wary—these venues offer thieves a wider selection of devices that are likely to contain sensitive information. Conference sessions and meal times offer more opportunities for thieves to access guest rooms in search of unattended laptops and other mobile devices.
- Do not leave electronic devices unattended, including in locked hotel rooms.
- Do not use public devices (e.g., computers supplied in hotel office centers or cyber cafes) for Judiciary business.

21

Posting Court-Sensitive Information Online

- The use of iPads and social networking present new challenges for securing court data
- Internet postings could have an indefinite life as information could be made public and searchable for a long time
- The use of "Cloud" technologies like Google Docs allow content to be stored on servers that are outside the court's jurisdiction

22

Once You Post Information Online

- You lose control of them
- Think before you type or upload an image

You are telling the world

You cannot take it back

23

How Can You Tell That a Website is Secure?

- Before submitting financial information through a website, make sure that the website is secure. How can you tell if a website is secure?
- You will notice either a closed lock or an unbroken key at the bottom of the browser window. You may also notice that the URL begins with [https://] ("s" stands for secure). While https:// by itself is not an indication of a secure site, when it is combined with the lock or the unbroken key, it indicates data is being encrypted as it crosses the Internet.

24

When Working in a Public Location

- Be aware of shoulder surfers -- people peering over your shoulder at what you might be working on

- Use a laptop privacy screen to prevent others from peeking at your work – especially if you are working on sensitive information

25

Public Wi-Fi

- Wireless public access like those in hotels and airports can allow others connected to that network to scan your device in search of sensitive information

- Avoid connecting with your court-assigned laptop

26

Utilize a Virtual Keyboard

- To protect against keylogging (though not fully secure)

- An example of a virtual keyboard can be found in Microsoft Windows XP by selecting **Start** >> **Programs** >> **Accessories** >> **Accessibility** >> **On-Screen Keyboard**

27

Never Plug an Unknown Flash Drive, CD, or DVD Drive into Your Computer

- The "autorun.inf" configuration file directs the operating system to automatically run a specified program which could contain malware

28

4

SOFTWARE, SOCIAL ENGINEERING, E-MAIL & SPAM

Social Engineering – Give It Up!

- Social engineering is in essence the art of persuasion—convincing individuals to disclose confidential data or perform some action like giving something up

30

Social Engineering email sample

E-Mail

ATTENTION ALL EMPLOYEES!!

THIS WEEK ONLY WE ARE JOINING FORCES WITH OUR MOST LUXURIOUS RESORTS PROVIDING AN UNFORGETTABLE VACATION. AS SUMMER ENDS, WE ARE OFFERING LUXURY CORPORATE VACATION PACKAGES FOR ALL EMPLOYEES AND THEIR FAMILY.

VACATION DETAILS

- DESTINATIONS: CANCUN, DOMINICAN REPUBLIC, YOU CHOOSE.....
- 5 DAYS 4 NIGHTS
- PACKAGES ARE OPEN ENDED FOR 12 MONTHS WITH NO BLACK OUT DATES
- PRICE $249.00 P/P

INCLUDED IN PACKAGE:

- RESORT STAY -4 TO 5 STAR ACCOMMODATIONS AT THE RESORT OF YOUR CHOICE
- CORPORATE MEAL PLAN -ALL MEALS AND DRINKS (ALCOHOL/NON ALCOHOL) INCLUDED
- CHILDREN UNDER 5 STAY AND EAT FOR FREE
- UNLIMITED ACTIVITIE, WHICH INCLUDES NON-MOTORIZED WATER SPORTS
- YOU MUST CALL NOW BEFORE WE RUN OUT.

CALL NOW TO BOOK YOUR RESERVATIONS:
1877-828-3451

Phishing
A form of Social Engineering

- It's a criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication like e-mail

Spear phishing
A Targeted Form of Phishing

- The apparent source of communication is likely to be an individual within the recipient's own circle

- For example, you may get an email from what looks like your friend inviting you to open pictures from a family gathering. You unsuspectingly click on the link and download malware to your PC

Incoming E-Mail

- Much of the email sent to our inboxes are unsolicited, and includes SPAM.

- Be careful opening email attachments, even looks like it's from a friend or coworker.

- Only open email attachments that you are expecting, or that are sent with a reasonable explanation.

- Encrypt or password protect email messages with attachments that contain sensitive information.

Adhere to Good Practices for E-mail Usage

- Question e-mails from **known** senders in which the subject line or content appears to be suspicious

Be Careful Opening Email Attachments

- Never open attachments with suspicious file extensions

- For example, .exe; .bat; .js; .cmd; .lnk

How to Scan E-mail Attachments

- Scan E-mail Attachments for viruses before opening
  - Save the attachment to your PC (e.g. Desktop)
  - Right click and select **Scan for Viruses…**

37

If You Send an Email
With an Attached File…

- Include a text message explaining what is included in that attachment
- If you suspect an email (or its attachment) is not legitimate, delete it unread

38

Sending Messages Via Internet

- Messages sent over the Internet should be treated as non-confidential
- Avoid using personal e-mail to send work-related correspondence

39

Peer-to-Peer Software Prohibition

- The Judicial Conference and Committee on Information Technology prohibits the use of peer-to-peer file sharing, chat rooms, and instant messaging for communicating with persons or entities outside the Judiciary's private data communications network

40

Peer-to-Peer File Sharing

- Peer-to-Peer file sharing involves using software that allows internet users to share files that are housed on their individual computers

LimeWire: P2P file-sharing application for music, video, pictures, games, text documents, etc.

Skype: Allows users to make voice calls over the Internet.

BitTorrent: Often used for distribution of very large files.

41

Software Download Dangers

- It may be tempting to download and install software that you can obtain for free on the Internet to your court PC

42

Software Downloads Dangers

- It may be tempting to download and install software that you can obtain for free on the Internet to your court-provided PC, but these tools may carry hidden costs.
- For example, they may cause other programs to stop working, display unwanted ads and even slow your PC. Not only that, but they may contain malicious code or spyware that can cause harm, including stealing confidential information.
- Users of court-provided PC's are prohibited from installing any type of software through CD's, disks or downloading to their court-provided PC. In addition, the court's software must be used according to the manufacturer's licensing agreement and United States Copyright laws.
- Personnel are not allowed to make illegal copies of copyrighted software.

43

But These Tools May Carry Hidden Costs

- They may cause other programs to stop working
- Display unwanted ads, annoying pop-ups, and even slow your PC
- They may contain malicious code or spyware that can steal confidential information

44

Fake-Antivirus

- Fake Antivirus has become an increasingly successful medium through which to spread malware.
- Through social engineering tactics users are tricked into downloading and installing Fake AV onto their PCs.
- For example, the user may see a pop-up ad advising that their PC is infected with viruses and suggesting that it be scanned in order to remove the viruses. If the unsuspecting user clicks on the pop-up malware is downloaded to their PC.
- You should avoid visiting suspicious-looking sites and do not download and install software to your work PCs.

45

Identity Theft

- Be Aware of the Causes
- Who can control it?
- You, co-workers, family members
- Shredding, wiping drives
- Practice to resist phishing
- Don't surf where you shouldn't
- Install controls at home; don't auto-save passwords
- Teach family members to manage information postings
- Banks
- Businesses
- Technologies

46

Summary

1. 
The Goal of IT Security

2. 
Passwords & Unauthorized Access

3. 
Internet-Posted Content, Mobile Devices

4. 
Software, Social Engineering E-mails & Spam

47

Congratulations!

You have successfully completed the Computer Security Awareness Training .

It's now time for the "QUIZ" portion of the training. This is a learning tool to help you review some of the main points of the program and will not be formally graded.

48

IT SECURITY QUIZ QUESTIONS

Quiz: Question #1

How might you tell that a computer security incident may have occurred?

A. Frequent system crashes.
B. Unexpected screen activities.
C. Attempted unauthorized access to you workstation.
D. All of the above.

Answer: Question #1

Correct Response (D) to Question #1

Correct!
By selecting "D", you recognize that frequent system crashes, unexpected screen activity, and/or attempted unauthorized access to your workstation are indicators of a computer security incident.

Wrong Response (A, B, C) to Question #1

Quiz: Question #2

When creating a password, users need to combine letters, symbols, and numbers so that the password is easy for you to remember and hard for someone else to guess.

A. True
B. False

Answer: Question #2

Correct Response (A) to Question #2

Correct!
A good password includes more than alphabet letters. The addition of numbers and symbols make a password harder to guess. You should choose a password that is not a dictionary word and is easy for you to remember.

Wrong Response (B) to Question #2

Quiz: Question #3

Why is "JUNIOR65" not a good password?

A. The password does not contain both lower and upper case letters.
B. The password does not contain a special character.
C. The password includes a word found in the dictionary.
D. All of the above.

Answer: Question #3

Correct Response (D) to Question #3

Correct!
Good passwords contain a combination of uppercase and lowercase letters, numbers, and special characters. In addition, good passwords do not include words that would be in a dictionary.

Wrong Response (A, B, C) to Question #3

Quiz: Question #4

How should you make backups of your information files?

A. Install anti-virus software.
B. Store your data on the [user personal drive] drive.
C. Completely shut down your system nightly.

Answer: Question #4

Correct Response (B) to Question #4

Correct!
Users are responsible for storing data on their [user personal drive] drive. The [user personal drive] drive is automatically backed up by the IT Department.

Wrong Response (A, C) to Question #4

Quiz: Question #5

It is acceptable to use your computer to visit an inappropriate web site using your work computer?

A. True
B. False

Answer: Question #5

Correct Response (B) to Question #5

Correct!
It is never acceptable to visit inappropriate web sites with your work computer. If, in the course of doing official business, you encounter an inappropriate site by accident, you should inform the Help Desk. Likewise, if a site is blocked that you believe should not be blocked, contact the Help Desk about making the site available.

Wrong Response (A) to Question #5

Quiz: Question #6

You are expecting a fax which contains Sensitive Information. You should:

A. Promptly retrieve the copy from the receiving fax machine.
B. Retrieve the copy from the receiving machine the following day.
C. Assume someone else will pick up the fax and place it in your mail slot.

Answer: Question #6

Correct Response (A) to Question #6

Correct!
When faxing documents containing Sensitive Information, promptly retrieve the original from the sending fax machine and alert the recipient to promptly retrieve the copy from the receiving fax machine. When expecting a faxed document containing Sensitive Information , watch the fax machine closely and retrieve the fax as soon as it arrives. When available, use fax machines located in secure rooms.

Wrong Response (B , C)to Question #6

Quiz: Question #7

You have received an email forwarded from someone you do not know. The email has a file attached. What do you do with the file?

A. Delete the email without opening the attachment.
B. Scan the file with anti-virus software before opening it.
C. Either A or B.

Answer: Question #7

Correct Response (C) to Question #7

Correct!
In this situation, you must evaluate the options and determine what controls and actions are most appropriate. Since you do not know the person who sent you the file, the safest action may be to delete the email without opening it. If you believe that the attachment is work-related and would be useful, be sure to scan the file with anti-virus software before opening it.

Wrong Response (A, B) to Question #7

Quiz: Question #8

A friend gave you a copy of a software program that you really like. You want to use it at work because you feel it will make you more productive. You should:

A. Install the software yourself.
B. Contact the Help Desk and wait for a technician to install the software.
C. Submit the software to the Help Desk requesting an approved licensed copy of the software.

Answer: Question #8

Correct Response (C) to Question #8

Correct!
All software use on computers must be approved by and used according to the manufacturer's licensing agreement and United States Copyright laws.

Wrong Response (A, B) to Question #8

Quiz: Question #9

You are working with Sensitive Information when a sales representative stops by to say hello. You should:

A. Ask him to sit down and chat for a while.
B. Place the Sensitive Information out of sight.
C. Show him what you are working on and ask for his services.

Answer: Question #9

Correct Response (B) to Question #9

Correct!
When unauthorized individuals are present, place Sensitive Information out of sight.

Wrong Response (A & C)to Question #9

Quiz: Question #10

As a computer user, your single most important Information Security responsibility is:

A. Recognizing and reporting known or suspected incidents.
B. Choosing a strong password and changing it often.
C. Familiarizing yourself with computer security regulations.
D. All of the above.

Answer: Question #10

Correct Response (D) to Question #10

Correct!
This is another one of those questions designed to get you thinking. All the choices are correct.

Wrong Response (A, B, C) to Question #10

End of IT SECURITY QUIZ QUESTIONS

- I _____ have completed the USDC of MD Security Awareness training course.

- Sign _____ Date:_____