

Information presented in this handout is from the following:

www.secureflorida.org and www.worldstart.com.

	<h2>Our Mission</h2> <p>To protect the citizens and economy of Florida by safeguarding our information systems, reducing our vulnerability to cyber attacks, and increasing our responsiveness to any threat</p>
	

Computers 101 _____

Q:

What are the 25 most common mistakes we all make in accordance to e-mail security?

A:

Okay, I must confess. No one wrote in and asked me that question, but I thought it was so important to cover, I had to get it in here somehow. Now, I know that 25 is a rather large number, but don't worry. I'm not going to go over all of them in one day. We'll do 12 of them today and the other 13 for tomorrow. So, make sure you stay tuned, because all 25 of them are very important to know! Alright, what do you say we get started?!

1.) **Only Using One E-mail Account** - We here at WorldStart have actually told you this before. It's very important that you familiarize yourself with more than one e-mail program. You can't think of your e-mail address like your home address. You need to have more than one! In all actuality, it's best to have even up to three open e-mail accounts. That way, you can have one for your home e-mails, one for your office e-mails and an extra one for all the other things you do online. For example, always use your third account to sign up for newsletters, contests, etc. It's also best to have maybe one paid e-mail account and the other two can be one of the free ones that are available today, such as Yahoo!, Hotmail or Gmail. With more than one account, you are saving yourself in the long run.

2.) **Keeping the Spam Around** - Have you ever had an e-mail account that just got spammed out? You know, pretty much all you ever received from that account was spam. So, after awhile, you probably got tired of it, but instead of switching to another e-mail client, you just started to accept it. Well, I'm here to tell you not to do that anymore! When one of your accounts gets spammed out, just get rid of it and start fresh. I know it's easy to get attached to an e-mail program, because you're familiar with it, etc., but it's not healthy to keep all that spam around. It's only going to get worse, so my advice is to get rid of it while you're still somewhat ahead.

3.) **Forgot to Close the Browser** - Do you ever check your e-mail from another location apart from your home computer? You know, like the library or even maybe a cyber café. Well, when you do that, you have to make sure you log out of your e-mail account when you're finished. Along with that, be sure that you always close down the browser window as well. If you don't do this, your username may remain on the screen and it will really put you on target for some security risks.

4.) **Forgot to Clear It** - Here's another important tip if you're using another computer outside of your home. Always make sure you clear the browser cache, the history and your passwords. Most Web browsers will hold onto that information and even though it's trying to save you time, it's a hazard if you're using a public computer. You never know who could get on that computer after you. Here are some quick instructions on how to do all of that, so you won't ever have to worry about it.

In Internet Explorer, go to **Tools, Internet Options** and click on all three buttons that say, "**Clear History**," "**Delete Cookies**" and "**Delete Files**." In Firefox, you can simply use the keyboard combination of **Ctrl + Shift + Del** in the open browser window. Doing that will keep you much safer!

5.) **Using Insecure Accounts** - This one has a little more to do with larger corporations, but you never know when it could affect you. Often times, corporation employees are careless and they use their personal e-mail accounts for business purposes. If this happens, they are at risk of sending out sensitive information that could really hurt the company. Doing this could put their job at risk as well. Always use your personal account for personal items and leave everything else out.

6.) **Forgot to Use the Telephone** - We all know how convenient e-mail is, but in some cases, it's not always the best option. If you're going to be e-mailing something very sensitive or private, you might want to consider just picking up the telephone and doing it that way. In these types of cases, using the telephone is a much safer option to use than e-mail. It may take a few more minutes to do, but if it's possible, just call.

7.) **Forgot to Use the BCC** - We've told you about the BCC (Blind Carbon Copy) feature before in the newsletter, but I'm willing to guess that some of you still don't use it. This works the best when you're e-mailing multiple people. If you insert the e-mail addresses onto the BCC line, the recipients won't be able to see any of the other e-mail addresses you're sending the e-mail to. Now, don't get this confused with the CC option either. BCC is really the way to go to keep everyone's addresses safe and secure.

8.) **Used the Reply All Button** - Do you ever get confused as to whether you should hit the Reply or Reply All buttons when you're replying to an e-mail message? If you click on Reply All, your reply will go to each and every e-mail address that the original message was sent to. Yes, it will go to the person you intended as well, but if you're sending them a personal message, you don't want everyone else to be able to see it. Always use Reply first. It's a safer shot.

9.) **Forwarding Spam** - Did you know that forwarding e-mails can bring on a new batch of spam mail? Well, if you didn't know before, you know now. If you aren't careful, forwarding e-mails can pose a big security threat for you and the earlier recipients of the e-mail. When you forward an e-mail, make sure you delete all of the previous addresses first. This way, the person you forward the message to won't be able to see the addresses of who all already got it. If you keep all the e-mail addresses on there, spammers can quickly grab up that entire list and just go to town. Everyone will get spammed, including you. And I know you don't want that to happen!

10.) **Forgot to Back It Up** - Again, we here at WorldStart are always telling you to back up the data on your computer. Well, e-mails are no exception. If you've got important e-mails on your computer that you're going to want to hang on to for awhile, don't forget to back them up frequently. These types of e-mails could be anything from legal contracts to financial information or even personal information you want to keep. Either way, run a backup on them and you won't ever have to worry about losing them for good. Read [here](#) for some tips on getting the backup process done easily.

11.) **Mobile Access** - Do you ever access your e-mail through a mobile device, such as your cell phone or a Blackberry? With today's technology, you can check your e-mail from just about anywhere, but is it really safe? They are safe, but you have to remember a couple of things if you're using this method. Sometimes, the software on your mobile device will not keep the e-mails you check on the server for very long. Therefore, certain e-mails will not be on your home or office computer later on when you need them. So, if you delete them from the device, they will be deleted from your Inbox as well. Check the default settings on your mobile device to make sure they are set to keep the e-mails around for as long as you need them. This is very important, especially for urgent e-mails.

12.) **It's Gone For Good** - Yes, we've all done it. We've sent embarrassing e-mails to our friends or we received very inappropriate e-mails from other senders. When those come in, what do you do? Probably delete them right away, right? Well, when you delete them, are they gone for good? The answer is no. Just because you delete an e-mail from your Inbox or even your Deleted folder, the e-mails are not gone forever. They usually remain on your server until something else takes its place. Even then, they sometimes stay in backup folders and other remote servers for years. If this happens, spammers can get ahold of them and you know what happens after that. So, when you're sending e-mails, think about what you're writing in them. It may come back to haunt you later on.

Okay, that's the last one for today. Like I said before, we'll do the rest tomorrow, so don't forget to check out that issue. If you think these 12 tips were good, wait until you see what I have for you next. You're all going to be the safest e-mail users ever by the time we get done. And if that happens, my work here is complete. See you all tomorrow!

**For information on all of these topics visit
www.secureflorida.org.**

Search engines:

www.google.com

www.yahoo.com

www.dogpile.com

www.lycos.com

www.metacrawler.com

Free Stuff:

www.downloadshareware.com

www.downloads.com

www.tucows.com

www.shareware.com

www.versiontracker.com

freshmeat net

Cybercrime:

www.secureflorida.org

www.fdle.state.fl.us/fc3

www.cybercrime.gov

Anti-virus:

www.my-etrust.com/microsoft (Computer Associates Anti-Virus)

free.grisoft.com/freeweb.php (AVG Anti-Virus)

www.free-program-download.com/avast (Avast Anti-Virus)

www.symantec.com (Norton/Symantec Anti-Virus)

www.messagelabs.com

www.sophos.com

www.mcafee.com

www.trendmicro.com

Rootkit detection:

<http://www.pctools.com/spyware-doctor/> (Spyware Doctor)

<http://www.sysinternals.com/Utilities/RootkitRevealer.html>

(Rootkit Revealer)

Spyware:

www.javacooisoftware.com/eulalyzer.html (Eulalyzer)

www.safer-networking.org

www.lavasoft.de (Ad-aware)

<http://www.webroot.com/consumer/products/spysweeper> (Spy Sweeper)

<http://www.microsoft.com/athome/security/spyware>

<http://www.intermute.com/products/cwshredder.html>

(CWShredder)

<http://www.xintercept.com/pkpeek>

.htm (Pocketknife Peek)

<http://www.amfsoftware.com/windows/nospy.html>

(AMF NoSpy)

<http://www.pctools.com/spyware-doctor/> (Spyware Doctor)

Spam:

www.spamcop.net

www.cauce.org

<http://spamcon.org>

www.spamhaus.org

<http://www.ftc.gov/bcp/online/pubs/online/inbox.htm>

Frauds and Scams:

<http://www.fdle.state.fl.us/Fc3/nigerian.html> (Nigerian Scam)

www.anti-phishing.org

www.fraud.org

www.ic3.gov

Urban Legends, hoaxes and Myths:

www.snopes.com hOaxbusters.ciac.org

www.f-secure.com/news/hoax.htm

www.vmyths.com urbanlegends.about.com

Passwords:

<http://www.microsoft.com/athome/security/privacy/password.msp>

Cyberstalking:

www.MissingKids.com

kids.getnetwise.org

www.CyberAngels.org

www.HaltAbuse.org

<http://www.haltabusektd.org> (for kids) www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Identity Theft:

www.myfloridalegal.com/identitytheft

www.consumer.gov/idtheft

www.usdoj.gov/criminal/cybercrime/cyberstalking.htm www.ftc.gov/bcp/online/pubs/credit/idtheft.htm

<https://www.annuaicreditreport.com>

Firewalls:

www.zonelabs.com

www.tinysoftware.com

<http://centralops.net>

<http://www.symantecstore.com>

<http://us.mcafee.com>

<http://www.blackice.com/PCProtection-Firewall.htm>

Patches:

www.windowsupdate.com

office.microsoft.com/officeupdate

www.apple.com/support/downloads

Florida Related:

www.myflorida.org

www.fdle.state.fl.us/fc3

www.fdle.state.fl.us/flsenate.gov

Increasing Awareness:

www.cert.org

www.us-cert.gov

www.dhs.gov/dhspublic/display?theme=70

www.cerias.purdue.edu

www.gocsl.com

www.sans.org/newsletters

isc.sans.org

Places to go for More Information

www.bewebaware.org

www.cert.org/homeusers

www.cert.org/tech_tips/home_networks

www.getnetwise.org

www.firewallguide.org

www.microsoft.com/athome/security

www.pcworld.com

www.pcmagazine.com

www.sans.org/rr/whitepapers/hsoffice

www.staysafeonline.info

www.us-cert.gov

www.secureflorida.org

www.spywarewarrior.com

www.antiphishing.org

www.ftc.gov

www.pcmagazine

www.pcworld

www.microsoft.com

www.symantec.com/athome/security

www.hhi.corecom.com/phishing.htm

www.phishinginfo.org

www.corestreet.com/spoofstickfirewallguide

Places to go for More Information (continued)

www.firewallgude.com/anti-virus

www.anti-virus-software-review.com.

www.hackfix.org

www.tom-cat.com/security

www.practicallynetworked.com

This information is from www.techdata.com Presentation Computer Security @ Home

by Jim Coffman

FIREWALL

Windows Firewall

ZoneAlarm

Kerio

Comodo

Installed with WindowsXP SP2

<http://www.zonelabs.com>

<http://www.sunbelt-software.com/kerio.com>

<http://www.personalfirewall.comodo.com>

ANTI-VIRUS

Grisoft AVG

Avast

ClamWin

<http://www.zonelabs.com>

<http://www.avast.com/eng/download-avast-home.html>

<http://www.clamwin.com>

PHISHING TOOLBARS

Netcraft

Earthlink

PhishGuard

Spoofstick

CallingID

<http://toolbar.netcraft.com>

<http://www.earthlink.net/software/free/toolbar/>

<http://www.phishguard.com/default.htm>

<http://www.spoofstick.com>

<http://callingid.com/Default.aspx>

SPAM

K9

SpamBayes

Despammed

SpamAssassin

<http://www.keir.net/k9.html>

www.spambayes.sourceforge.net

www.despammed.com

<http://spamassassin.apache.org>

SPYWARE

MS Windows Defender

Lavasoft Ad-ware

Javacool Spyware Blaster /Guard

Spybot Search & Destroy

Grisoft ewido

Sophos RootKit Eliminator

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

<http://www.lavasoft.de/software/adaware/>

<http://havacoolsoftware.com>

<http://spybotsafer-networking.de/en/>

<http://free.grisoft.com/doc/ewido-anti-spyware-free/Ing/us/tpl/v5>

<http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html>

WEB BROWSING TOOLS

McAfee Site Advisor

ShieldsUp Online Test

HackerWhacker

<http://www.siteadvisor.com/>

www.grc.com

<http://hackerwatch.org/probe/>

OTHER INFORMATION

From Microsoft

www.onecare.live.com



Windows Live OneCare: All-in-one security and performance for your PC

- Antivirus
- Antispyware
- Anti-phishing
- Firewall
- Performance tune-ups
- Backup and restore





Dictionary definitions provided from Smart Computing

ANTIVIRUS PROGRAM-Software that monitors a computer for viruses by looking for irregularities in a computer system and then comparing its findings to a database of virus information. Viruses not included in the antivirus program's database will go undetected, so it is important to periodically update antivirus programs with information about new viruses. Such updates usually can be purchased on a subscription basis from the company that produced the antivirus program. The regular use of an antivirus program often can eliminate a virus before any damage is caused. Antivirus applications should be used when foreign software is introduced into a computer.

BACKUP-A copy of a file or files created in case the original is destroyed or damaged. It is always a good idea to make backups of important files.

COOKIE-A cookie is a small information file placed on your hard drive and later read by a Web site. It is basically an identification marker. It lets a Web site recognize you when you log in and keeps track of you while you're at the Web site.

ELECTRONIC MAIL (email)-Text messages sent through a network to a specified individual or group. Received messages are stored in an Inbox and can be kept, deleted, replied to, or forwarded to another recipient, depending upon the e-mail program. Besides a message, an email may have an attached file or graphic. Users can make sure a message was received by requesting a receipt. Although not all items can be sent electronically, email's big advantage over postal mail, nicknamed "snail mail," is speed. Email can be delivered within seconds or minutes across thousands of miles. May also be spelled e-mail or E-mail.

FIREWALL-Software or hardware that limits or restricts certain kinds of computer access from a network or other outside source. A router is a good example of a hardware device that often has a built-in firewall. Firewalls are used to thwart would-be hackers from infiltrating computer systems.

MALWARE-Software intentionally designed for a malicious purpose, such as to erase a computer's memory or gain unauthorized access to a system. Trojan horses and purposefully system-damaging viruses are some examples of malware.

PASSWORD-A set of secret characters or words needed to gain access to a computer or to files and programs within the system. Passwords ensure that only authorized users can reach certain information.

PHISHING- is the act of trying to trick users into giving up personal information by making them think they're dealing with a legitimate business. A phisher sends unsolicited bulk emails to a large number of users. The email claims to be from a legitimate company, such as AOL or eBay, and claims the user's account will be suspended unless they click on the provided URL and supply the requested information (often passwords, credit card numbers, and other personal information). The URL is on a server controlled by the phisher, but its appearance is similar to that of the real site

REGISTRY KEY-Microsoft uses keys to store configuration keys in Windows. The value of the keys is changed each time a new program is installed or settings are modified. Applications must open a key before they can add data to the registry. In order to open a key, an application must supply a handle to another key in the registry that is already open. The system is able to define standard handles that are always open. An application can then use these predefined handles as entry points into the registry. Predefined keys help an application navigate in the registry and make it possible to develop tools that make it possible for a system administrator to manipulate categories of data. Applications that add data to the registry should always work within predefined keys, so administrative tools can find and use the data.

SPAM-As a noun, unsolicited bulk email on the Internet or Usenet newsgroup postings sent to large numbers of newsgroups. As a verb, to send copies of the same types of messages. Advertisers often spam recipients intending to market products, Web sites, or commentary. The beneficiary often considers spam as junk mail, and it is considered poor form to send it. A person or email address that receives many unwanted messages is said to have been "spammed."

SPYWARE-A category of software that tracks user behavior without a user's knowledge. Spyware can find its way onto a user's computer in a variety of ways. It may, for instance, manifest itself as part of a virus or Trojan horse. Recently, however, spyware is increasingly finding its way onto user's computer systems through legitimate software and applications. Companies may, for instance, install spyware on a user's computer to track browsing habits and relay the information to advertisers. Companies such as DoubleClick and RealNetworks have come under fire in spyware-related incidents.

VIRUS-A program designed to destroy data or halt operation on systems by copying itself into files and executing when those files are loaded. Viruses, which are carried among computers in files contained on diskettes or in online transmissions, usually cause problems on a system. When infected files are shared among computers on a company network, for example, the virus can cause extreme damage to a company's data. With antivirus software, users can avoid infection by a virus by disinfecting every diskette and file that is introduced to the computer. Several popular packages check files for viruses and eliminate any found

Wi-Fi-A standard set by the Wireless Ethernet Compatibility Alliance (WECA) to ensure compatibility of 802.11b wireless equipment

WORM-A destructive program containing code that replicates itself until it fills the target drive or network, thereby causing it to malfunction. Worms are sent out either as a practical joke or for purely malicious reasons; for the recipient whose computer or network has crashed, however, worms are not fun. See [virus](#).