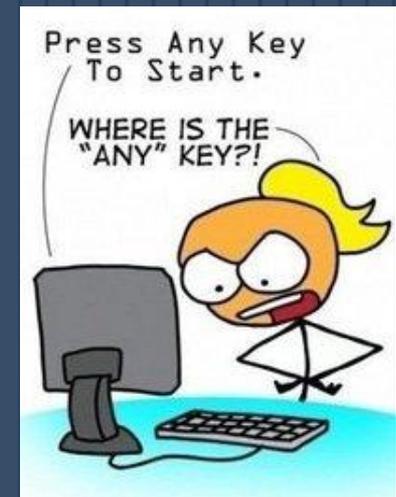




Mark R. Herring
Attorney General
Commonwealth of Virginia
Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-2071 (Telephone)
(804) 786-1991 (Facsimile)

Introduction to Cyber Security

Cyber Security Issues for Non-Technical Computer Users





Overview

- About the OAG's Computer Crime Section
- What is Cyber Security?
- Virus Basics & Protecting Yourself
- Wireless Network Security
- Cloud Computing Security
- Mobile Device Security
- Geotagging
- Practicing Good Security Habits
- Additional Resources
- Contact Information



About the OAG's Computer Crime Section

- Formed in July 1999
- Investigates and Prosecutes under Virginia Computer Crimes Act 18.2-(152.1-152.16)
- Prosecuted Illegal Spamming (first law of its kind in U.S.)
- Prosecutes Child Pornography/Exploitation Cases
- Investigates and Prosecutes Identity Theft
- Assists Local, State, and Federal Law Enforcement as well as Prosecutors
- Coordinates VA's Internet Crime Fighting.



What is Cyber Security?





What is Cyber Security?

▣ Almost Everything Relies on Computers and the Internet Now:

- Communication (e-mail, cell phones)
- Entertainment (digital cable, mp3's)
- Transportation (car engines, airplane navigation)
- Shopping (online stores, credit cards)
- Medicine (equipment, medical records)

▣ Cyber security involves protecting that information by Preventing, Detecting, and Responding to attacks on electronic data.



What Can You Do?

- Protect Yourself by Recognizing the Following:
 - Identifying the Risks
 - Understanding the Terminology





What Are the Risks?

□ Among These Dangers Are:

- Viruses erasing your entire system
- Someone breaking into your system and altering files
- Someone using your computer to attack others
- Someone stealing your credit card information and making unauthorized purchases.

□ There's not a 100% guarantee you'll be protected, but there are steps you can take to minimize the chances.





Terminology

▣ Hacker, Attacker, or Intruder

- Applied to the people who seek to exploit weaknesses in software and computer systems for their own gain.
- Attacks can be harmless, but usually are in violation of the intended use of the systems they are exploiting.
- The results can range from mere mischief to malicious activity (i.e. stealing or altering information).





Terminology

▣ Malicious Code

- Sometimes called malware, is a broad category that includes any code that could be used to attack your computer.

▣ Malicious code can have the following characteristics:

- It might require you to actually do something before it infects your computer.
- This action could be opening an email attachment or going to a particular web page.
- Some malicious code claims to be one thing while in fact doing something different behind the scenes.
- Once a machine is infected, the code can be passed on



Terminology

□ Vulnerabilities

- Often caused by programming errors in software.
- Attackers might be able to take advantage of these errors to infect your computer/cell phone/smart phone.
- It is important to apply updates or patches that address known vulnerabilities.

□ Patches

- Are updates that fix a particular problem or vulnerability within a program.
- A version upgrade to a program may also be called a patch.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Patches

- When patches are available, vendors usually put them on their websites for users to download.
- It is important to install a patch as soon as possible.
- Some software will automatically check for updates, while others may offer automatic notifications.
 - If these automatic options are available, we recommend that you take advantage of them.
 - If they are not available, check your vendors' websites periodically for updates.





Patches

- ▣ Make sure that you only download software or patches from websites that you trust.

- ▣ Do not trust a link in an email message
 - Attackers have used email messages to direct users to malicious websites where users install viruses disguised as patches.

- ▣ Beware of email messages that claim that they have attached the patch to the message
 - Again, these attachments are often viruses.



Viruses

Virus Basics & Protecting Yourself





Virus Basics

□ What is a Virus?

- Small software program that is designed to spread from one computer to another and to interfere with computer operation.
- Some viruses are harmless, while others may damage or even destroy files.

□ Viruses used to be spread when people shared floppy disks and other portable media, now viruses are primarily spread through email messages.

□ Unlike worms, viruses often require some sort of user action (e.g., opening an email attachment or visiting a malicious web page) to spread.



Virus Basics

▣ What is a Worm?

- A type of virus that can spread without human interaction.
- Worms often spread from computer to computer and take up valuable memory and network bandwidth, which can cause a computer to stop responding.
- Worms can also allow attackers to gain access to your computer remotely.





Virus Basics

□ What is a Trojan Horse?

- A computer program that is hiding a virus or other potentially damaging program.
- It can be a program that purports to do one action when, in fact, it is performing a malicious action on your computer.
- They can be included in software that you download for free or as attachments in email messages.



Virus Facts

□ Can I get a virus by reading my email messages?

- Yes & NO
- Most viruses, Trojan horses, and worms are activated when you open an attachment or click a link contained in an email message.
- If your email client allows scripting, then it is possible to get a virus by simply opening a message.
- It is best to limit what HTML is available in your email messages. The safest way to view email messages is in plain text.



Virus Facts

□ How Can I Avoid a Virus Infection From Email?

- Never open anything that is attached to an email message unless you know the contents of the file.
- If you receive an attachment from a familiar email address, but were not expecting anything, you should contact the sender before opening the attachment.
- If you receive a message with an attachment and you do not recognize the sender, you should delete the message.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Avoiding Viruses

- Install Anti-Virus Software From a Reputable Vendor. Update It and Use It Regularly.
 - AVG, Microsoft Security Essentials, McAfee, Bitdefender, Avast!

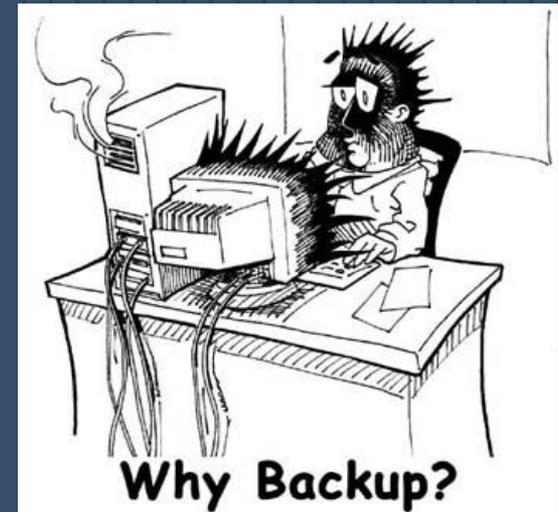
- Scan for Viruses on a Regular Interval.
 - Most programs are set to run at least once a week.

- Install an "On Access" Scanner.
 - Included with most anti-virus programs.
 - Allows the user to scan files at any given time.



Avoiding Viruses

- Be careful about accepting files or clicking links you receive from chat rooms/online communities.
- Back up your data on a regular interval onto a disc or external hard drive.
 - In the event of a virus, this allows the user to utilize non-infected files.





Recognizing Fake Anti-Viruses

□ What is a Fake Anti-Virus?

- Malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software.
- Makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program.
- It also causes realistic, interactive security warnings to be displayed to the computer user.



Recognizing Fake Anti-Viruses

□ How will I know if I am infected?

- Extreme Presence of Pop-ups.
- Most of these will display unusual security warnings and ask for credit card or personal information.



Wireless Network Security

Threats Have Gone Airborne





Wireless Network Security

□ How do Wireless Networks Work?

- Rely on radio waves rather than wires to connect computers to the internet.
- A transmitter, AKA a wireless router, is wired into an internet connection. This provides a "hotspot" that transmits the connectivity over radio waves.
- Computers that have a wireless capability and have permission to access the network can take advantage of the network connection.



Wireless Network Security

- What Security Threats are Associated with Wireless Networks?
 - Because wireless networks do not require a wired connection, it is possible for attackers who are within range to hijack or intercept an unprotected connection.

- Wardriving
 - Practice involving a person and a wireless device.
 - Drive around searching for unsecured wireless networks.
 - Often used with malicious intent.
 - Downloading Child Pornography, Stealing Personal Info.



Wireless Network Security

□ What Can You do to Minimize the Risks?

- Change Default Passwords

- Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup.

- Encrypt the Data on Your Network

- WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices.

- Encrypting the data would prevent anyone who might be able to access your network from viewing your data.



Wireless Network Security

- Install a Firewall
 - On both your computer and wireless network.
- Maintain Anti-Virus Software
 - Install on all devices and make sure your virus definitions are up to date.
 - Many of these programs also have additional features that may protect against or detect spyware and Trojan horses.



Cloud Computing

New Technology = New Risks



Cloud Computing

□ What is the Cloud?

- A subscription-based service where you can obtain networked storage space.
- Examples: Google Docs, Skydrive, Dropbox
- Just Think E-mail.
 - Not housed on your physical computer.
 - It can be accessed from anywhere.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Cloud Computing

□ How Can You Use the Cloud?

- Allows You to be Mobile.

- Your computer does not have to be used for data storage.
- Rather, it is just a means of accessing the Cloud.

- A cloud provider may just own/house the hardware/software necessary to run your home or business applications.



Cloud Computing Types

▣ Types of Clouds

- Public Cloud - Can be accessed by any subscriber with an internet connection and access to the cloud space.
- Private Cloud - Is established for a specific group or organization and limits access to just that group.
- Community Cloud - Is shared among two or more organizations that have similar cloud requirements.
- Hybrid Cloud - Is essentially a combination of at least two of the cloud types.



Cloud Computing Threats

- ▣ The information housed on the cloud is often seen as valuable to individuals with malicious intent. why?

- ▣ More and More People are Transferring Data to the Cloud.
 - This leads to an increase in personal information and potentially secure data being put on the internet.



Cloud Computing Threats

- ▣ Look into the security measures that your cloud provider already has in place.
 - What encryption methods do the providers have in place?
 - What methods of protection do they have in place for the actual hardware that your data will be stored on?
 - Will they have backups of my data?
 - Do they have firewalls set up?
 - If you have a community cloud, what barriers are in place to keep your information separate from other companies?





Cloud Computing Security

□ If You are Considering Using the Cloud:

- Identify what information you will be putting out in the cloud.
- Know who will have access to that information.
- Know which cloud will best fit your needs.
- Review the reputation and responsibilities of the providers you are considering before you sign up.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Cyber Threats and Mobile Devices

Not Just for Computers Anymore



Cyber Threats to Mobile Devices

- As mobile device technology evolves, consumers are using it at unprecedented levels.
- There are an estimated 4.6 billion mobile cellular subscriptions globally at the end of 2009.
- Mobile devices have become equally susceptible to malicious cyber activity as computers.



Cyber Threats to Mobile Devices

□ The following Threats are Known to Target Mobile Devices:

- Social Engineering
- Exploitation of Social Networking
- Exploitation of Mobile Applications
- Exploitation of M-Commerce



Social Engineering

- Very common method for spreading malware on the Internet.
- Most malicious activity is often successful because users are deceived into believing it is legitimate.
- Extremely lucrative and will likely significantly increase in the mobile market.



Social Engineering

□ Social Engineering Schemes:

- Phishing - Attempting to manipulate a victim into providing sensitive information by appearing as a valid entity.
- Vishing - Entice a victim to call a certain number and divulge sensitive information.
- Smishing - Involves text messages that contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number.



Exploitation of Social Networking

- Involves social networking sites such as Facebook & Twitter.
- Information sharing often occurs with an unwarranted, inherent trust among users.
- Often share and accept data from unauthenticated parties.



Exploitation of Mobile Applications

- Commonly called “Apps”.
- Provide enhanced convenience and functionality.
- Developers have created mobile applications for various uses and activities.
- Anyone can potentially develop and distribute mobile applications with little oversight.
 - Makes apps a potential attack vector for cyber criminals.



Exploitation of M-Commerce

- Consumers Can Use Mobile Devices From Any Location to:
 - Research Product Information
 - Compare Prices
 - Make Purchases
 - Communicate with Customer Support

- Using mobile devices for purchases, offers a potential for credit card/bank account information to be leaked or stolen.



Protecting Mobile Devices

□ Best Practices to Help Protect Mobile Devices:

- Maintain up-to-date software, including operating systems and applications.
- Install anti-virus software as it becomes available and maintain up-to-date signatures.
- Enable the personal identification number (PIN) or password to access the mobile device.
- Encrypt personal and sensitive data.
- Disable features not actively in use such as Bluetooth or Wi-Fi.



Protecting Mobile Devices

▣ Best Practices to Help Protect Mobile Devices:

- Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices.
- Use caution when opening email and text message attachments and clicking links.
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages.
- Avoid joining unknown Wi-Fi networks.
- Delete all information stored in a device prior to discarding it.





Geotagging and Social Networks

Geotagging: What Is It and How Can You Protect Yourself?



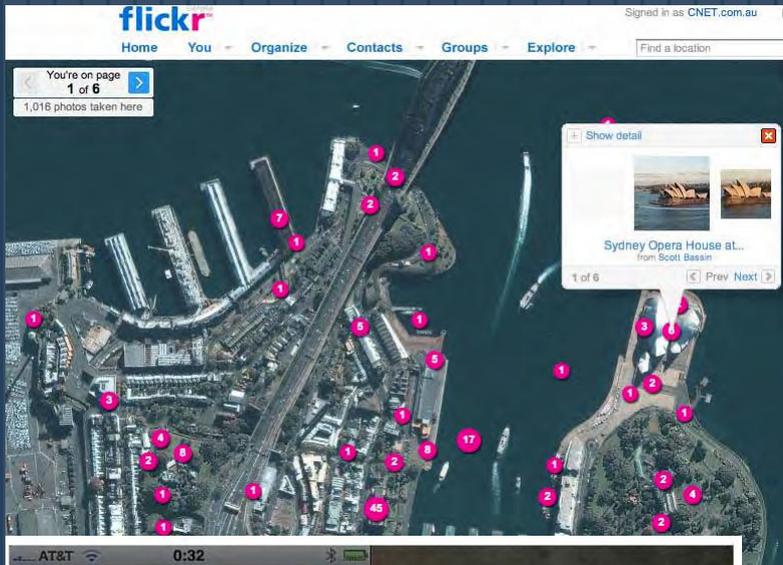
The Dangers of Geotagging

- It Starts With Taking a Photo Electronically...
 - What Personal Information Could Possibly be Exposed?
 - What is the Threat?

- Your photos can tell everyone:
 - Where You Live
 - Where You Spend Your Time
 - Where You Park Your Car
 - And Other Information You Would Not Want to Tell



What is Geotagging?



Definition:

- The process of adding your location to a file.
- It is the equivalent of adding a grid coordinate to everything you post on the internet.





The Dangers of Geotagging

- In August of 2010, Adam Savage, of “MythBusters,” took a photo of his vehicle using his smartphone.
- He then posted the photo to his Twitter account including the phrase “off to work.”
- His phone attached metadata revealing his exact location.





Location-based Social Networking

□ Location-based social networking allows a user to broadcast their geographic location.

□ Commonly used to “check in” at various locations to earn points, badges, discounts and other geo-related awards.

□ Adversely affects security and privacy of an individual.





Why are These Applications Potentially Dangerous?



□ Establishes Patterns

□ Exposes Places of Work, School and Home

□ Identifies Location of Potential Victims



Turning Off the GPS Function on Phones



- Avoid displaying location information by disabling the geotagging function on your Smartphone.
- Most Smartphones automatically display geographical location.
 - It takes a little more effort on the user's part to protect their privacy.



Geotagging Tips

- Be aware of the ability for your images to be geo-tagged.
- Understand the risks involved.
- Know when to use the geotagging feature and when not to use it.
- Know how to disable you cell phone's or camera's geotagging feature.
- If using geotagging websites, control with great care the people who are able to see where you are located.
- Be aware when you post your pictures and what geotagged information you leave.



Practicing Good Security Habits

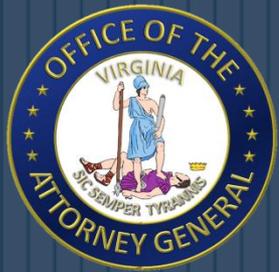
General Practices for Computers and Mobile Devices





Good Security Habits

- How Can You Minimize the Access Other People Have to Your Information?
 - Its easier to identify people who may have *physical* access to your computer/mobile device.
 - However, Identifying the people who could gain *remote* access to your computer becomes much more difficult.
 - As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing your information.



Good Security Habits

- Lock Your Computer When You are Away From It.
- Disconnect Your Computer From the Internet When You Aren't Using It.
- Evaluate Your Security Settings.
 - Including web browsers, e-mail clients, & social networking sites.
- Protect Your Computer Against Power Surges and Brief Outages.
- Backup All of Your Data on a Regular Interval.



Protecting Portable Devices

- Password-Protect Your Device
- Keep Your Valuables with You at All Times
- Downplay the Possession of a Laptop or Mobile Device
- Be Vigilant of Your Surroundings
- Consider an Alarm or Lock



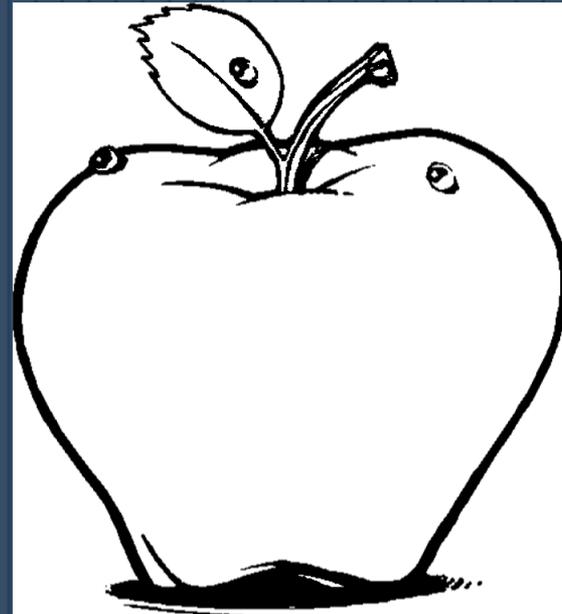
Protecting Portable Devices

- What Can You Do if Your Laptop or Mobile Device is Lost or Stolen?
 - Report the loss or theft to the appropriate authorities.
 - If your device contained sensitive information, immediately report the theft to your organization.
 - If possible, remote data wipe the device.
 - Devices with this ability include: Android's, iPhone's, & Mac's.



Practicing Good Security Habits

Apple-Based Products





8 Simple Tips for Mac Security

- Back Up Your Data with Time Machine
- Install New Software Updates ASAP
- Enable Keychain: Built-In Password Manager
- Know Your Download Source(s)
- Disable Java and Flash Plug-ins
- Install an Anti-virus
 - Intego, Sophos, and Avira
- Use a Stronger Firewall
 - OS X has a built-in firewall (disabled by default)
- Encrypt with FileVault 2
 - Encrypts your entire hard drive with AES 128 encryption

Article Date: August 21, 2012

pcmag.com

<http://www.pcmag.com/article2/0,2817,2408621,00.asp>



Cyber Security Tips for a Business Environment





Cyber Security Guidance

▣ For Employees:

- Make your passwords complex. Use a combination of numbers, symbols and letters (upper and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do not give any of your user names, passwords, or other computer/website access codes to anyone.
- Do not open e-mails or attachments from strangers.



Cyber Security Guidance

□ For Employees:

- Do not install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual problems with your computer or assigned cell phone to your IT department.



Cyber Security Guidance

□ For Management & IT Department:

- Establish clear policies and procedures for employees.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your anti-virus software daily.
- Regularly download vendor security “patches” for all of your software.
- Change the manufacturer’s default passwords on all of your software.
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks.



Additional Resources

- www.us-cert.gov
- www.dhs.gov
- www.cert.org
- www.onguardonline.gov
- www.stopthinkconnect.org
- www.ic3.gov
- www.ftc.gov
- www.ag.virginia.gov



Visit the CCS on Facebook

facebook

Search

Home Profile Find Friends Account



Wall

Info

Friend Activity

Photos

Links

About

The Computer Crime Section in the Virginia Attorney General's Office prosec...

More

239 like this

Create a Page

Add to My Page

Subscribe via RSS

Report Page

Share

Virginia Attorney General's Computer Crime Section



Government Organization · Richmond, Virginia

Wall



Virginia Attorney General's Computer Crime Section

Cybersecurity in the News: Sega is the latest in a long line of companies falling victim to data breaches. In the last few weeks, large data breaches have occurred at Sony, Citigroup, and RSA, among others, endangering the personal information of consumers. If you think your information may have been compromised, you should vigilantly monitor your credit report and be especially aware of phishing scams.



Sega Says More Than One Million Affected By Sega Pass Breach | threatpost

threatpost.com

Sega says that more than a million customers of Sega Pass gaming network were affected by a data breach.

June 21 at 4:24pm · Share · Translate

RECENT ACTIVITY



Virginia Attorney General's Computer Crime Section edited their **Founded and Location**.



Virginia Attorney General's Computer Crime Section

Cybertip of the Month: Turn on your computer's firewall, even if you have a Mac. Apple alerted users to a scam involving fake antivirus software. Fake websites will notify a user that a computer is infected with a virus, tricking him into installing fake antivirus software. The scam is designed to steal the user's credit card information. Turning on your firewall will help protect your personal information.

May 26 at 11:24am · Translate



Virginia Attorney General's Computer Crime Section

Cybersecurity in the News: If you have been affected by the Epsilon data breach, this article provides some good advice on how to protect yourself and your information. Be particularly aware of phishing scams, avoid clicking on any

Recommend This Place



Help your friends discover great places to visit by recommending this.

Write a recommendation...



Contact Information

- Address: Computer Crime Section
Office of the Attorney General
202 North Ninth Street,
Richmond, VA 23219

- Web: www.ag.virginia.gov
- Email: CyberCrimeUnit@oag.state.va.us

- Phone: 804.786.2071