Cyber Security Tips

Cyber threats at work and at home are real – and they are becoming more common in today's world where we count on technology to stay connected.   Below are tips to help you protect yourself from online threats at the office and at home:

Malware, Spyware and Computer Viruses

Malware is malicious software designed to gain access to or damage a computer system without the owner's consent. It includes computer viruses, worms, Trojan horses, spyware, dishonest adware, and other malicious and unwanted software.

- Malware damages your system, causes instability, or exhibits behavior such as changing settings or interfering with a computer's registry and security settings. The majority of malware programs have been written in order to steal personal information, such as credit card or social security numbers.

Spyware are programs used to gather information about computer users by showing them pop-up ads or altering web-browser behavior for the financial benefit of the spyware creator. For instance, some spyware programs redirect search engine results to paid advertisements.

- Spyware can use up precious system resources like memory and hard disk space, causing your computer to run really slow. It can also compromise your privacy, providing outsiders with information about your computer habits.

A **computer virus** attaches itself to a program or file so it can spread from one computer to another, damaging hardware, software or files. Viruses are sometimes confused with computer worms and Trojan horses.

- A *worm* can spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book.

- A *Trojan horse* will appear to be useful software, but will actually do damage once installed or run on your computer. Some Trojans are designed to be more annoying than malicious (changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised.

The infected computers can be used to send out spam messages. If you don't get rid of the virus, there is a strong likelihood that eventually you'll pass it on to a friend or coworker. As it spreads, the virus will use up computer resources and could bring the system to a halt. This means more computers have to be disinfected, which mean more time is lost out of the workday, not to mention the possible loss of data.

A **botnet** is a collection of software robots (or bots) which run automatically. A botnet's originator can control the group remotely to give instructions to all the infected systems simultaneously. If your machine is infected with a botnets, attackers can use your computer to steal serial numbers, login IDs, and financial information. They can also use your computer to attack websites in order to bring them down, known as a “denial of service” attack.

Key loggers record the user's keystrokes when entering a password, credit card number, or other information. This information is then transmitted to the malware creator automatically, enabling credit card fraud and other theft.

Tips to Avoid Malware and Spyware

- **Update your operating system and web browser software.** Your operating system (like Windows or Linux) may offer free software “patches” to close holes in the system that spyware could exploit. You can configure your PC to download these updates automatically. At work, our internet security is automatically updated.

- **Install a personal firewall to stop uninvited users from accessing your computer.** A firewall blocks unauthorized access to your computer and will alert you if spyware is on your system and is sending information out. At work, our firewalls are designed to block unauthorized access to our systems and databases.

- **Be cautious when downloading software.** Don’t install any software without knowing exactly what it is. Take the time to read the end-user license agreement before downloading any software. If the agreement is hard to find – or difficult to understand – think twice about installing the software.

  It can be appealing to download free software like games, peer-to-peer file-sharing programs (this type of software allows computers to connect to each other to download files from individual computers – i.e. music or movies), customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware that some of these free software applications bundle other software – including spyware.

  At work, you should not download any software onto your computer without assistance from IT.

- **Check your browser security setting.** Make sure your browser security setting is high enough to detect unauthorized downloads. Use at least the “Medium” setting for Internet Explorer. Keep your browser software updated.

- **Run anti-virus software.** Many of these contain anti-spyware scanners or blockers. Be sure to update the software regularly.

- **Be careful of links.** Don’t click on any links inside pop-up windows. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the “X” icon in the title bar. Also, do not click on links in emails that claim to offer anti-spyware software. Some software offered in spam actually installs spyware.

- **Create complex passwords.** Use numbers, capital letters and special characters. Don’t use the same password on more than one financial site. Do not save your password on internet sites – retype them each time for enhanced security.

Clues That Spyware is on your Computer

- You get bombarded with pop-up ads.
- Your browser takes you to websites other than those you type into the address box.
- A sudden or repeated change in your computer’s Internet home page.

- New and unexpected toolbars or icons at the bottom of your computer screen.
- Keys that don't work (the "Tab" key might not work when you try to move to the next field in a Web form)
- Random error messages
- Sluggish or extremely slow performance when opening programs or saving files

If You Think Your Computer Contains Spyware

1. Install an anti-spyware program from a vendor you know and trust. Many anti-virus software programs include anti-spyware software.
2. Configure the anti-spyware to scan at least once a week – and every time you start your computer.
3. Delete any software programs the anti-spyware program detects that you don't want on your computer.

For use at home, the following sites offer free spyware software:

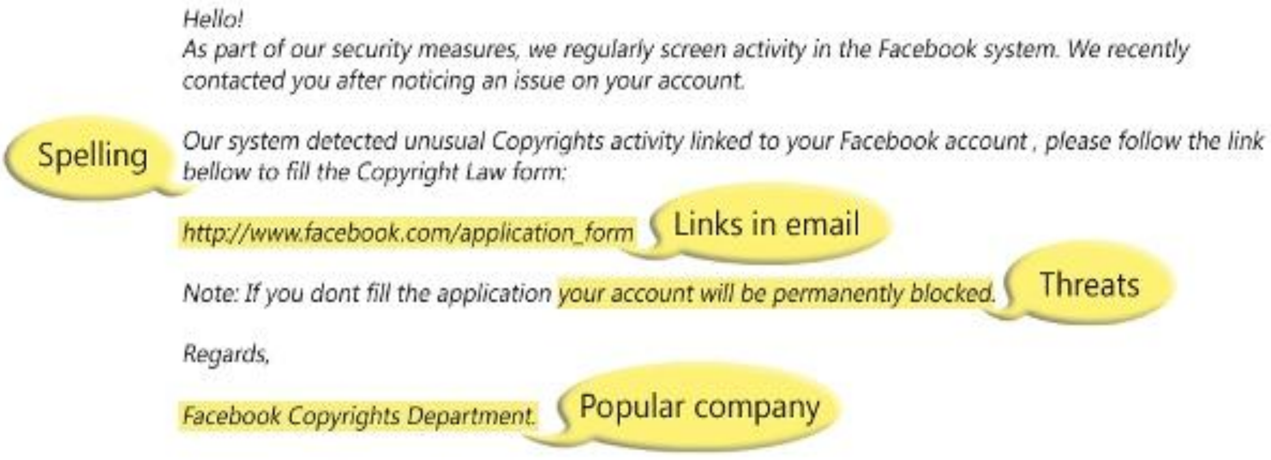
Ad-Aware www.lavasoftusa.com/software/adaware/
Spybot Search and Destroy www.safer-networking.org/
Microsoft Safety Scanner www.microsoft.com/security/scanner/en-us/default.aspx
Microsoft Malicious Software Removal Tool www.microsoft.com/security/pc-security/malware-removal.aspx

At work, contact your agency's help desk immediately if you think your computer contains spyware or malware.

Phishing

Phishing (pronounced fishing) is when an identity thief attempts to get your username, password, credit card details, social security number or other personal information by email – and they do this by masquerading as a company you do business with. They may act like your bank, internet service provider, online payment service, or even a government agency.

Phishing emails ask you to update, validate or confirm your account information by sending you're an email or pop-up message. Some messages may claim there is a problem with your account and may even threaten a consequence if you do not respond. These messages are not real – they have sent you a link to a fake website with the sole purpose in tricking you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.

Source: Microsoft Safety & Security Center

Don't reply to an email or pop-up message that asks for personal or financial information. Don't click on the link in the message. Legitimate companies do not ask for this information via email. Do not cut and paste the link from the message into your Internet browser—phishers can make links look like they go to one place, but they actually send you to a different site. Instead, call the company using a telephone number you trust or search the internet for your company using a tool you trust (Google, Bing, etc.).

- **Use anti-virus software and a firewall -- and keep them up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can help protect you from inadvertently accepting such unwanted files.
  - Look for anti-virus software that recognizes current and older threats, can effectively reverse the damage, and updates automatically.
  - A personal firewall blocks unauthorized access to your computer and can alert you if spyware is on your computer and is sending information out.
  - Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information, contact the requestor using a telephone number you know to be genuine.

- **Forward spam that is phishing for information** to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.
  - You can also report spam to the Federal Trade Commission at spam@uce.gov or the Anti-Phishing Working Group at reportphishing@antiphishing.org. They use these reports to fight phishing. (And yes, you can look up these organizations instead of clicking on our links if you're already practicing our tips!)

- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

You can learn other ways to avoid email scams and deal with deceptive spam at the Federal Trade Commission (ftc.gov/spam).

Identity Theft

According to a Federal Trade Commission survey, there are almost 10 million victims of identity theft every year. It's important to protect your personal information which can otherwise provide instant access to your financial accounts, credit record, and other personal assets.

- **Don't open unsolicited or unknown email messages.** If you get an email or pop-up message asking for personal information, don't reply to the email or click on any links in the message. Do not respond to requests for your personal or financial information by email. Instead, call the company to verify any questions.
  - Tip: to avoid automatically opening the next new email, turn off the "Preview Pane" and set your messages to plain text to avoid active links or pop-ups in the messages.

- **Adopt a "need to know" approach to your personal data.** If you're asked for your name, email, home address, telephone number, account numbers, or Social Security number – learn how it's going to be used and protected before you share it.
  - Example: the more information you print on your checks (such as home telephone number), the more personal data you are routinely handing out to people who may not need that information.

- **Be careful when shopping online.** Be cautious about providing your personal or financial information through a company's website without taking measures to reduce the risk. Some indictors to show that vendors have taken measures to secure their sites include (1) a lit lock icon on the browser's status bar, or a website address that begins with "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof – some scammers have forged security icons.

- **Read website privacy policies.** They should explain what personal information the website collects, how the information is used, and whether it is provided to third parties. The privacy policy also should tell you whether you have the right to see what information the website has about you, whether they provide and/or sell your information to third parties, and what security measures the company takes to protect your information. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

Monitoring Your Personal Information

- ✓ Check your financial information regularly, and look for what should be there and what shouldn't.

- ✓ Ask periodically for a copy of your credit report. **You are able to get a free credit report once a year from each of the three main credit reporting companies. Consider asking for a new report quarterly so you are able to monitor your credit history regularly.**

- ✓ Maintain careful records of your banking and financial accounts.

Strong Passwords

A good password is one that's hard to guess, yet easy to remember. Passwords should **never** be written down or stored online. **Change your password at least every 60 days.**

A strong password has the following characteristics:

- Has at least eight characters
- Contains both upper and lower case letters (a-z, A-Z)
- Has digits and punctuation characters (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Is not a word in any language, slang, dialect, or jargon
- Is not based on personal information (names of family, pets, co-workers, birthdays, etc.)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be "This May Be One Way To Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password Don'ts

- Don't reveal a password over the telephone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to your boss, colleagues or family members.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Do not use the "Remember Password" feature of any application or website.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Don't use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Don't use common computer terms or company names, such as “State of Wisconsin” or “password.”

Keeping Kids Safe Online

- **Be involved.** Consider activities you can work on together, whether it's playing a game, researching a topic you had been talking about (family vacation spots, a hobby, a historical figure), or putting together a family newsletter. This will allow you to supervise your child's online activities while teaching good computer habits.

- **Keep your computer in an open area**. If your computer is in a high-traffic area, you will be able to easily monitor the computer activity. This deters a child from doing something they know they are not allowed to do, and it also gives you the opportunity to intervene if you notice a behavior that could have negative consequences.

- **Set rules and warn about dangers**. Make sure your child knows the boundaries of what he/she is allowed to do on the computer. These boundaries should be appropriate for the child's age, knowledge, and maturity, but they may include rules about how long they are allowed to be on the computer, what sites they can visit, what software programs they can use, and what tasks or activities they are allowed to do. You should also talk to children about the dangers of the internet so that they recognize suspicious behavior or activity. The goal isn't to scare them – it's to make them more aware.

- **Monitor computer activity**. Be aware of what your child is doing on the computer, including which websites they are visiting. If they are using email, instant messaging or chat rooms, get a sense of who they are corresponding with and whether they actually know them.

- **Keep lines of communication open**. Let your child know they can approach you with any questions or concerns about behaviors or problems they may have encountered on the computer.

- **Consider partitioning your computer into separate accounts.** Most computers give you the option of creating a different user account for each user. If you're worried that your child may accidentally access, modify, and/or delete your files, you can give them a separate account and decrease the amount of access and number of privileges they have.
  - If you don't have separate accounts, you need to be especially careful about your security settings. In addition to limiting functionality within your internet browser, avoid letting your browser remember passwords and other personal information. It is always important to keep your virus definitions up to date.

- **Implement parental controls.** Many computers and some anti-virus programs have an option to configure parental controls that can help you control and monitor what your child does online.

Below are some helpful websites for parents:

Kids.getnetwise.org
OnGuardOnline.gov
Search for Microsoft Windows - Parental Controls
Search for FBI - Parent Guide to Internet Safety

Wi-Fi Networks

Using a public wireless network or hotspot can expose you to risks you should know about:

- Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk.

- Enable or install a firewall. A firewall is the first line of defense for your computer since it's designed to prevent unauthorized access to your computer. Firewalls screen incoming and outgoing access requests to make sure they are legitimate and approved. Both Windows and Mac operating systems have built-in firewalls that you should make sure are enabled, especially before connecting to a public wi-fi.

- Because you're likely to connect to an unsecured, unencrypted network connection when you use public wi-fi , be careful about what you do online. Consider avoiding online banking, online shopping, sending email and typing passwords or credit card numbers.

This information comes from the Multi-State Information Sharing and Analysis Center.

If You Are a Phishing or Identity Theft Victim

- **If you believe you've been scammed or you're a victim of phishing, contact the Federal Trade Commission** to report the situation. They can be reached online at www.consumer.gov/idtheft or call 1-877-438-4338.

- **Contact all financial institutions where you do business.** You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).
- **Contact all creditors where your name or data has been fraudulently used.** For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

- **You may also need to contact other agencies for other types of identity theft:**
    - Your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity.
    - The Social Security Administration if you suspect that your Social Security number is being fraudulently used. Call 800-269-0271 to report the fraud.
    - The Internal Revenue Service if you suspect the improper use of your identification on federal tax return filings. Call 1-800-829-0433 to report the violations.
    - The Wisconsin Department of Revenue if you suspect the improper use of your identification on state tax return filings. Call 608-266-2486 to report the violations.

- **Contact the major check verification companies:**
    - CheckRite -- (800) 766-2748
    - ChexSystems -- (800) 428-9623
    - CrossCheck -- (800) 552-1900
    - Equifax -- (800) 437-5120
    - National Processing Co. (NPC) -- (800) 526-5380
    - SCAN -- (800) 262-7771
    - TeleCheck -- (800) 710-9898

Contacting the Credit Agencies

If you are a victim of identity theft, call the fraud units of the three principal credit reporting companies to alert them. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report.

You can also ask the credit agencies to put a "fraud alert" on your credit file. This is something that the major credit bureaus attach to your credit report. When you or someone else tries to open up a credit account by getting a new credit card, loan or apply for credit, the lender should contact you by phone to verify that you really want to open a new account. If you aren't reachable by phone, the credit account shouldn't be opened. This should slow down anyone trying to open credit in your name.

You can request a fraud alert even if you aren't a victim of identity theft.

- Equifax: (800) 525-6285
- Experian: (888) 397-3742
- Trans Union: (800) 680-7289

You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

Other Helpful Resources

Kids.getnetwise.org
OnGuardOnline.gov
Federal Trade Commission
Wisconsin Office of Privacy Protection