Protecting your Identity web and personal

By P. Hopkins

The first port of call is your windows operating system, and what's installed, and what should be installed. This should be a decent firewall and Anti virus software. This software should include a pop-up blocker, but if not the Google tool bar has one and IE8 upwards and Firefox have settings you can configure for pop-up blocking.

Pop-ups whilst on the internet, that is... If your getting pop-ups on your computer about security alerts, asking you to install a tool or go to a site to get one (even when web browsers not running) then you are most likely infected with mal ware or a virus meaning your identity and security is already at risk.

Installing good security software

There are so many security programs out there, what with Anti virus and mal ware and key loggers and malicious websites. So good protection starts with having the following applications installed.

Firewall

Most people are aware of what computer firewall's are, but many are not. Firewall's hide your computer software ports used by the system to network. They also keep track of network permissions for programs that are allowed or denied by you. Make sure you have a good firewall installed which monitors internet traffic in/out and program permissions for internet and network access.

Commodo is a good firewall with Anti virus as optional, which also allows you to run programs in sand-box mode isolating them from the system until proven safe. But if you have spyBot you may have to remove it as they clash with each other without a more complex approach to their configuration.

Online Armor is another good firewall with comprehensive protection for the internet connection and program permissions. This runs fine along side SpyBot if installed.

Avast anti virus and firewall all in one has come a long way, representing some very comprehensive protection with good detection results, and very easy to use. ZoneAlarm and AVG are also good all round protection for the computer.

Anti-Virus software

This is very important as Trojans can install key-loggers to monitor your key presses, and now the most common way of identity theft. Redirecting your web browser to malicious websites is another popular malicious trend. You can get infected just by visiting a rouge website.

Anti Virus authors all offer free and paid versions, the difference is usually less updates and some disabled proactive defence like background scanning. Its best to go paid protection on a system of high internet usage.

Avg is also a popular free and paid Anti-virus software suite, but Trojans have been known to disable the free version. It's easy to use and has a good browser tool bar plug in that checks website url's for known malicious activities.

Full blown Paid-for commercial packages

These days the fight for supreme protector is between Kasperskay Nortons 2010 upwards and BitDefender. Avast has also become a comprehensive package. The thing is, they all change each year when they tinker with what they've got and improve on it. So it's best to check some independent security sites for reports on who's in the lead for the current year.

Extra security tools

Key-loggers are nasty, when it comes to collection of private information, so surely the best form of defence is prevention. KeyScrambler is a free or paid tool, and scrambles the key strokes before a key logger can record them. So if one gets on your system, all it gets is Mickey Mouse talk and no real personal data. It runs as a web browser plug in so when you're on the bank site or social sites your key strokes are safe.

PeerGuardian from phenix-Labs monitors what web gates and internet routers your computer uses to send and receive data across the internet. It protects your data path from known routers and gateways that record their traffic movement.

The last port of call is you, and how you should conduct yourself on the internet. It's often refereed to, as having Netiket or being net-wise.

The Way you conduct yourself on the internet is also key to staying safe. We've covered some of the following rules in our NetWise article, but here's a quick re-cap.

Be vigilant with e-mails and don't go to a web site just because they say it's good.
If an e-mail states as such, then research the web site or resource on Google first.

Be careful on social sites like facebook, not to give too much away concerning identity.
Always check the privacy policies in their terms and conditions to make sure you're not authorizing them to pass it on to 3rd party bodies. Always check your account settings and limit what you show to those outside your friends list. If the social site has apps and plug-ins for your user page, research them first, especially facebook apps and plug ins as authors aren't always good with your data.

When going to your banking web site, NEVER use the drop list to select the sites address or your history. Click in the address bar and type it in. Trojans can inject false history into your browser configuration files, sending you to copy-cat web sites when you select a site from history panel or address bar.

It's a good idea to familiarize yourself with the banks website address so you can check its right in the address bar if using browser history links.

Buy a good paper shredder and use it. If you can't afford one then all that you rip up, spread over two bin bags and dispose of them on different weeks.

If you buy with credit card allot over the internet then set a low credit limit within your spending. This way the card should never have much available credit on it for offenders to spend with. Register the card with Pay Pal and use Pay pal on any sites that accept it, this way your card details remain hidden.

NEVER use your credit card on web sites that are not using secure payments. You can tell by the web browsers address bar, it should start with **http's://** and not just 'http'. If it isn't when you reach the payment section, then don't use it, as your card details can be seen by others in between the connection.

If you're using fire fox then check bottom right of browser for a pad-lock icon and click it, to view the sites security and authenticity certificate. On IE the padlock's at the end of the address bar and again you click it for security information. On Google chrome the padlocks at the start of the address bar at the top.

Final words

Always try and research an issue on Google first if you're not sure about something you've received or want to do. Never trust so-say quick money making schemes THEY DON'T EXCIST! it will always involve hard work if genuine. If an email is asking for a password it's bogus. If an email claims to be facebook admin or your banks administration either check their website for any related info or call them first to authenticate the request, 9/10 times its bogus.

Don't be too trusting, be vigilant in your mind's eye on security and if you haven't already, go through our security related articles and tutorials and get yourself clued up.

Join computer magazine forums like **PCmag** or **PCformat** or **WebUser**. These sites belong to Magazine companies, but the forums are full of experts that will answer your questions, and there's many free articles on security and stability.