



# NYS Office of Cyber Security

## Monthly Security Tips NEWSLETTER

November 2012

### Using Encryption to Protect Data

#### *From the Desk of Thomas D. Smith, Director*

According to the Privacy Rights Clearinghouse, more than 23 million records have been involved in a data breach so far this year. Protection of data requires multiple layers of defense and the use of encryption to secure sensitive data is a critical tool in this multi-layered approach.

Encryption scrambles a message or file so that only the sender and the authorized receiver can decode it with the proper decryption key. Encryption solutions generally encompass two types: hardware and software. Examples of hardware encryption include a pre-encrypted USB device or hard drive. Software encryption consists of a program installed on a machine that encrypts some or all of the data on the system.

The list below includes guidance on how, when and where encryption should be implemented in order to enhance security and data protection:

- **Laptop protection** - Theft of laptops can result in unsecured information being used by a third party to gain access to bank accounts, internal networks, and other sensitive information. A stolen company laptop can become a security risk if it contains confidential information or passwords for a closed network. Enabling laptop encryption is a recommended way to reduce these risks, while ensuring that information cannot be easily retrieved. Laptops can be encrypted in various ways such as encrypting specific directories and files or encrypting the entire hard drive (full disk encryption). Some analysts recommend using both forms of encryption on the same laptop as that is more secure than either method on its own. Minimally, file level encryption should be implemented while full disk encryption is a best practice.
- **Wireless networks** – The first line of defense for a Wi-Fi network is encryption, which encodes the data transmitted between your electronic device and the wireless access point. Unfortunately, most wireless access points ship with encryption turned off and many owners of wireless access points don't turn encryption on, leaving users completely exposed. If you haven't already, enable your wireless access point's encryption, and use the strongest form supported by your network. The Wireless Protected Access (WPA) protocol and more recent WPA2 have supplanted the older and less-secure Wireless Encryption Protocol (WEP). It is highly recommended that your network support WPA2. Both WPA and WEP are considered to be significantly weaker, as the algorithms for those have been cracked.
- **E-mail** – It is important to realize that e-mail and instant messages (IM) pass through numerous servers and routers before reaching their final destination. Standard e-mail messages are sent in plain text, so it's possible for someone else to snoop and read them. When you encrypt mail, on the other hand, it makes the messages completely unreadable to anyone who doesn't possess a decryption key. There are several ways to encrypt e-mail. The simplest way is to use software that plugs into your existing e-mail client. Confidential or sensitive data should not be sent via e-mail in clear text.
- **Backup tapes and media** – Organizations regularly create backups on media that are then stored at an outside facility. These backups should be encrypted to prevent unauthorized access in the event of a physical breach.
- **Removable media** – CDs, DVDs, and USB flash drives are great for transporting files and documents from the office to a meeting or on a business trip. This portability does however have inherent risk. The media is often small and easy to lose or misplace. Your best defense is to encrypt the files on your removable media or use, where available, pre-encrypted removable media such as a pre-encrypted USB drive.

- **Smartphones, PDAs and other similar devices** – Gone are the days when a cell phone is used primarily for placing phone calls. Modern smartphones, PDAs, etc., can surf the Internet, e-mail, text and take pictures and videos. They have large amounts of internal memory capable of storing large volumes of information. Though this is undoubtedly convenient, it makes losing your phone a frightening prospect. With so much personal data at risk, and identity theft such a major concern, you need to take steps to protect yourself. It is recommended that you enable the encryption features on your smartphone. Further information may be found on the following sites:
  - **Encryption on Blackberries:**  
How to encrypt files on an installed media card in the BlackBerry smartphone - [http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB12999&sliceId=2&cmd=displayKC&dialogID=115279&docType=kc&isLoadPublishedVer=&stateId=115282&docTypeID=DT\\_SUPPORTISSUE\\_1\\_1&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl](http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB12999&sliceId=2&cmd=displayKC&dialogID=115279&docType=kc&isLoadPublishedVer=&stateId=115282&docTypeID=DT_SUPPORTISSUE_1_1&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl)
  - **Data Protection in iOS Devices:**  
<http://support.apple.com/kb/HT4175>
  - **Encryption on Android Devices:**  
<http://support.google.com/android/bin/answer.py?hl=en&answer=1663755>

A variety of encryption tools are available in the marketplace, some of which are open source. Please note, any solution you implement should be compliant with accepted industry standards. Given the current environment, you should minimally employ a 128-bit Advanced Encryption Standard (AES) solution.

**For more cyber security monthly tips go to:**  
[www.dhSES.ny.gov/ocs/awareness-training-events/news/](http://www.dhSES.ny.gov/ocs/awareness-training-events/news/)

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

**Brought to you by:**

