The Critical Dozen

By:

Mark Massey
Accessible Computer Security
727 – 644-0188
Mark@markmassey.org

Kathryn Kleiman, Esq.
Internet Counsel, Fletcher, Heald & Hildreth, PLC
703-812-0476
Kleiman@fhhlaw.com

The Critical Dozen

1. Do not open attachments in e-mails from people you do not personally know.
2. Do not ever type your credit card or bank information into a browser (Internet Explorer, Firefox, Chrome) unless it shows a Lock and says “HTTPS” in the address window.
3. Do use a modern Anti-Malware program and set it to automatically update.
4. Do keep All of the software on your systems licensed and up to date.
5. If you use a Point of Sale device that is a PC ensure that it is never used to surf the Web.
6. Do use a “Safe Search” tool bar.
7. Realize that sooner or later a disaster will happen to your system and plan for it.
8. Do have a “Firewall”.
9. Ensure that all default passwords have been changed to something hard to guess on all of your systems.
10. Do have a written computer usage security policy for your organization and see to it that all users have read it and understand it.
11. If your business uses portable devices, ensure that client and business information stored on them is encrypted.
12. Do not let people who do not appreciate (or understand) the need for data security use your business computers.

A Bit Deeper Dive

- Do not open attachments in e-mails from people you do not personally know.
  - Opening an attachment is the same as allowing the execution of a computer program on your computer. There is a substantial chance it contains some kind of malware!

- Do not ever type your credit card or bank information into a browser (Internet Explorer, Firefox, Chrome) unless it shows a Lock and says “HTTPS” in the address window.
  - HTTPS is an abbreviation for a method of communicating information that ensures the data can not be read in transit. It has other security features too.

- Do use a modern Anti-Malware program and keep it up to date.
  - Modern anti-malware programs include e-mail scanners, anti-virus, and often “safe browsing” capabilities. If you do nothing else do this!!
  - Some good affordable programs are: Viper, AVG, McAfee, Symantec

- Do keep All of the software on your up to date.
  - Software is written by people; people make errors and technology changes causing older safe methods to become unsafe. Good software companies make corrections to their software. These are called “patches”. It is very important that your systems have all needed corrections (patches) applied.

A Bit Deeper Dive

- If you use a Point of Sale (POS) device that is a PC ensure that it is never used to surf the Web.
  - According to Verizon Annual Security Survey most attacks on retail stores occur because an attacker was able to get into a POS device via the Internet. Surfing the Web with a POS is an invitation to trouble
- Do use a "Safe Search" tool bar.
  - This is a tool bar added to your browser. When you use it to search the web sites that have been checked and are known safe will have some kind of mark (for example a check mark) showing the site is known safe.
  - Such as AVG "Safe Search"
- Realize that sooner or later a disaster will happen to your system and plan for it.
  - This includes items such as having your data and applications backed up and fully RESTORABLE. It is the ability to Restore that is important (And needs to be tested regularly).
  - Ensure that there is a fairly recent back up kept off-site!
- Do have a "Firewall".
  - A firewall can be either hardware or software. It helps protect the security and privacy of your network and computer from unwanted communication from the Internet. Having a Firewall is very important!
- Ensure that the default password have been changed to something hard to guess on all of your systems.
  - Any technical person can find or already knows the manufacturer's default passwords to any system. This means the bad hats know them too! Leaving default passwords in place is an invitation to the bad guys.
- ONE MORE -- Use a high quality voltage regulating , battery backup uninterruptable power supply (UPS).
  - Some surge protectors may not be as effective as you may have been led to believe.

A Bit Deeper Dive

- Do have a written computer usage security policy for your organization and see to it that all users have read it and understand it.
  - The security policy should include points such as:
    - Do not download unauthorized software
    - Protect the personal information relating to customers, patients, and donors with the highest level of your organization's security.
    - Have a written privacy policy that describes how your organization accomplishes the above.
- If your business uses portable devices, ensure that client and business information stored on them is encrypted.
  - Encryption of information impacts the organization's liability in the event a device containing personal information is lost.
  - Encryption is available on practically every mobile device.
  - Password protect your portable device
- Do not let people who do not appreciate (or understand) the need for data security use your business computers.
  - Technology and information sharing is so much a part of younger peoples lives they might not natively realize the difficulties potentially connected with surfing the web.

Various Types of Malware

- There are various general categories of Malware - some of the most advanced malware has elements of each
- Here is a brief description and summary
  - Virus – A form of malware that does something destructive to a computer or data
  - Worm - A form of malware that duplicates itself from computer to computer
  - Trojans – A form of malware that delivers something else (some other form of malware into your system – such as a Spyware – see below)
  - Spyware – Something that tracks your actions and delivers this info to other systems
  - Root Kit – A technically advanced from of malware. Difficult to find and relatively dangerous. Thankfully somewhat hard to implement.
  - "Drive by Exploit"- This particular breed of nasty basically makes your computer execute instructions when you visit a website. What's particularly nasty about this one is that when it executes , it executes as though it is YOU executing it. In other words with your log in ID, security, etc!