10 Tips of the Day

John Hally
1/12/12

1. **Know who you are allowing to enter a secure building or area.**

   It is polite to hold the door open for someone, but this circumvents the purpose of physical security access controls. If they have an access card, make sure they swipe it before entering. If they do not have an access card, direct them to Reception.

2. **Sanitize configuration files/examples as much as possible when submitting information for technical support.**

   It is common practice to submit configuration files or examples when requesting technical support. Always make sure to sanitize this information as much as possible. Items that should be able to be obfuscated are:

   SNMP community strings

   IP addresses (unless required for specific issues such as routing)

   User account information

   NEVER submit actual configuration information to forums or email distribution lists. This information could be discovered during reconnaisance if you are targeted by attackers.

3. **Always check the file hash to validate downloads.**

   When downloading files, you should always check the file hash from the download location against the hash of the files that were downloaded. Most linux systems have a built in command for generating MD5 hashes called md5sum. Running the command md5sum <filename> will generate the hash value that can be compared to the hash value supplied by the download site. Mac users can use the built-in command md5 in the same way.

   Windows users unfortunately have to install a third party application. Microsoft has an unsupported tool that will generate both MD5 and SHA1 hashes (http://support.microsoft.com/kb/841290). There are also other commercial tools as well as plugins for the firefox browser.

   It is also good practice to validate the hash value against multiple download sites if possible.

4. Nuke that media!

Always make sure to wipe any media that you are going to donate or discard. Disk drives from older PCs that have been discarded or donated can be a treasure trove for nefarious individuals looking to gather sensitive personal data to steal identities. Before discarding any media make sure the data is eliminated. Erasing files does not get rid of all the data on all of the sectors on the disk. Tools such as DBAN (Darik's Boot and Nuke) http://www.dban.org is a free utility that can be used to securely wipe the disks of most computers.

CD/DVD discs should be shredded. Heavy duty shredders that can handle CDs and DVDs can be purchased at local office supply stores.

5. Identity Theft - Monitor your credit.

With the proliferation of identity theft, any precaution that can be taken should be taken. One of the simplest things you can do is to monitor your credit for any suspicious activity. You can do this yourself by requesting and reviewing your credit history (free once a year from each credit reporting agency), or you can sign up for a monitoring service to watch your history and notify you of any discrepancies. It is also a good idea to stagger the free report requests during the year in order to detect inconsistencies or errors earlier. There are plenty of commercial vendors who offer this service (LifeLock, IdentityGuard), but you may be already eligible for credit monitoring through one or more of your existing credit card providers. More tools and tips are available by the Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html

6. Google search yourself.

Google (and other search engines) find an amazing amount of information, and sometimes the information may not be intended for the world to see. It is a common practice for hackers to scour search engines for sensitive information that has found itself indexed inadvertently. With that in mind, it is a good idea to perform searches on Google and other search engine sites for sensitive information about yourself. Searching your full name with other items such as address, phone number, social security number, etc. can tell you if any sensitive information about you has somehow leaked into the search engine's database, and if so, steps can be taken to remove the information. Google in particular has online tools that can expedite this process located here:

http://support.google.com/bin/static.py?hl=en&ts=1114905&page=ts.cs

Always remember to use caution whenever sending blogging, posting to forums, using social media, and any other form of Internet activity.

7. Work from home and make a fortune!

In tough economic times there are plenty of people either out of work or looking for supplemental income. Individuals seeking employment opportunities should be wary of job opportunities that seem too good to be true. Many times these job offers that offer high pay potential by working in the comfort of your own home doing simple tasks are just scams looking to gather your personal information or worse. These job opportunities have been seen on websites such as Monster.com, Craigslist, and others.

Be wary of ads that:

- Promise huge compensation that is not within the normal range for the job type (i.e. up to thousands of dollars a month for small part assembly).
- Require the submission of sensitive information such as a social security number.
- Require a processing payment.
- No company information or limited contact information such as a first name and a phone number that only allows you to leave a message.
- Uses incorrect spelling, grammar, or format such as ALL CAPS, incorrect punctuation, etc.

If a company name is divulged, check the Better Business Bureau to see if it is a legitimate business. Always trust your instincts and if it doesn’t seem right, keep looking.

8. Be wary of that ATM.

Be careful when using ATMs. There have been numerous reports of ATM machines that were outfitted with account skimmer hardware to steal credit card or bank card account information on ATMs. When using ATMs:

- Avoid the small portable units sometimes located in out of the way areas.
- Avoid using ATMs in dimly lit areas.
- Avoid ATMs that appear to be damaged in any way.
- Use ATMs at physical bank branch locations.

Additionally, review all of your monthly statements for signs of unauthorized usage.

9. iPhone/iPad Erase Data After 10 Passcode Attempts.

A simple way to protect your sensitive data from an iPhone is to enable the "Erase Data After 10 Passcode Attempts" setting. This is located under Settings -> General -> Passcode Lock. When enabled, the device will erase all of the data contained within the phone after the 10th consecutive attempt to enter a passcode and return it to the factory default state. Provided that frequent backups are performed, a full restore from iTunes will return the phone configuration. More information can be found at: http://support.apple.com/manuals/

10. Find My iPhone/iPad.

A great security feature available on the iPhone and iPad is the 'Find My iPhone/iPad" setting. By enabling this feature you can:

- Locate the device on a map.
- Send a message to the device, or play a sound.
- Remotely lock the device.
- Remotely wipe the data on the device.

These tasks can be performed by using the Find My iPhone app on another device. These features also require the iCloud or MobileMe settings to be configured as well. By enabling these features, the device can be located if lost or stolen, and/or the sensitive data destroyed. More information on these features can be found at: http://support.apple.com/manuals/