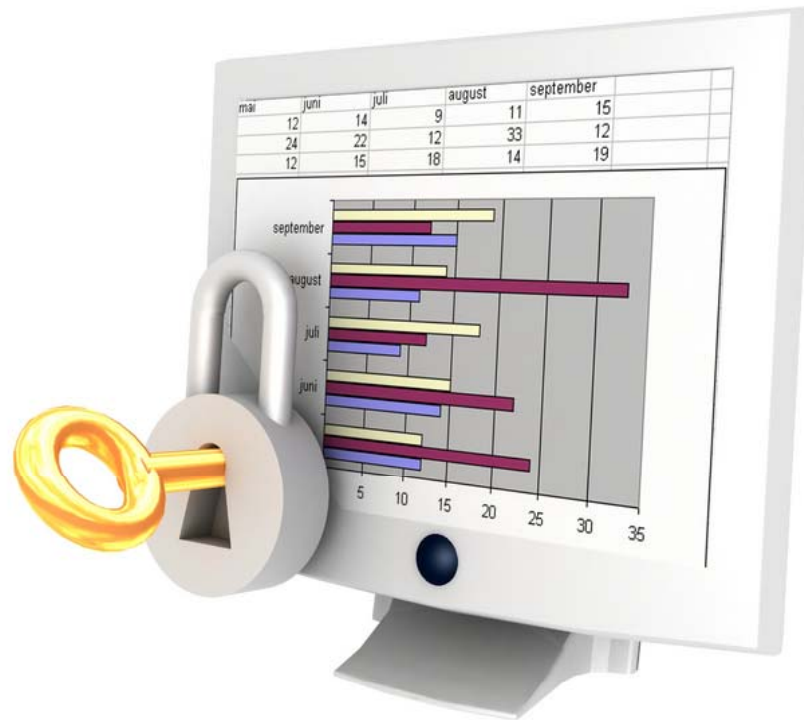


# IT Security Awareness

What you need to know...



## NABE Mid-Year Meeting – IT Workshop

February 2010 - by Bill Dickinson, IT Director Virginia State Bar

# Protecting IT Systems and Data

- Sensitive data that falls into the wrong hands can result in Identity theft
- Identify theft and the improper disclosure of sensitive data can cause harm and embarrass members, volunteers, and staff
- It is everyone's responsibility to protect sensitive data
- Here are few examples of sensitive data:
  - Social Security number (SSN)
  - Credit card number
  - E-mail Address
  - Personal information
  - Confidential legal data



# Why Worry About Security?

- Personal Privacy
- Professional Privacy
- Legal Liability
- Loss of Data and Equipment



# Why Worry About Security?

- Today many have the misconception that technology alone can solve all the security problems
- We all need to understand and be aware of the existence of internal and external threats
- Many lack understanding about the risks of using technology resources
- IT security is sometimes an afterthought

# Problems Hacker Cause

A hacker intrusion could create a legal liability and public embarrassment for you and your organization

- **Vandalism**—Destruction or digital defacement of a computer or its data for destruction's sake
- **Theft**—Gaining access to intellectual or proprietary technology or information, sometimes for resale
- **Hijacking**—Many of the financially motivated hackers are interested in remotely controlling PCs
- **Identity theft**—Electronic theft of personal info that can be used to steal financial resources
- **Terrorism**—Some experts believe that terrorists will eventually launch an attack using hacking techniques



# What Tools Can Hackers Use to Compromise Your Computer?

- Malware
- Denial of Service Attacks (DOS)
- Network Scanners and Probes
- Password Crackers



# Malware

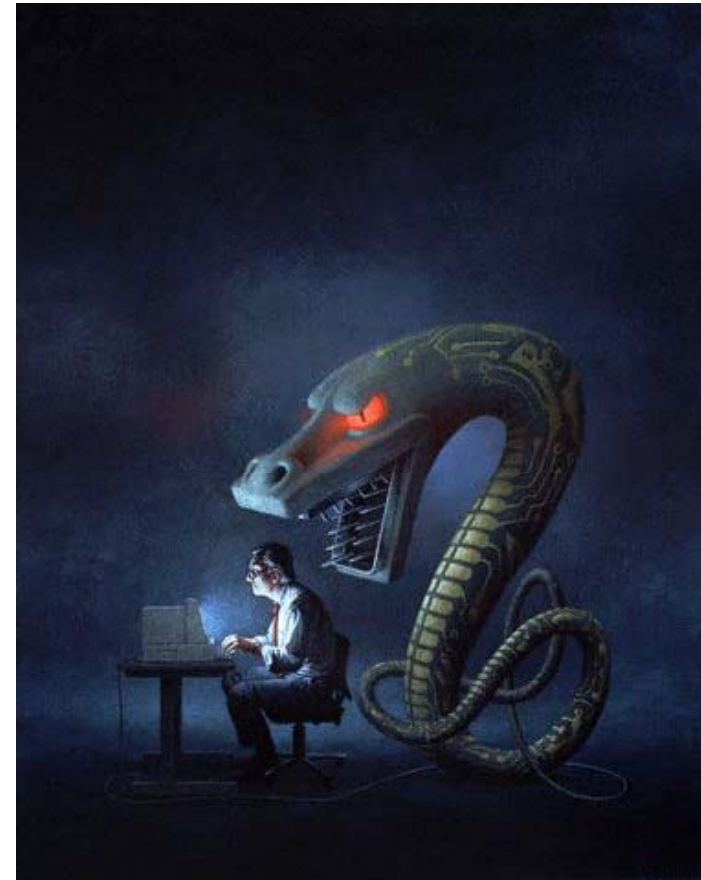


- **Malware** – (aka Crimeware and Computer Contaminant) is any program which can corrupt files and/or secretly report your information from your computer or network
- Viruses, Worms, Trojans, and Spyware are the most common types of malware
- Many of these destructive programs attempt to reinstall and replicate themselves and are designed to be very difficult to remove from the host computer

# Malware

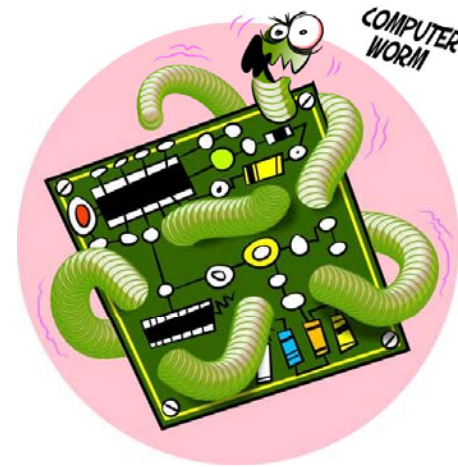
**Virus** - Software that gets installed on your computer, usually without your knowledge

- You can get “infected” by accessing something that is already infected with a virus
- Sources include floppy disk, USB drives, website, and e-mail



# Malware

**Worm** – Software that actively tries to spread itself to infect other computers



- Software worms can actively scan networks to infect others
- Worms can also be spread by e-mail applications that use the computer address book

# Malware



**Trojan** - Damaging software that hides its identity by posing as something else such as a screen saver or a greeting card. The Trojan, once installed, gives the attacker a back door into your system that can be used by the hacker as needed



# Malware

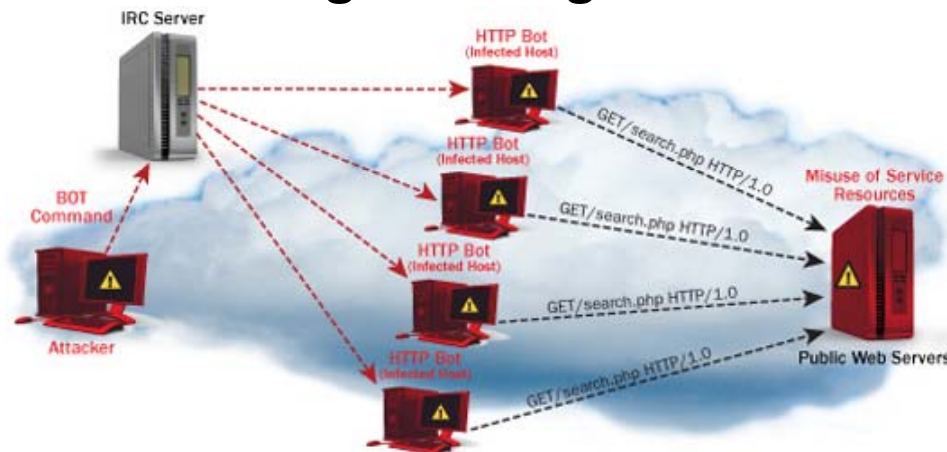


**Spyware** – A malicious data collection program designed to retrieve and log your Internet usage, website visits, and other information about your web browsing habits and then reports this back to it's source

# Denial of Service Attacks

**Denial of Service** is an attack designed to render a computer or network incapable of providing normal services

- The most common DOS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests can not get through



# Passwords

- The primary purpose of a password is to authenticate a user granting access to a secured resource
- Password are commonly the first layer of protection between your computer and the rest of the world



# Weak Passwords

- Any easy to guess common words
- Most are quickly solved by *password cracking programs*
- Weak Password Examples:
  - Common name (human, pet, fantasy character, etc...)
  - Double-words (kittykitty, mikemike, etc...)
  - Any Number (phone, ssn, license plate, birth date, etc...)
  - Any information that is easily obtained about you
  - Blank Password

# More Examples of Weak Passwords

- Words such as Jedi, Wizard, Guru, Gandalf, God...
- Passwords of all the same letter
- Simple patterns on the keyboard, like “qwerty “
- Reversals: terces, wordpass, nhojnhoj
- Any of the above preceded or followed by one or two digits especially 1 or 01

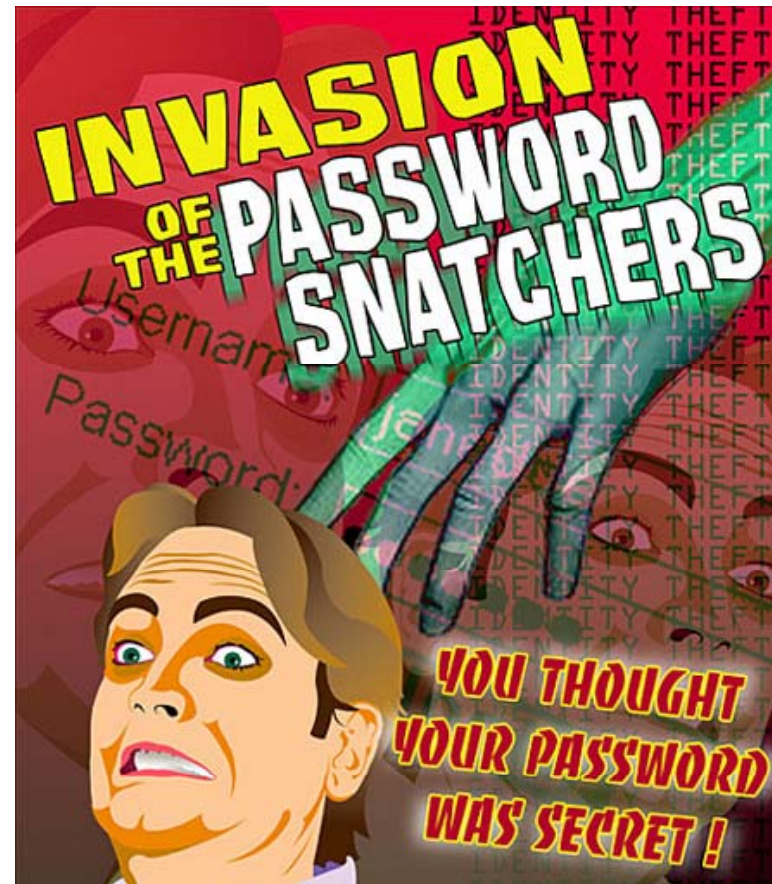
# Passwords - Weakest of the Weak

- password
- 123456
- qwerty
- abc123
- letmein
- computer
- myspace1
- password1
- summer
- (your first name)



# The Problem with Passwords

- Most folks find it hard to remember difficult passwords consisting of numbers and weird characters
- The number of passwords required by a single individual is growing constantly
- Software is available to hackers that contains complete dictionaries from several different languages and popular words from today's culture, movies, and books



# Techniques for Strong Passwords

- Use stronger passwords that are longer and more complex, making them more difficult to crack
- Choose passwords that are difficult or impossible to guess
- Assign unique passwords to each accounts



# Techniques for Strong Passwords



Use a minimum of 8 **characters** in you password



Make sure you use one or more **capital letters** (A...Z)



Include one or more **lower case letters** (a...z)



Include one or more **numbers** (0-9)



Use **special characters** (!, \*, &, %, \$, #,@) if possible.

# Password Best Practices

- Never display or conceal passwords in your work area, no matter how well-hidden
- If you feel that your password has been compromised in any way, change it immediately
- Don't let others watch as you type your password
- Don't use the same password more than once

# How Your Computer Can Be Compromised

- E-mail
- Network Intrusion
- Unsecured Location
- Social Engineering





# E-mail Vulnerabilities

- Now the most widely used method of communication
- Unfortunately it is not the safest or most reliable
  - Do not open e-mail attachments from anyone who is a stranger; the subject line or attachment name is often alluring
  - Do not open e-mail attachments that arrive unexpectedly. It is possible that the e-mail was sent without the sender's knowledge from an address book of an infected computer
  - Do not open executable attachments with an extension of exe, vbs, bat, scr, com, etc.



# E-mail Vulnerabilities

## Sensitive Data

- Don't assume that all e-mail messages are private
- Avoid sending sensitive data, passwords, and personal information via e-mail
  - encrypt the information being transmitted
- Always ensure that you have updated security patches for the e-mail client software

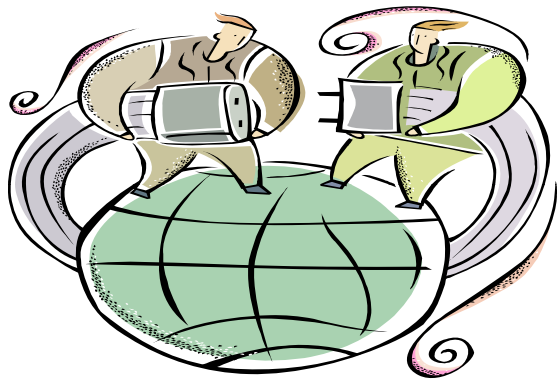


# E-mail Vulnerabilities

## Viruses

- Viruses and other types of malicious code are often spread as attachments to electronic mail messages
  - If you must open an attachment from an unknown source contact the IT department for help
  - Do not send programs or e-mails to friends or coworkers simply because they are amusing - it might be malware

# Network Intrusion



Today, most computers are connected to some sort of network providing access to the world. The following are ways to protect your computer from being compromised:

- Power down your computer when not in use for extended periods of time
- Logout of your computer when not in use

# Unsecured Location



- Make sure your computer is not left unattended in a public place
- If your computer is located in an unsecured physical location use a security cable to help prevent theft
- An unattended unsecured computer left alone even for a few minutes can give access to your data
- Use a password protected screensaver

# Safe Web Browsing

- Use and maintain anti-virus software, a firewall, and anti-spyware software
- Keep software, particularly your web browser, up to date – install software patches
- Evaluate your software's security settings – hackers can take advantage of low security settings
- Do on-line business with reputable vendors - before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor



# Safe Web Browsing

- Take advantage of security features - passwords and other security features add layers of protection if used appropriately
- Be wary of e-mails requesting information - legitimate businesses will not solicit this type of information through e-mail
- Check privacy policies before providing personal or financial information
- Make sure your information is being encrypted - many sites use SSL. Look for a URL that begins with "https:" instead of "http:" and a lock icon in the bottom right corner of the browser window
- Check your statements - keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements



# Safe Web Browsing

## Where's Waldo?

If he has been on the web someone knows

- Websites track web users as they navigate cyberspace
- Tracking information can include:
  - Your name
  - E-mail address
  - Internet address of your computer
  - Name of your computer
  - Date and time of your visit & last visit
  - Lots of info about your computer



# Safe Web Browsing

- **Wireless** or **Wi-Fi** is becoming more prevalent
- Don't assume that your wireless transmission are private
- Many "hot spots" do not use any form of encryption in their Wi-Fi



# Disposal of Data Storage Media

## Data Erasure

Software-based overwriting uses a software application to write patterns of meaningless data onto each of a hard drive's sectors

- This method of erasure goes beyond basic file deletion commands

**Degaussing and physical destruction** will also render the disk unreadable and unusable



# Encryption

- Encryption is a way of scrambling a message so that it can only be read by the person you are sending it to.
- Once a message is encrypted it will appear as a meaningless garble of characters to anyone except the owner of the key to unscramble it.

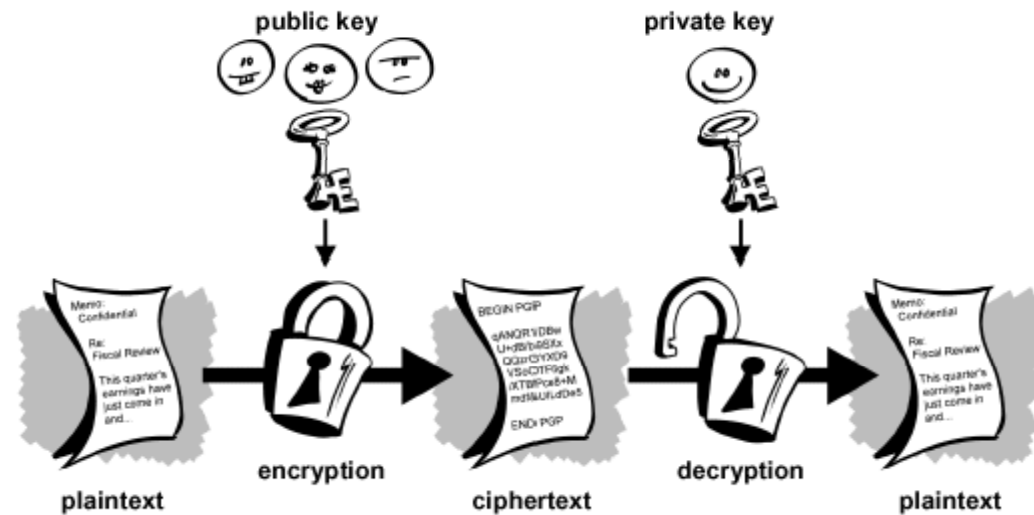


# Encryption

- The simplest way to encrypt a message is to write your message in a word processing program and save it with a password.
  - You can then attach the file to your e-mail.
- The recipient must also know the password in order to be able to read the file.
  - Obviously the password can't be sent in the e-mail

# Encryption

**Public Key Encryption** - provides a way to send an encrypted message, and ensures that the recipient has the key to decode them



# Encryption

- If you want to send a confidential message, encrypt it with your public key
- When you receive an encrypted message, you decrypt it into readable text with your private key
  - You make your public key is available to everyone so that they can encrypt messages to you, but only you can read those messages using your private key

# Social Engineering

**Social engineering** is the art of manipulating people into performing actions or divulging confidential information.

- Similar to a confidence trick or simple fraud, the term typically applies gathering personal info via the computer system
- Attackers rarely come face-to-face with the victim



# Social Engineering

## Some examples:

- **Pretexting** is the act of creating and using an invented scenario (the pretext) to persuade a targeted victim to release information
- **E-mail Phishing** Typically, the phisher sends an e-mail that appears to come from a legitimate business — a bank or credit card company — requesting "verification" of information and warning of some dire consequence
- **Baiting** is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim. The attacker leaves a malware infected floppy disc, CD ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate look and simply waits for the victim to use the device
- **Quid pro quo**, the attacker calls random numbers at a company claiming to be calling back from technical support. Eventually they will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and in the process have the user type commands that give the attacker access or launch malware

# Separation of Duties

- Separation of duty, as a security principle, has as its primary objective: prevention of fraud and errors
- Disseminating the tasks and associated privileges for a specific business process among multiple users
  - *Example:* The functions of warehouse/delivery, sales, and receipt of payments are each performed by different parties, with a policy that each party reports every transaction to a fourth function, accounting
- In information systems, segregation of duties helps reduce the potential damage from the actions of one person

# Software and Content Legalities

- Intellectual Property Rights
- Software Licensing
- Copyright Issues
  - Copyright is the exclusive right to control reproduction and commercial exploitation of your artwork.



# Safe Computing

© 1999 Randy Glasbergen. www.glasbergen.com



**"It's the latest innovation in office safety.  
When your computer crashes, an air bag is activated  
so you won't bang your head in frustration."**

- Keep Passwords Secure
- Change Passwords Regularly
- Use Strong Passwords
- Use Unique Passwords for Each System
- Log Out/Lock Computer When Appropriate
- Use a Password Protected Screen Saver

# Safe Computing Review

- Use and Update Antivirus Software.
- Use Safe E-mail Practices.
- Beware of Intruder Social Engineering.
- Back up Your Important Data.
- Keep System and Applications Updated with Latest Patches.



# Conclusion

- As Internet usage and technology continues to grow, so does the need to protect our systems and information from unauthorized access
- All computer users play a role in keeping our systems and data secure

# Thank You

