



Multi-State Information Sharing & Analysis Center (MS-ISAC)

Monthly Cyber Security Tips

NEWSLETTER

March 2007

Volume 2, Issue 3

Safeguarding Your Data

From the Desk of William F. Pelgrin, Chair

How do you safeguard sensitive/confidential data? The manner of protection often depends on what kind of data you are safeguarding, how important or sensitive it is to you, to your organization or your customers.

The following tips will help you become aware of how to protect data both at work and at home.

Types of data

Data can be defined, or classified, with labels such as public, personal, sensitive, confidential, secret, top-secret, or other categories. The more valuable or sensitive the data, the more it needs to be protected. By classifying the data you handle you are performing the first step of protection - by knowing what your data is you can then implement specific kinds of controls for that data.

Some types of data might already be classified in some way by federal or state law, or require specific levels of protection because they are covered in laws or standards such as the Health Insurance Portability and Accountability Act, or in the Payment Card Industry Standards. Yet even at home or at work you may handle data that might not be covered by these laws or standards but still are sensitive or confidential, like credit card numbers, account numbers, personnel information, Social Security numbers, tax records, network diagrams, business plans, passwords, sensitive emails, or personal medical records. Whether it is work data or your personal or family data, you need to understand what the data is and what might happen if that data becomes compromised. Then you can work to protect that data accordingly.

Below are tips on how to safeguard your data.

Access to the Data

- **Password-protect your access** - Use a strong password or pass-phrase to protect access to your data.
- **Identify where the data is stored** - Have specific places within your network or computer where you store sensitive/confidential data. Those network shares, hard drives, servers, or system folders can then have specific protection methods used to keep them more secure.
- **Limit transportation and transmission of data** - Refrain from transporting or transmitting sensitive/confidential data if you don't need to do so. For example, don't allow your sensitive/confidential data to be sent via email or removed on a USB stick unless there is a clear need. When you do transport or transmit it, ensure that it has an appropriate level of security.
- **Limit physical access** - Whenever possible, store sensitive/confidential data on devices that are physically secured. Allow only authorized individuals access to those devices, and monitor access to those devices whenever possible.

- **Restrict network or shared access** - Do not allow anyone access to sensitive/personal data unless they specifically require access. At work a web server administrator may not need access to confidential data in the backend database, a manager may not need access to the network password storage files, or a secretary may not need access to sensitive personnel files. Similarly at home, your children do not need access to your electronic tax records or bank account records. By limiting access to sensitive/confidential data to only those who really need it you can limit the risk of both accidental and malicious exposure. Additionally, by limiting access to only those requiring it, you are not only protecting the data, you are protecting your organization/family as well.
- **Temporary data storage** - If you need to store sensitive/confidential data temporarily on a memory stick, laptop, or other device, remove that data from the device when you have finished. Ensure that data has been completely erased and not just deleted. Be sure to only use the method or tool your organization has approved. See *August 2000 Newsletter on "Erasing Information and Disposal of Media"*.
- **Encrypt stored sensitive/confidential data** - Whenever possible, encrypt stored sensitive/confidential data, whether it is being permanently or temporarily stored. This can help prevent unintended disclosure even if your system has been compromised. Data can be protected by encrypting the entire storage drive (whole disk encryption) or as selectively as you need, such as by folder or even individual files. Be sure to only use the method or tool your organization has approved. If the encryption key or password is lost, access to the data may be lost as well. There are many products or options available, so be sure to carefully select one that is right for you and your organization.
- **Use separate local or network accounts** - By using separate accounts, individuals can be assigned very specific access rights and privileges. Using separate accounts with differing access levels limits the potential for accidental or malicious data exposure. In addition, it is far easier to attribute actions to a specific person using their unique account than to a single person in a group of people utilizing a shared account.
- **Limit the type of access an account or process requires** - Limit the kind of access to sensitive/confidential data based on how that data needs to be handled. For example, auditors often only require 'read' access to data files and cannot 'write' or alter a file's contents. Conversely, a system program may only need to execute or run a program without needing to access the confidential data it is handling. At home and work, use your computer as a standard user instead of an administrator to limit what files or data you may have access to on a daily basis. By limiting the kind of access an account has, you can limit what data or systems configuration controls can be accessed as well.

The US-CERT has created the following tips to help protect both your personal and work-related data by protecting the computer systems that handle your organization's data.

- **Use and maintain anti-virus software and a firewall** - Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall (see [Understanding Anti-Virus Software](#) and [Understanding Firewalls](#) for more information). Make sure to keep your virus definitions up to date.
- **Regularly scan your computer for spyware** - Spyware or adware hidden in software programs may affect the performance of your computer and give attackers access to your data. Use a legitimate anti-spyware program to scan your computer and remove any of these files (see [Recognizing and Avoiding Spyware](#) for more information).
- **Keep software up to date** - Install software patches so that attackers cannot take advantage of known problems or vulnerabilities (see [Understanding Patches](#) for more information). Many operating systems offer automatic updates. If this option is available, you should turn it on.
- **Evaluate your software's settings** - The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the Internet (browsers, email clients, etc.). Apply the highest level of security available that still gives you the functionality you need. Note, business users should follow their organizations policy on software settings.

- **Avoid unused software programs** - Do not clutter your computer with unnecessary software programs. If you have programs on your computer that you do not use, consider uninstalling them.
- **Establish guidelines for computer use** - If there are multiple people using your computer, especially children, make sure they understand how to use the computer and Internet safely. Setting boundaries and guidelines will help to protect your data (see [Keeping Children Safe Online](#) for more information).
- **Follow corporate policies for handling and storing work-related information** - If you use your computer for work-related purposes, make sure to follow any corporate policies for handling and storing the information. These policies were likely established to protect proprietary information and customer data, as well as to protect you and the company from liability.
- **Dispose of sensitive information properly** - Simply deleting a file does not completely erase it. To ensure that an attacker cannot access these files, make sure that you adequately erase sensitive files (see [Effectively Erasing Files](#) for more information).
- **Follow good security habits** - Review other [security tips](#) for ways to protect yourself and your data.

Brought to you by:



MS-ISAC

<http://www.msisac.org>



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

<http://www.us-cert.gov/>