



## SECURITY BEST PRACTICES

The Internet and email offer unprecedented freedom to communicate, learn and entertain. On the flip side of this freedom lies the potential for your privacy and data to be compromised by malicious software, such as viruses and spyware, among other threats.

The good news is that there are many simple steps you can take to enhance the security of your notebook. By following the best practices outlined below, you can comfortably enjoy the benefits offered by the Internet and email, knowing that your privacy is well-protected.

In this brief, the following topics are covered:

- Internet
- Email
- Passwords
- Anti-Virus
- Firewall
- Anti-Spyware
- Security Updates

### INTERNET

#### WHO CAN I TRUST?

You should use your best judgement when spending time on the Internet and stick to visiting trusted sites. If you are browsing an unfamiliar web site, make sure it has a published privacy policy that you can review first. A good privacy policy will tell you how the site collects, uses, shares and protects any information you provide.

#### HOW CAN I PROTECT MY PERSONAL INFORMATION?

The best way to protect your personal information is to keep it to yourself. A good rule of thumb is to avoid sharing any information that you wouldn't want in the public domain, such as your name, address, financial information, family details, phone number, etc.

In addition to relying on common sense, there are several tools available that help protect your personal information. Here are some tips to help you.

#### I) MICROSOFT: SECURE WEB PAGES WITH INTERNET EXPLORER

The Microsoft Internet Explorer (IE) web browser helps protect your personal information by supporting standard security protocols, including: Secure Socket Layer (SSL), digital certificates and 128-bit encryption. These technologies work together to keep your data safe wherever the Internet takes you.



Further, there are server-side functions provided by the webpage host. These functions are not set locally in your browser but by the webpage hoster. Before you enter any personal information on a web page, you can quickly check to see if the page is secured by the webpage hoster. Look for the yellow lock icon in the bottom right corner of your browser window and ensure that the web address prefix includes an “s” (i.e. https).

Learn more about how IE keeps your data safe at <http://www.microsoft.com/windows/ie/using/articles/browsingsafety.mspx>.

### **II) MICROSOFT INTERNET EXPLORER: BROWSER SECURITY OPTIONS**

Most browsers offer built-in measures to increase the security of your browsing experience. For example, Microsoft Internet Explorer 6 lets you classify web sites as “Trusted” or “Restricted.”

### **III) MICROSOFT INTEREXPLORER: POPUPS AND BLOCKING**

Although many pop-ups are just a marketing tool designed to get your attention, they can also have a malicious intent: to install spyware, adware, viruses, etc. on your notebook, without your knowledge. Spyware and adware are umbrella terms that refer to programs that are secretly loaded onto your notebook in order to track your Internet activity or collect personal information.

To minimize the chance of spyware infecting your notebook, click only on pop-ups you can trust. When a pop-up does present itself in your browser, always use the “x” in the top right hand corner, or type the shortcut “Alt+F4,” to close it down safely.

Perhaps the best defence against pop-ups is to prevent them from appearing in the first place. By adjusting the settings in your browser (using the **Tools** menu item to do so) or third-party security application, you can block pop-ups from opening while you are browsing the Internet.

### **HELPFUL LINKS**

#### **Managing pop-ups with Norton Internet Security or AntiSpam**

[http://service1.symantec.com/SUPPORT/nip.nsf/bcb7bbe8a333053d8825705800827216/73ecaa0895e6e96e88256d900006ba39?OpenDocument&src=bar\\_sch\\_nam](http://service1.symantec.com/SUPPORT/nip.nsf/bcb7bbe8a333053d8825705800827216/73ecaa0895e6e96e88256d900006ba39?OpenDocument&src=bar_sch_nam)

#### **Managing pop-up ads with Microsoft Internet Explorer (SP2)**

<http://www.microsoft.com/windows/ie/using/howto/privacy/restrictedsites/stop-popups.mspx>



#### **IV) DOWNLOADING TIPS**

Downloading content off the Internet onto your notebook is a very convenient way to quickly access the programs and data that you are interested in. Unfortunately, some downloads can provide a direct route for security threats to infiltrate your notebook. One way to guard against unwanted threats is to download only from websites that you trust.

Even though the task can sometimes seem arduous, it is also very important to read licence agreements in their entirety before accepting the terms. This is the only way to be 100% certain that the content you are downloading is something you actually want on your notebook.

#### **HELPFUL INTERNET SECURITY LINKS**

##### **MICROSOFT**

<http://www.microsoft.com/windows/ie/using/securityandprivacy/default.aspx>

##### **GETNETWISE.ORG**

<http://privacy.getnetwise.org/browsing/>

#### **V) EMAIL**

Email is an efficient and cost-effective way to communicate with others. It's also another vehicle for malicious security threats to enter your notebook. By taking a few simple precautions, you can ensure that your email remains problem-free.

##### **I) SHOULD I BE CONCERNED ABOUT UNFAMILIAR OR UNEXPECTED EMAILS?**

If you have an email address, chances are you have spam. "Spam" is essentially electronic junk mail—unwanted communications that you didn't solicit. If you do receive an unfamiliar email, even if it is written in a familiar tone, you should delete it without opening or responding to it. These emails can contain hooks that capture your email address when you open them, transmitting it back to the spammer and essentially identifying your email as fair game for spam campaigns. It's also important to never open an attachment in an unfamiliar email. Doing so can infect your notebook with a virus which, in addition to compromising your notebook's performance and data, has the potential to spread to others in your email address book.

##### **II) SHOULD I BE CONCERNED ABOUT FRAUD OR PHISHING?**

Yes. Perpetrators of fraud will try to get you to disclose valuable personal information, such as credit card, bank account numbers, login accounts and passwords (e.g. E-Bay and Paypal accounts). One way of doing this is to send an email that appears to be from a trusted source.

Such a tactic is referred to as a "phishing attack." Phishing emails often appear to be credible or trustable sources because they include official-looking logos. Another tactic is to create a mirrored "spoof" site that borrows content from the legitimate that the phish email claims to represent.

For more information on email fraud, please visit: <http://www.microsoft.com/athome/security/email/phishing.aspx>.



### **III) HOW CAN I PREVENT FRAUD?**

Trust your instincts. If an email seems suspicious, it probably is. Perpetrators of fraud will often give you a limited timeframe to respond in an attempt to force you to react without thinking. Don't let a sense of urgency override your good sense. Do not follow links or click attachments in suspicious emails.

Here are some additional protective measures for protection against fraud:

- If the anti-virus program on your notebook doesn't already have a built-in spam filter, you can purchase and install a third party solution.
- Make sure to update your anti-spam program and scan your notebook regularly. You can pre-define an update schedule to ensure that you don't forget to do this.
- Set up a secondary email address to use when doing web transactions. This prevents potentially harmful spam from being sent to your primary email address.
- Pictures in email can secretly send a message back to the spammer, legitimizing your email address for future use. Many email programs enable you to stop pictures from downloading until you have had a chance to read the message they are attached to.
- Spam can also infiltrate instant messages. You can prevent these unwanted messages by setting up the spam filter in Windows Messenger or MSN Messenger.

#### **HELPFUL EMAIL SAFETY LINKS**

##### **MICROSOFT**

<http://www.microsoft.com/athome/security/email/default.mspx>

##### **GETNETWISE.ORG**

<http://privacy.getnetwise.org/communicating/>

### **IV) PASSWORDS**

Passwords help keep your internet account(s) and notebook computer safe by through access control. The best way to guard against unauthorised access is to implement a stringent password policy.

#### **PASSWORD CREATION TIPS**

- Do set up a system password that is required before your system can even boot up
- Do include a mix of alphabetic characters, numbers, upper- and lower-cases and punctuation
- Find ways to make your password memorable, i.e. you can remember a password by taking the first character of a common or funny sentence such as Mmild2C, which stands for "My mother-in-law drank 2 Cokes."
- Do remember to change your password frequently, at least every few months
- Don't choose a password with fewer than six characters
- Don't ever divulge your password to anyone



- Don't choose an intuitive or easily-obtained password, such as the name of someone close to you, your telephone number, login name or birth date
- Don't create a password that is made up exclusively of letters or numbers

#### **HELPFUL PASSWORD LINKS**

For more detailed information on email safety, please visit: [http://www.microsoft.com/smallbusiness/resources/technology/security/5\\_tips\\_for\\_top\\_notch\\_password\\_security.msp](http://www.microsoft.com/smallbusiness/resources/technology/security/5_tips_for_top_notch_password_security.msp)

#### **ANTI-VIRUS**

There are many dependable anti-virus programs on the market that can keep viruses, worms and Trojan horses from infecting your notebook. However, any anti-virus software is only as effective as its last update. That's because new viruses are created every day. To ensure your notebook has maximum coverage, make sure you have anti-virus software installed on your system. Then, check for updates and scan your system regularly.

The following are some popular anti-virus products on the market today:

- Norton Anti-Virus (Symantec): <http://www.symantecstore.com>
- McAfee Virus Scan: <http://us.mcafee.com>
- Trend Micro PC-cillin: <http://www.trendmicro.com>

#### **FIREWALL**

Computer firewall programs are similar to anti-virus programs in that they protect your system from various outside threats, such as hackers and malicious software (or "malware"). Firewall software prevents incoming attacks by blocking any unauthorised communications. Firewall software can also prevent unwanted outbound communications, such as undetected spyware attempting to send out data behind the scenes.

A firewall should be an integral component of any computer connected to a network or the Internet. Even if you have an anti-virus program installed on your notebook, you still need a firewall to ensure maximum protection.

**Toshiba Tip:** If you have Windows XP Service Pack 2 installed, you will find Windows Firewall in the Control Panel.

The following companies offer firewall products:

- MS-Firewall: <http://www.microsoft.com/athome/security/viruses/fwbenefits.msp>
- Norton Personal Firewall 2006 (Symantec): [http://service1.symantec.com/SUPPORT/nip.nsf/caa700f6e4d4255a8825705800827218/e8365b52a1facdaf88257060007d41a1?OpenDocument&src=bar\\_sch\\_nam](http://service1.symantec.com/SUPPORT/nip.nsf/caa700f6e4d4255a8825705800827218/e8365b52a1facdaf88257060007d41a1?OpenDocument&src=bar_sch_nam)
- McAfee personal firewallplus: <http://uk.mcafee.com>
- Trend Micro PC-cillin Internet Security: <http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>



## **ANTI-SPYWARE**

### **WHAT IS SPYWARE?**

Spyware refers to a collection of unwanted computer programs that are installed without your knowledge.

In some instances, this occurs via a process known as “back-door” consent. When installing software, many users click OK to accept a licence agreement, without having first read the terms and conditions. In some instances, this means that they may be agreeing to unwanted data exchange. Beware. Freeware Software is not always free: you may be installing Spyware along with the program. Read the license agreement carefully to make sure that you truly agree to accept all of the terms and conditions.

Spyware programs can perform a range of activities, from collecting personal information or data, to making your notebook exhibit annoying behaviour, such as repeatedly opening unwanted pop-ups. Often the first sign that you have unwanted spyware installed on your notebook is noticeably slower performance, as spyware requires system resources to perform its dastardly deeds.

### **HOW CAN I AVOID SPYWARE INFECTION?**

The best way to avoid the bothersome task of detecting and removing spyware from your notebook is to prevent it from getting there in the first place. This can be accomplished by installing an anti-spyware product. Most anti-virus software offers built-in anti-spyware functionality to prevent infection.

Other precautions you can take, include:

- Read the terms and conditions of software licensing agreements in detail
- Read all privacy agreements for websites, web forms and software
- Ensure your browser security settings are set to medium, or higher
- Follow safe Internet and email practices by only downloading, or opening attachments, from trusted sources
- Install a firewall on your notebook.

### **HOW CAN I REMOVE SPYWARE FROM MY NOTEBOOK?**

In the event that your notebook is infected with spyware, there are a variety of products you can leverage for effective removal. Current Toshiba notebooks come pre-loaded with Symantec Norton Internet Security, Anti-Spyware Edition. See this link for more information: <http://service1.symantec.com/SUPPORT/nip.nsf/docid/2005022315283436>

Below is a list of additional anti-spyware products:

- McAfee Security Center: <http://us.mcafee.com/root/product.asp?productid=msc>
- McAfee AntiSpyware: <http://us.mcafee.com/root/package.asp?pkgid=206&cid=16261>
- Trend Micro PC-Cillin Internet Security: <http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>
- Freeware Products: Microsoft Anti-Spyware, Ad-Aware, Spybot Search & Destroy.



### MICROSOFT UPDATES

One final important step to ensure maximum notebook security is to keep your Microsoft software updated. At different intervals, Microsoft releases bundles of the most up-to-date drivers, tools, security updates, patches and customer-requested product changes to their operating systems. These updates are delivered as “Service Packs”, and between Service Packs as MS Automatic Updates.

### AUTOMATIC UPDATES

With Windows XP Service Pack 2 (SP2) installed, you can benefit from the enhanced security that Microsoft provides by signing up to receive Automatic Updates.

With SP2 installed, you can go through the following steps to change and set your security settings, including choosing automatic updates: Click on **Start** and go to the **Control Panel**. Then open the **Security Center**.

With Automatic Updates enabled, updates are automatically installed on your notebook. If you prefer to be more involved in the update process, you can choose to have the updates downloaded to your computer, with notification for you to finish the installation at your convenience.

### SECURITY UPDATES

Microsoft is active in securing the Windows XP Operating System. On a “need-be” basis, Microsoft offers Critical Updates to address severe security leaks or issues. At minimum, one should ensure that all Microsoft Critical Updates are installed. Otherwise your notebook will be unsecure or runs the risk of becoming infected with a virus when you go online.

More information on Microsoft Automatic Updates is available at: <http://www.microsoft.com/athome/security/update/bulletins/automaticupdates.msp>.