Be Safe.

Take Note to These Social Networking Tips.

You've probably heard about identity theft — people stealing other people's personal information to use for illegal purposes. In a new tactic called "phishing," ID thieves trick people into providing their social security numbers, financial account numbers, PIN numbers, mothers' maiden names, and other personal information by pretending to be someone they're not. Avoid getting hooked by a phisher by knowing what to look for and taking basic security precautions.

WATCH OUT FOR "PHISHY" EMAILS. The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to "confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Another tactic phishers use is to say they're from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft! In one case, a phisher claimed to be from a state lottery commission and requested people's banking information to deposit their "winnings" in their accounts.

DON'T CLICK ON LINKS WITHIN EMAILS THAT ASK FOR YOUR PERSONAL INFORMATION. Fraudsters use these links to lure people to phony Web sites that looks just like the real sites of the company, organization, or agency they're impersonating. If you follow the instructions and enter your personal information on the Web site, you'll deliver it directly into the hands of identity thieves. To check whether the message is really from the company or agency, call it directly or go to its Web site (use a search engine to find it).

BEWARE OF "PHARMING." In this latest version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you're taken to a fake copy of the site without realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.

NEVER ENTER YOUR PERSONAL INFORMATION IN A POP-UP SCREEN. Sometimes a phisher will direct you to a real company's, organization's, or agency's Web site, but then an unauthorized pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens. Install pop-up blocking software to help prevent this type of phishing attack.

PROTECT YOUR COMPUTER WITH SPAM FILTERS, ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE, AND A FIREWALL, AND KEEP THEM UP TO DATE. A spam filter can help reduce the number of phishing emails you get. Anti-virus software, which scans incoming messages for troublesome files, and anti-spyware software, which looks for programs that have been installed on your computer and track your online activities without your knowledge, can protect you against pharming and other techniques that phishers use. Firewalls prevent hackers and unauthorized communications from entering your computer , which is especially important if you have a broadband connection because your computer is open to the Internet whenever it's turned on. Look for programs that offer automatic updates and take advantage of free patches that manufacturers offer to fix newly discovered problems. Go to www.onguardonline.gov and www.staysafeonline.org to learn more about how to keep your computer secure.

ONLY OPEN EMAIL ATTACHMENTS IF YOU'RE EXPECTING THEM AND KNOW WHAT THEY CONTAIN. Even if the messages look like they came from people you know, they could be from scammers and contain programs that will steal your personal information.

KNOW THAT PHISHING CAN ALSO HAPPEN BY PHONE. You may get a call from someone pretending to be from a company or government agency, making the same kinds of false claims and asking for your personal information.

IF SOMEONE CONTACTS YOU AND SAYS YOU'VE BEEN A VICTIM OF FRAUD, VERIFY THE PERSON'S IDENTITY BEFORE YOU PROVIDE ANY PERSONAL INFORMATION. Legitimate credit card issuers and other companies may contact you if there is an unusual pattern indicating that someone else might be using one of your accounts. But usually they only ask if you made particular transactions; they don't request your account number or other personal information. Law enforcement agencies might also contact you if you've been the victim of fraud. To be on the safe side, ask for the person's name, the name of the agency or company, the telephone number, and the address. Get the main number from the phone book, the Internet, or directory assistance, then call to find out if the person is legitimate.

JOB SEEKERS SHOULD ALSO BE CAREFUL. SOME PHISHERS TARGET PEOPLE WHO LIST THEMSELVES ON JOB SEARCH SITES. Pretending to be potential employers, they ask for your social security number and other personal information. Follow the advice above and verify the person's identity before providing any personal information.

BE SUSPICIOUS IF SOMEONE CONTACTS YOU UNEXPECTEDLY AND ASKS FOR YOUR PERSONAL INFORMATION. It's hard to tell whether something is legitimate by looking at an email or a Web site, or talking to someone on the phone. But if you're contacted out of the blue and asked for your personal information, it's a warning sign that something is "phishy." Legitimate companies and agencies don't operate that way.

ACT IMMEDIATELY IF YOU'VE BEEN HOOKED BY A PHISHER. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts right away. For information about how to put a "fraud alert" on your files at the credit reporting bureaus and other advice for ID theft victims, contact the Federal Trade Commission's ID Theft Clearinghouse, www.consumer.gov/idtheft or 877-438-4338, TDD 202-326-2502.

REPORT PHISHING, WHETHER YOU'RE A VICTIM OR NOT. Tell the company or agency that the phisher was impersonating. You can also report the problem to law enforcement agencies through the National Fraud Information Center/Internet Fraud Watch, www.fraud.org or 800-876-7060, TDD 202-835-0778. The information you provide helps to stop identity theft.

WEB ALERT:

SEVEN PRACTICES TO STAY SAFE ONLINE

The widespread availability of computers and connections to the Internet provides everyone with 24/7 access to information, credit and financial services, and shopping. The Internet is also an incredible tool for educators and students to communicate and learn.

Unfortunately, some individuals exploit the Internet through criminal behavior and other harmful acts. Criminals can try to gain unauthorized access to your computer and then use that access to steal your identity, commit fraud, or even launch cyber attacks against others. By following the recommended cyber security practices outlined here, you can limit the harm cyber criminals can do not only to your computer, but to everyone's computer.

However, there is no single cyber security practice or technological solution that will prevent online crime. These recommended cyber security practices highlight that using a set of practices that include Internet habits as well as technology solutions can make a difference.

The National Cyber Security Alliance's top cyber security practices are practical steps you can take to stay safe online and avoid becoming a victim of fraud, identity theft, or cyber crime.

1) Protect your personal information. It's valuable. To an identity thief, it can provide instant access to your financial accounts, your credit record, and your other personal assets. Keep in mind that if you are asked for your personal information, such as your name, email or home address, phone number, account numbers, or social security, learn how it's going to be used, and how it will be protected, before you use it. In addition, do not open unsolicited or unknown email messages, be careful about providing your personal or financial information when shopping online, and read website privacy policies, which should explain what personal information the website collects, how the information is used, and whether it is provided to third parties.

2) Know who you are dealing online. A legitimate business or individual seller should give you a physical address and a working telephone number at which they can be contacted in case you have problems. If you are shopping online, check the seller before you buy.

3) Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure. Look for anti-virus software that recognizes current viruses, as well as older ones, effectively reverses the damage, and updates automatically.

4) Be sure to set up your operating system and Web browser software properly, and update them regularly. Hackers may take advantage of unsecured Web browsers (such as Internet Explorer or Netscape) and operating system software (such as Windows or Linux). You can lessen your risk by changing the settings in your browser or operating system and increasing your online security. Check the "Tools" or "Options" menus for built-in security features.

5) Use strong passwords or strong authentication technology to help protect your personal information. Remember to keep passwords in a secure place, and out of plain view. You can make it more difficult for hackers by following these guidelines: using passwords that have at least eight characters and include numerals and symbols, avoiding common words (some hackers use programs that can try every word in the dictionary), not using your personal information, your login name, or adjacent keys on the keyboard as passwords, changing your passwords regularly (at minimum every 90 days), and using a different password for each online account you access or at least a variety of passwords with difficulty based on the value of the information contained in each.

6) Back up important files. If you have important files stored on your computer, copy them onto a removable disc, and store them in a secure place in a different building than your computer. If a different location is not practical, consider encryption software. Encryption software scrambles a message or a file in a way that can be reversed only with a specific password. Also, make sure you keep your original software start-up disks handy and accessible for use in the event of a system crash.

7) Learn what to do if something goes wrong. f your computer gets hacked or infected by a virus follow these guidelines:

- Immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software, and update your firewall.
- Take steps to minimize the chances of another incident.
- Alert the appropriate authorities by contacting: your ISP and the hacker's ISP (if possible), and the FBI at www.ifccfbi.gov.

Visit staysafeonline.org for more ways to remain safe online.

You may contact EIT at:
(850) 412-HELP (4357)
or **helpdesk@famu.edu**,
Monday–Friday 8:00 am – 5:00 pm