

Cyber Security



TABLE OF CONTENTS

[INTRODUCTION](#)

[DEVICE-BASED
SECURITY MEASURES](#)

[ON-LINE FRAUD
PREVENTION](#)

[PERSONAL
INFORMATION
PROTECTION](#)

[RESOURCES](#)

[REFERENCES](#)

Cyber Security in the 21st Century

October 8, 2010

INTRODUCTION

The Internet is no longer a novelty. It is an established presence in many, many people's lives. Having grown from a computer-based 'fad' to an integral part of mobile phone technology, the Internet has become a must-have item for not only business people and students, but just plain folks.

Unfortunately, the Internet, available to virtually anyone, is also home to a whole new type of predator. No one is exempt from problems that could arise from this type of predator. Identity theft, cyberstalking, cyberbullying, all terms relatively new to users of the World Wide Web, have become items of global concern. Because of these concerns, yet another term has been coined, cyber security. People need to learn how to keep themselves and their [children safe online](#).

October is National Cyber Security Awareness Month (NCSAM). Microsoft and the National Cyber Security Alliance (NCSA) have teamed up with the Department of Homeland Security (DHS) to bring education and awareness to Internet users about keeping themselves and their Internet-

accessible devices safe. [1] For those with children using the Internet, teaching them about the risks as well as the benefits of the Internet, and providing intelligent usage advice will help keep our younger generations safe.

The focus of 2010's NCSAM is that cyber security is not the responsibility of any single person or organization. It is the responsibility of everyone who uses the Internet. It is a shared resource, and keeping it safe is our shared responsibility.

DEVICE-BASED SECURITY MEASURES

The absolute minimum

There are three basic protections [2] every computer user needs to enforce if he or she will ever be on the Internet. The first is a firewall. A firewall helps prevent hackers from gaining access to computers and keeps them from forwarding personal information without the owner's permission. PCs with Windows XP or later and Macs with OS X have built in firewalls that may need to be turned on. If a computer or hardware device does not come with a firewall, there are many firewall software options available - both free (i.e., ZoneAlarm or Online Armor) and for purchase (e.g., McAfee Internet Security).

Next is anti-virus software, which protects computers from viruses, trojan horses, and worms. Viruses, worms and trojan horses are programs written with intent to cause mischief on Internet-accessible devices at least, or to take over and completely obliterate systems at most. Any of these can be unknowingly downloaded from unsafe websites, or can be spread via email. An effective anti-virus program updates regularly, recognizes new bugs as well as old ones and repairs them. There are several competent anti-virus programs available, both free (i.e., AVG Free or Avira), and for purchase (i.e., McAfee, Norton, AVG).

The third basic protection stops spyware from establishing itself on computers or [cell phones](#) with Internet access. Spyware is aptly named as it can collect information about a user while he/she is surfing the Web. Anti-spyware software is frequently included with anti-virus software, but independent anti-spyware software is available, as well.

While it is possible to run multiple anti-spyware software packages, as different software looks for different things, it is never wise to run more than one firewall. One firewall is adequate; more than one can slow down a computer to a non-productive level.

Keep up with updates

Software is not static. It is always changing and improving. Operating systems change to address changes in the industry, and anti-virus and anti-spyware software update frequently for the same reason. It is essential that hardware users keep their software current. Many software packages offer the option to automatically update, which is a good option for most people. Software that doesn't automatically update does notify users in some manner, either by email or with a pop-up on software start up. These notifications should not be ignored for long. Keeping software current is paramount to keeping hardware safe.

Back up, back up, back up

The biggest mistake any hardware user can make is to ignore backing up their data. Software can be reinstalled; data lost is irreplaceable. We are in a digital age and a lot of our data is stored digitally – bank records, photos, letters, music. A recent NCSA/Symantec study showed that over 68% of Americans store more than 25% of their photos digitally, for example. [3] There are any number of ways data

can be lost. Accidental deletion is common. Device failure happens. Natural events, such as electrical or wind storms, fires, or floods can eradicate data. Cyber events such as viruses, spyware or other cyber attacks can remove data, as well.

Making a backup is a multi-step process:

1. Decide what files/folders/drives you wish to back up. Personal data is a definite, but there could be other data that's key to daily functioning that also needs to be stored.
2. Make copies of your chosen data. Many computer operating systems offer backup tools. A user could choose to back up just personal data; just data changed since last backup; entire systems; or just new data.
3. A backup has to be stored to some external device. Depending on the amount of data, a CD, DVD, flash drive or external hard drive could hold the backup. There are also Internet subscription backup services that effectively remove the extra layer of hardware (an external storage device). These third party Internet backup services also manage the next step in backup, which is
4. Safe storage of backed up data. Backed up data should be stored off-site. With an Internet backup service, that would be an offsite server. Keeping a backup with family or a trusted friend or neighbor is another option. The point is that a backup serves no purpose if it's in the same location as the computer. If the computer and the flash drive with backup data are in the same house, and something happens to that house (e.g. fire, theft, flooding), the backup will have served no purpose.

Passwords

Although the science of [password creation](#) may change – how long should it be; what characters can be included; how they should be stored – what doesn't change is the fact that there must be passwords.

Passwords are the most common means to authenticate that the person who is accessing a particular site or set of data is the correct person authorized to do so.

Most people select a password that is based on personal information and, therefore, easy to remember. That's good for hackers, too, because passwords based on personal information are easier to crack. [4] A mnemonic based on personal information offers a safer way to create a password. Include numbers and non-alphabetic characters, and an obscure, tough-to-crack but easy-to-remember password will be the result. For example, "Sundays are for watching Patriots football" could become "SafwPf." That's a little short for a password (the accepted minimum length has grown from 8 characters to 11 in the past two years), so change some letters to uppercase and put in a number and/or character or two. "Saf2WPf#," which is the above example with modifications, is now a much more secure password. Another option is to use a passphrase, instead of password, where the password length allows. "This pw is 4 My home PC," for example, is long enough, has a couple non-alphabetic characters and would be a challenge to crack.

A frequent concern is how often to change passwords. If a person thinks his or her password has been compromised on email or a VoIP (Voice over Internet Protocol) account like [Skype](#), for example, he/she should change passwords immediately. Otherwise, changing passwords every three months is sound advice [5], and not using the same password everywhere is more good advice. Parents should make this note for their children, too, as kids will make passwords as simple as possible and share with impunity. **"Don't share passwords" should be an adage for kids akin to "Don't speak to strangers."**

Keeping a list of passwords pinned to the wall next to the computer is not the best solution for keeping track. Yes, they should be in an easily

accessible place, but not such an obvious one. There are several options for secure tracking – handwritten in a notebook is great, if the notebook is then locked away. There are also software tools that will safely store passwords. With these, a user will only have to remember one password to gain access to all others. One suggestion is an open source, free software called KeePass. [6] Also, making a note on a calendar of when it's time to change passwords is a good way to remember to do it.

ON-LINE FRAUD PREVENTION

Secure and protected passwords are as important to online fraud prevention as they are to device-based security. Create unique and hard-to-crack passwords, keep them safe, and change them regularly.

Know Who You're Dealing With

Whether it's opening email, setting up a user account for a social networking or gaming site, or creating an account for [online shopping](#), know who you're dealing with. If an email is from someone unknown, delete it, especially if it includes an attachment. Attachments are where viruses and spyware live. Opening an attachment from an unknown sender is akin to opening a ticking box with no return address. It's just not wise.

As far as providing personal information online, a request for personal information is not a demand. Read the site's privacy policy to see how personal information will be used, if there is any doubt. The more personal the information, e.g., social security number, the more skeptical a user should be. [7]

Use care while surfing, whether on a computer or a smart phone or another Internet-accessible device. Anti-virus and anti-spyware software frequently include a web safety portion. While doing a web search, check for anti-virus approval on a site before accessing it.

Sketchy sites could be the source of innumerable problems, such as random downloads of viruses or malware. If the anti-virus software questions it, the user should, too.

Underage web users should be taught these lessons, as well.

Phishing

Phishing is a devious means of identity theft. A common phishing scam may involve an institution you know and trust, like your bank or PayPal, sending an email that requests account information and frequently includes urgent overtones. Except it isn't that institution; it's a phishing scam undercover. [8] Another common scam may be an [email](#) announcing a big lottery win. A real prize, monetary or material, never requires money to collect. Delete any email that asks for money in return for a prize. Yet another phishing scam is called 'rogue' software. It installs itself on your computer and then pops up a window on your monitor that says your computer has serious problems and immediate action is required to deal with them. The software will then ask for money to fix the problem. Remember, your own anti-virus or anti-spyware software will never ask for money to resolve a problem.

Always be skeptical. If you have doubts, don't respond to an email or a pop-up asking for personal information. Any trusted vendor will not ask for personal information via email or a scare-tactic pop-up. In the interest of shared responsibility for Internet safety, anyone suspecting a phishing scam should [report it](#) immediately.

Online Shopping

First, shop only on trusted, [legitimate sites](#). If you are not 100% sure of a [shopping site's validity](#), check for other shoppers' opinions via sites like [epinions.com](#) or [BizRate](#). Look for seals of approval from organizations like the BBB or TrustE. Check for secure URLs on the

web page that collects payment data. That means the web address starts with https, instead of http. The “s” stands for “secure.” Valid, rule-abiding online stores take this step to protect customer data. [9]

PERSONAL INFORMATION PROTECTION

Know Who You’re Dealing With

Whenever you provide personal information online, be certain of who is on the receiving end. Identity theft is no joke, and every piece of information carelessly given out makes the thief’s work that much easier. Passwords, bank account numbers, social security numbers should never be shared via email, and extremely cautiously via web sites.

Children and new users to the Internet, in particular, need to be guided about information sharing. One cannot communicate too much on this subject with new or young users.

Data Sharing and Social Networking

Social networking has grown incredibly in recent years. There are many social networking sites into which a user can link. Social networking sites are huge with kids and young adults, and there are sound ways to keep in touch with friends and family while maintaining safety for all. Here are some useful tips to keep you and your loved ones safe on a social networking site:

- Don’t post the exact details of your whereabouts before the fact. Announcing the exact dates of a two-week vacation; reporting when and where a child goes to and leaves school; saying anything that tells strangers too much about your location or your kids’ locations should be avoided.
- If you choose to upload pix to a social networking site via a smart

phone, [turn off geotagging](#).

- Monitor kids’ networked friends. Be sure they understand that they should not accept invitations from people they don’t know.
- Do not include [too many personal details](#). Birth month and day is adequate, for example, especially for information about children, but the same applies to adults, too.
- Use avatars or pet pictures for kids on social networking sites.
- Understand that [Skype](#) and other VoIP software can share too much information, too. Share information judiciously.
- Think before posting anything – pictures, facts or opinions. Privacy is a relative term on a social networking site, and things travel quickly on the Internet.
- Set and maintain your security settings. Do not assume that the site’s default settings are the best for you.

RESOURCES

Internet security is an ever evolving process. There are several valuable online sources where you can find additional learning materials about cyber security.

The National Cyber Security Alliance’s website is a great source. There are posters and lesson materials for both K-12 and for higher education. Classroom educators can find these materials at: <http://www.staysafeonline.org/>.

Microsoft, a partner in National Cyber Security Awareness Month, has a website dedicated to online safety. PC users will find Windows specific tips for Fraud Prevention and Data Protection, specifically, and other useful advice for Internet safety on this site. <http://www.microsoft.com/protect/default.aspx>

The United States Computer Emergency Readiness Team's website keeps current with alerts and tips to deal with online threats. One can sign up to receive these via email, or visit the site directly to keep current. <http://www.us-cert.gov/index.html>

Parents looking to learn how to keep their children safe online can find resources, tips, and tools on the following sites:

<http://www.ikeepsafe.org/>

<http://getnetwise.org/>

<http://www.connectsafely.org/>

Lastly, visit the blog at Safety Web often for up to date information about identifying and dealing with the latest Internet security issues. There are resource lists for parents, as well. <http://blog.safetyweb.com/>

REFERENCES

1. Stop. Think. Connect: National Cyber Security Month
<http://www.microsoft.com/protect/promotions/us/cybersecurity.aspx>
2. Core Protections. NCSA.
<http://www.staysafeonline.org/in-the-home/security-suite>
3. Back up important files. NCSA.
<http://www.staysafeonline.org/tools-resources/back-important-files>
4. Choosing and Protecting Passwords. National Cyber Alert System Cyber Security Tip ST04-002.
<http://www.us-cert.gov/cas/tips/ST04-002.html>
5. How Often Should I Change My Password?, WiseGeek.com
<http://www.wisegeek.com/how-often-should-i-change-my-password.htm>
6. Geek to Live: Securely track your passwords. Gina Trapani. LifeHacker.com
<http://lifelhacker.com/184774/geek-to-live--securely-track-your-passwords>
7. Protecting Personal Information. Staysafeonline.org
<http://www.staysafeonline.org/in-the-home/social-networking-0>
8. How to reduce the risk of online theft. Microsoft.com.
<http://www.microsoft.com/protect/fraud/phishing/reduce.aspx>
9. How to shop online more safely. Microsoft.com.
http://www.microsoft.com/protect/fraud/finances/shopping_us.aspx