MGT-438: How to Establish a Security Awareness Program
Ten Security Tips
TJ OConnor

1. Demand HTTPS Everywhere

The HTTPS protocol adds the SSL/TLS encryption protocol to the standard Hypertext Transfer Protocol (HTTP). Without using HTTPS to secure a connection, many clients are vulnerable to man-in-the-middle attacks or their traffic being intercepted by attackers. Many sites on the web only offer HTTPS only by opting-in to the protocol. To force a secure connection, try using the Electronic Freedom Foundation's HTTPS-Everywhere. For more information, visit :http://www.eff.org/https-everywhere.

2. No Script For You

One way attackers can compromise your computer is to run malicious JavaScript code in your web browser. In fact, this is the very way Google and 34 other companies were attacked in January of 2010. To prevent malicious JavaScript from running on your computer, enable the NoScript plugin. The NoScript plugin allows you to enable JavaScript for only the web sites of your choice. In addition, NoScript provides a powerful protection mechanism for Cross Site Scripting (XSS) attacks. For more information, visit: http://noscript.net/

3. Patch Those Third Party Apps

Most of us do a great job of keeping our Operating System updated with the latest security updates. However, we all do a worse job of patching third party application such as Adobe Reader, Apple iTunes, or Mozilla Firefox. Leaving those applications unpatched creates several vulnerabilities for attackers to exploit our systems. Try using a central tool to keep all your third party applications patched and updated to the latest version. For more information, see http://www.shavlik.com/sol-patch-management.aspx

4. Keep Your Data At Rest Safe, Enable Full Drive Encryption

Think very carefully, if an attacker stole your laptop today – what important or sensitive data would he have access to? What can an attacker access while your laptop is sitting unprotected in the office or the hotel? Prevent your computer from the worst-case scenario, use full-drive encryption to encrypt the contents of your entire hard drive. By using an algorithm such as AES-128 and a complex password, you can almost guarantee the attacker will not be able to read your sensitive files. Third party applications such as TrueCrypt can enable full drive encryption on your computer. Microsoft's Bit Locker also can encrypt the full drive. For more

information see either http://www.truecrypt.org/ or http://technet.microsoft.com/en-us/library/cc766200(WS.10).aspx.

5. Avoid Becoming a Sheep, Use Only WPA Protected Networks

Recently, a hacker released the Firesheep toolkit. It works by listening to unencrypted wireless traffic and intercepting cookies used on web sites to authenticate users. By reusing these cookies, the attacker can login to your Google, Facebook, Flickr, or Twitter accounts with your credentials. Prevent this very simple attack by always using WPA protected Networks that require you to enter a pass phrase to authenticate to the network and securely encrypt the end-to-end traffic between your laptop and the access point . Fore more information about FireSheep see http://codebutler.com/firesheep.

6. Open It Up Yourself, Avoid the Tab-Nab

A recent attack, dubbed tab-nabbing, opens impersonations of well known web sites in a browser's tab. A user, seeing the well known web site logs in and submits their account and password to the attacker. Prevent this from happening to you. If you didn't open the web site yourself, don't submit your login details and password. Fore more information on tab-nabbing, see http://en.wikipedia.org/wiki/Tabnabbing.

7. A Proxy Will Keep You Safe

A proxy can act as an intermediary between a client and a web server. Using a proxy to request your Internet traffic can help prevent attacks launched from malicious web pages. It can also aid in phishing attacks, where users click on links to malicious pages. You can either build a proxy yourself, by using popular open source software such as the Squid Web Proxy (http://www.squid-cache.org/) or pay for a proxy service. Several web sites offer black lists of known malicious web sites that can be incorporated into your proxy. For more on black lists, see http://www.shallalist.de/ or http://urlblacklist.com/?sec=download.

8. Delete Your Mobile Device Back-Ups

Your mobile device back-up has quite a bit of information about you. It may contain your text-messages, recent phone calls, recorded voice mails, emails, mobile banking information or even all the locations your phone has been. This back-up file is made and updated every time your phone is synched or paired with your computer. An attacker that gains access to your computer can get quite a bit of information about you. To see how an attacker can extract files, see http://supercrazyawesome.com/. For more information on deleting your iPhone mobile device back-up, see http://support.apple.com/kb/ht1766.

9. When Traveling, Use a VPN to Keep You Safe

When traveling, you are often forced to use unsecure wireless networks, guest corporate networks, or even Internet cafes. All of these networks lack the encryption and authentication methods to keep you safe. To use all of the encryption, authentications, and certification features of your normal private network, use a virtual private network (VPN) to protect yourself. By tunneling your traffic through a VPN, you can safely use the Internet while on an unsecure network. For a free VPN solution, take a look at http://openvpn.net/.

10. Avoid The Man-In-The-Middle Attack, Watch Your Arp

A man-in-the-middle attack on your local area network (LAN) can intercept your sensitive traffic by impersonating the physical address of your destination and relaying the traffic. An attacker can even disable SSL/TLS encryption used by web sites. The dsniff toolkit (http://monkey.org/~dugsong/dsniff/) allows attackers to passively and actively perform man-in-the-middle attacks. What's even scarier is that most network-based intrusion detection systems exist at our perimeter and not behind our LAN. To detect man-in-the-middle attacks, use a tool such as ArpWatch that monitors the physical and logical address pairings. For more information on ArpWatch see http://ee.lbl.gov/.