State of West Virginia
Monthly Security Tips
NEWSLETTER

April 2011 Volume 6, Issue 4

Safeguarding Your Personal Data

From the Desk of the West Virginia Office of Information Security and Controls – Jim Richards, Director (Jim.A.Richards@wv.gov)

Computers and the Internet have become an important part of our daily life, enabling a wide range of services to home users such as communicating with friends and family, shopping, paying bills, storing personal photos and music. This convenience and inter-connectivity does not come without risk however. Potential threats include viruses that could erase your entire system or hackers stealing your credit card information.

By understanding the risks and combining some common sense rules with a little bit of technology, home users can safeguard their data from these threats and understand the needs for security controls at work. The following tips will help protect your data.

Back Up Your Data

Your hard drive may crash or you may find that an infection has affected your computer so much that the operating system and applications need to be reinstalled. In cases like this it is best to have your important data backed up so you can restore your system without fear of losing your data. Below are some important steps you can follow:

- **Use your computer's backup tools.** Most operating systems provide backup software designed to make the process easier. External hard drives and online backup services are two popular vehicles for backing up files.
- **Back up data at regular intervals**. Weekly backups are recommended.
- **Verify the data has been backed up.** Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately.
- **Verify the ability to restore.** It is a best practice to periodically test that your backup data can be restored if loss occurs.

Use Strong Passwords

Passwords help protect your data. It is important to have a strong password for your computer, mobile device, and any other media used to store important and/or sensitive data. A strong password is at least eight characters that use a mix of upper case, lower case, and numeric or special characters. Each device should have its own strong password so that if one is compromised your others will stay secure.

Be Safe Online

- Below are a few helpful tips on how to keep safe on the Internet:
- Keep your operating system updated/patched. Set it to “auto update.”
- Use anti-virus and anti-spyware software and keep them updated.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for

"secure" and indicates that the communication with the webpage is encrypted.

- Keep your applications (programs) updated and patched, particularly if they work with your browser to run multi-media programs used for viewing videos. Set these programs to "auto update."
- Block pop-up windows, some of which may be malicious and hide attacks. This may prevent malicious software from being downloaded to your computer.

Encryption

Encryption is a process whereby the data is scrambled and can only be read by someone with the "encryption key" to unscramble the data. Users should consider encrypting sensitive information. Some new operating systems include tools to encrypt data while others require the installation of encryption software.

Dispose of Information Properly

It is important to properly handle data erasure and disposal of electronic media (e.g. PCs, CDs, thumb drives) in order to protect confidential and sensitive data from accidental disclosure. Become familiar with the proper methods of sanitizing, destroying, or disposing of media containing sensitive information.

Before discarding your computer or portable storage devices, you need to be sure that data has been erased or "wiped." Below are a few tips to assist in disposing your data:

- Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software. Software that meets DOD compliance standards can be downloaded from the Internet at no cost.
- Shred CDs and DVDs. This type of media should be physically destroyed.
- Media that does not have a need to be re-used or contains sensitive or private data that cannot be "wiped" should be physically destroyed.

Resources For More Information:
US-CERT Tips for Safeguarding Your Data
http://www.us-cert.gov/cas/tips/ST06-008.html
MS-ISAC Guidelines for Backing Up Information
http://www.msisac.org/awareness/
MS-ISAC Newsletter – Backing Up Your Files
http://www.msisac.org/awareness/news/2010-02.cfm
MS-ISAC Newsletter – Using Encryption to Protect Data
http://www.msisac.org/awareness/news/2008-05.cfm
MS-ISAC Tip – Surf Safe On The Internet
http://www.msisac.org/daily-tips/Surf-Safe-on-the-Internet.cfm
MS-ISAC Newsletter – Erasing Information and Disposal of Media
http://www.msisac.org/awareness/news/2006-08.cfm

For more monthly cyber security newsletter tips, visit:
http://www.technology.wv.gov/security/Pages/monthlynewsletter.aspx