12 tips to protect your electronic information

Information security is one of the biggest challenges facing healthcare companies and practitioners. With the ubiquity of technology, today's healthcare practitioner uses at least one computer device (PDA, mobile phone, laptop, notebook or netbook) in his/her daily routine. Most work with several devices and programs, transferring information from one program to another, often with questionable security provisions.

But alongside the solid productivity gains spawned by technology, are cyber predators who actively engaged in stealing valuable information, using malware (including various forms of viruses, worms, trojans) as the tool of choice. The consequences of becoming a victim can be devastating. In addition to hefty fines mandated by PHIPA, a publicized breach of information can have severe costs for employees, employers and consultants.

Don't become the next victim. Prevention is the best practice, especially in small to mid-size companies without dedicated technology and security support. Healthcare companies and practitioners would be prudent to consider a review of their information security systems. Here are two inexpensive suggestions you can start with:

I. Invest in a secure Case and Practice Management Software, with built-in encryption technology.
II. Implement a good security policy or security routine. Here are a few good policies and practices you can start with immediately.

1. Use a current operating system

Keep your computer operating system up-to-date.

First, your operating system should be one that is currently supported by the software vendor.

Windows 2000 software may be very good but is long discontinued by Microsoft. Current Microsoft operating systems include XP, Vista, Windows 7 and Windows 8. Microsoft will no longer support its XP operating system after April 8, 2014. You should plan to replace your XP operating systems with Windows 7 or 8.

Second, keep your computer operating system up-to-date. Free updates released by software vendors, close security loopholes, and keep you abreast with technology, among other things. There is an automatic update setting that, if turned on, allows your computer to download and update all critical updates

Support for Windows XP ends on April 8, 2014. If you're running this version of Windows after support ends, you won't get security updates for Windows

from Microsoft (which accounts for more than 85% of all personal computers).
Click this link to setup your automatic updates.

2. Use a standard user account

Use a standard user account to protect your computer from malware.

Administrative privileges are only required to change computer settings or install a new program.
Yet, most people use an administrator account for day-to-day operation, which makes their computer more vulnerable.

A standard account will not allow anyone or malware to install software or change the security settings on your computer. There is one downside however - you need to enter your administrative password when making a legitimate change to your system. Microsoft's Help and How-to site provides more information about the benefits of using a standard user account (in Vista, Windows 7 and Windows 8).

Newer versions of Windows have a User Account Control (UAC) feature that gives you additional control by seeking your permission whenever a program is about to make a change to your system. Set UAC to get your express permission before each change to your system.

3. Always password protect your computer

Use a password to protect your computer and storage devices against unauthorized access. Use a two-level authentication. Change your password once or twice every year or if you believe it has been compromised.

It is commonplace to see computers with no passwords or poorly constructed passwords, such as a person or company name. Research has shown that most users use the same password for many different accounts (computer, client access, Facebook, Twitter, etc.). A breach of one, breaches all.

We see passwords written on stickers at the front counter!!

Create a strong password by using a combination of numbers, letters and other keyboard characters. Use one password to access your computer and a different password to access your client program, preferable a password not used elsewhere.

In some clinics 5 or more therapists share the same PMS password

Many healthcare organizations encourage password sharing as a way to reduce their IT licenses and costs. This is poor practice that negates accountability and transparency. With each sharing, a password becomes more vulnerable. Each healthcare employee should have his/her own secure and confidential login credentials, for which he/she can be held accountable.

Keep your password secret; do not share it with anyone, especially colleagues or support personnel

4. A good antivirus is mandatory

A good antivirus program is mandatory to protect your computer against most common malware threats such as viruses, worms, trojan horses, etc..

There are many antivirus programs available, ranging from free to costly. Microsoft Essentials is free and provides real-time malware protection for your

Windows 7 and XP systems. Windows 8™ comes with Microsoft Defender to protect you from malware. Both programs offer several options:

- Real-time scanning will scan all files for known viruses before it accesses your computer. Keep this feature turned on.
- Update your virus program and scan regularly. In addition, perform a full manual scan once a month, as viruses can sneak through your defenses. This aim, after all, is one of their specialties.

Set a quick scan for every Sunday and a full system scan once every month.

Do remember that having the best antivirus software installed is not a panacea for keeping viruses out of your computer. An antivirus can only be developed after a virus has been found. Thus, new viruses can roam freely for some time. Be prudent!

5. Always use a good firewall

Like an antivirus program, a firewall is mandatory for anyone connecting to the internet or other networks. Always keep your firewall turned on.

Your computer has several ports which allows it to access the internet or local network services. A firewall closes unused ports and restricts use of others; it prevents unwanted communication with other computers on the internet or network or access to your computer.

If you are using a web-based software, a firewall may interrupt your connection. Do check with your software provider.

6. Protect your computer at all times

Protect your computer, desktop or laptop, from being stolen.

Failure to do so is not only costly but you stand to lose valuable data and weeks, if not months, of work. As a custodian of medical information, protection of your computer and data devices should be the first security rule in your organization. When in public places (airports, conferences, coffee shops), treat your computer like cash. Protect it at all times.

At the University of Toronto, six of us took a lunch break leaving our laptops in a room we considered secure only to return 50 minutes later to find 3 laptops missing.

7. Remove data from your old computer

Securely remove the data from hard drives and other storage devices you don't use. This practice reduces the exposure of your data.

How did you remove the information from your old system that you threw out or donated? You may be surprised to know that a simple delete does not remove your data. Deleted data can be restored and accessed again with dire consequences. Here is a link to a great article on safely removing data from your hard drive.

8. Be cautious with internet downloads

Use a trusted source whenever you download information, files or programs from the internet.
Computer predators will exploit the weaknesses of browsers and place malware on your computer, without your knowledge. Today's sophisticated malware can be embedded in file or a document such as a PDF file. These malware can damage your operating system, generate annoying pop-up ads, waste

your computer resources, track your internet usage and may even send personal information back to the predator. If you are a regular web user, running an anti-spyware is an excellent option. Spybot Search and Destroy is a free anti-spyware that does a great job.

9. Emails can be dangerous

Email attachments remain the most favoured tool used to propagate malware. You may receive an infected file or be invited to click on an email link that takes you to a site loaded with malware.

Follow these simple rules to avoid virus dissemination through emails.

- Be wary of email attachments from companies or unknown persons. If you wish to open an email, a safe approach is to right-click on the attachment, choose the download files option and scan the file using your anti-virus program.
- Delete chain emails as fast as you can. Worms (similar to ILOVEYOU or Melissa) use e-mail to carry their damaging payloads.
- Avoid clicking on links in an email from unfamiliar persons or sites. You can also turn on the *Plain Text* setting in your email. This option blocks the HTML beacons used by predators. However, this option may not be practical, as an increasing number of legitimate companies use enriched features of email as part of their marketing effort.

A good rule: Avoid downloading emails from people or companies you don't recognize.

10. Encrypt and secure your backups and flash drives

As a rule of thumb, your data should be encrypted at all times, even when it is stored on your own computer at the office or home. Unencrypted data has the potential for exposure and breach of PHI compliance.

So you perform a daily backup of your data. But is your backup password protected? Is it physically protected? Is it stored in the same location as your original data? Is your backup data encrypted? These are great questions to ask. Here are three simple rules to follow:

Backup rule 1: Keep your backup data password protected in a secure location away from your business premises or home.

Backup rule 2: All PHI data should be encrypted. Encryption is a great second level protection that prevents unauthorized access to your data.

Backup rule 3: Remove all unused data on your storage devices (if you don't need it, delete it). If it's an old hard drive, follow rule #7.

A colleague did his backup diligently and locked it in a safe in his office. Despite his efforts, he lost both his original and backup data to a fire.

11. Avoid public computers

Avoid using public computers to access your business network, PMS or CMS software.

A public computer (and these include computers in hotels, airports, conferences centres, etc.) can be used by predators to collect confidential information. A key logger (a program that records all your key-strokes) can be used to record your personal information. See Microsoft Safety Tips for using a public computer. Entering sensitive information should be done from your own or a trusted computer. Even checking email, which is done by more than 75% of people, is suspect.

12. Avoid public Wi-Fi connections

Think twice about using public Wi-Fi to connect to your network at the office or elsewhere. A public Wi-Fi network is exactly what it says, public. With these networks, your privacy is akin to making a confidential phone call while surrounded by strangers, except you don't know who is eavesdropping. Since many people share public networks, the risk of a hacker stealing your password or personal data is very high. If you do use a public wireless network, use only encrypted wireless networks and be sure to leave your firewall turned on. You should also avoid sending passwords through public networks.

Do not login to your neighbour's free internet connection. It may have a raison d'être. Free does not mean absolutely free!

Rogers provides a safe mobile internet connection for users on the go. *Rocket Mobile Internet Stick* comes with monthly plans starting from $22. Also most mobile plan will allow you to setup and connect to your own secure hotspot.

If you use a wireless connection, in the office or at home, encrypt it with a strong password.

In summary

Using a computer and the internet can be enormously rewarding and productive. At the same time, it can be costly and dangerous. Take the time to learn the rules and practice them diligently. You would not get a ticket for using an outdated antivirus or operating system, but worse you could lose your clients' data, and your job or business with it.

A few simple but important precautions with your computer and internet usage can prevent you from becoming the next innocent victim. Be Prudent!

About the Author

Danny Doobay has been a Business and IT consultant to industry and government for more than 25 years. He has held executive positions in both public and private sectors. He has also project managed software development, implementation and data migration.

He is currently the CEO of Baylaan Technologies, a software solutions developer based in Markham, Ontario. Baylaan develops both custom and packaged software solutions for several sectors, including Financial, Health, Educational and Government.

Danny Doobay, MBA, BA (Hons.)
Chief Executive Officer
Baylaan Technologies Inc.
Tel: 905-202-4716
Email: ddoobay@baylaan.com
http://www.baylaan.com/

Follow Danny on: