West Virginia Executive Branch
Privacy Tip

October is National Cyber Security Awareness Month!

In recognition of National Cyber Security Month, we are supplying tips to keep you safe in your work life and your "away from work" life also!

Keep a Clean Machine.

- **Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.**

- **Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.**

- **Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.**

- **Plug & scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.**

Used with permission National Cyber Security Alliance STOP. THINK. CONNECT. www.staysafeonline.org

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

West Virginia Executive Branch
Privacy Tip

October is National Cyber Security Awareness Month!

Each week we will give you a tip to help you stay Cyber Safe!

This week's tip:

Protect Your Personal Information

- Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.
- Write it down and keep it safe: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Used with permission National Cyber Security Alliance STOP. THINK. CONNECT. www.staysafeonline.org

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

WV Executive Branch Privacy Tip

In recognition of Cybersecurity Month, the Office of Technology is supplying tips to keep you safe in your work life and your "away from work life" also.

Good Security Habits

There are some simple habits you can adopt that, if performed consistently, may dramatically reduce the chances that the information on your computer will be lost or corrupted.

How can you minimize the access other people have to your information?

You may be able to easily identify people who could, legitimately or not, gain *physical* access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. 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 or corrupting your information; however, you can develop habits that make it more difficult.

- **Lock your computer when you are away from it.** Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.
- **Evaluate your security settings.** Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate.

What other steps can you take?

Sometimes the threats to your information aren't from other people but from natural or technological causes. Although there is no way to control or prevent these problems, you can prepare for them and try to minimize the damage.

- **Protect your computer against power surges and brief outages.** Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.
- **Back up all of your data.** Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information. Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.
National Cyber Security Alliance STOP. THINK. CONNECT. www.staysafeonline.org

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

WV Executive Branch Privacy Tip

In recognition of Cybersecurity Month, the Office of Technology is supplying tips to keep you safe in your work life and your "away from work life" also.

Debunking Some Common Myths

There are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself.

How are these myths established?

There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true.

Why is it important to know the truth?

While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?

- *Myth: Anti-virus software and firewalls are 100% effective.*
  Truth: Anti-virus software and firewalls are important elements to protecting your information. However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.
- *Myth: Once software is installed on your computer, you do not have to worry about it anymore.*
  Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities. You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.
- *Myth: There is nothing important on your machine, so you do not need to protect it.*
  Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other.
- *Myth: Attackers only target people with money.*
  Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage.
- *Myth: When computers slow down, it means that they are old and should be replaced.*
  Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack.

National Cyber Security Alliance STOP. THINK. CONNECT. www.staysafeonline.org

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

WV Executive Branch Privacy Tip

In recognition of Cybersecurity Month, the Office of Technology is supplying tips to keep you safe in your work life and your "away from work life" also.

Reducing Spam

Spam is a common, and often frustrating, side effect to having an email account. Although you will probably not be able to eliminate it, there are ways to reduce it.

What is spam?

Spam is the electronic version of "junk mail." The term spam refers to unsolicited, often unwanted, email messages. Spam does not necessarily contain viruses—valid messages from legitimate sources could fall into this category.

How can you reduce the amount of spam?

There are some steps you can take to significantly reduce the amount of spam you receive:

- **Don't give your email address out arbitrarily** - Email addresses have become so common that a space for them is often included on any form that asks for your address—even comment cards at restaurants. It seems harmless; so many people write them in the space provided without realizing what could happen to that information. For example, companies often enter the addresses into a database so that they can keep track of their customers and the customers' preferences. Sometimes these lists are sold to or shared with other companies, and suddenly you are receiving email that you didn't request.
- **Check privacy policies** - Before submitting your email address online, look for a privacy policy. Most reputable sites will have a link to their privacy policy from any form where you're asked to submit personal data. You should read this policy before submitting your email address or any other personal information so that you know what the owners of the site plan to do with the information.
- **Be aware of options selected by default** - When you sign up for some online accounts or services, there may be a section that provides you with the option to receive email about other products and services. Sometimes there are options selected by default, so if you do not deselect them, you could begin to receive email from lists those lists as well.
- **Use filters** - Many email programs offer filtering capabilities that allow you to block certain addresses or to only allow email from addresses on your contact list. Some ISPs offer spam "tagging" or filtering services, but legitimate messages misclassified as spam might be dropped before reaching your inbox. However, many ISPs that offer filtering services also provide options for tagging suspected spam messages so the end user can more easily identify them. This can be useful in conjunction with filtering capabilities provided by many email programs.
- **Report messages as spam** - Most email clients offer an option to report a message as spam or junk. If your has that option, take advantage of it. Reporting messages as spam or junk helps to train the mail filter so that the messages aren't delivered to your inbox. However, check your junk or spam folders occasionally to look for legitimate messages that were incorrectly classified as spam.
- **Don't follow links in spam messages** - Some spam relies on generators that try variations of email addresses at certain domains. If you click a link within an email message or reply to a certain address, you are just confirming that your email address is valid. Unwanted messages that offer an "unsubscribe" option are particularly tempting, but this is often just a method for collecting valid addresses that are then sent other spam.
- **Disable the automatic downloading of graphics in HTML mail** - Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message—when your mail client downloads the graphic from their web server, they know you've opened the message. Disabling HTML mail entirely and viewing messages in plain text also prevents this problem.

- **Consider opening an additional email account** - Many domains offer free email accounts. If you frequently submit your email address (for online shopping, signing up for services, or including it on something like a comment card), you may want to have a secondary email account to protect your primary email account from any spam that could be generated. You could also use this secondary account when posting to public mailing lists, social networking sites, blogs, and web forums. If the account start to fill up with spam, you can get rid of it and open a different one.
- **Use privacy settings on social networking sites** - Social networking sites typically allow you to choose who has access to see your email address. Consider hiding your email account or changing the settings so that only a small group of people that you trust are able to see your address. Also, when you use applications on these sites, you may be granting permission for them to access your personal information. Be cautious about which applications you choose to use.
- **Don't spam other people** - Be a responsible and considerate user. Some people consider email forwards a type of spam, so be selective with the messages you redistribute. Don't forward every message to everyone in your address book, and if someone asks that you not forward messages to them, respect their request.

National Cyber Security Alliance STOP. THINK. CONNECT. www.staysafeonline.org

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.