BIZCOMMUNITY

Be proactive in your online safety

By Carolyn Holgate

4 Apr 2013

The internet is a part of our daily lives; we use it for everything - communication, reading, research, education, current events, exploring the world, entertainment, shopping, networking and business.

The internet gives us magical access to everything at the press of a button, yet it also gives strangers access to us.

By acting responsibly and taking proactive steps, you can ensure that you are protected from phishing attacks and malware. MWEB provides information and suggestions on how you can protect yourself while not giving up any of your internet freedom.

What is phishing?

Phishing is a scam designed to steal valuable personal data, such as login details, PIN numbers, passwords or credit card details.

Scammers set up fake websites that look exactly like trusted banks or business sites where you might store credit card details. They then randomly send out millions of e-mails that appear to be coming from the trusted site, asking users to come and update their information. If a user enters any sensitive details, the scammers can use these details to access their online bank accounts, make fraudulent purchases on their credit cards, or use the stolen data in other illegal ways.

How do I protect myself?

You should be suspicious of unexpected emails that appear to be from trusted sites, asking you to follow a link and confirm your details. If you think it may be legitimate; rather than following the link, log in to the site as you normally would and see if there are any notices similar to what was mentioned in the email.

Most browsers such as Internet Explorer 7, Firefox 2 and Opera 9 have anti-phishing features built-in which will check the sites you visit against a constantly updated list of known phishing sites and warn you if you are accessing one. Check your browser's Help to learn how to enable this feature. If you receive what you suspect is a phishing e-mail, report it as 'spam' to your service provider.

What is Malware?

Malware, or malicious software, is a term for a number of different types of programmes designed to break into or damage your computer.

There are many kinds of malware, many with names you might recognise:

• Viruses are designed to duplicate by "infecting" other programmes with copies of itself. They are most commonly transferred through infected programmes sent via e-mail or built into pirated software.

• Worms infect PCs over networks, without the need for a user to run an infected file. The danger of a worm is that they can slow down or even incapacitate an entire network, as more and more infected computers repeatedly send out thousands of copies of it. Some install "backdoors" that allow hackers to take control of infected PCs.

• Trojans are malicious software that appears to be useful or entertaining, but will do some form of damage when run. For instance, a Trojan may install a virus or a "backdoor" programme to allow hackers access to the computer it is run on.

• Spyware spies on you - and sends personal information, such as your credit card details or passwords, to its creators without your knowledge or consent. It can also slow down your computer and use up your bandwidth.

How do I protect myself?

Malware is also often sent via e-mail, so you should follow the same precautions as proposed above, in addition to running virus scans on all attachments.

Make sure you purchase reputable software; don't use pirated copies, even from your friends. Pirated software can make your PC more vulnerable to attacks by viruses and malware.

With licensed software you'll get after sales support should you need it, as well as benefiting from automatic software updates.

Many routers have a built-in firewall to protect from hackers and malware, however, if you use a normal ADSL modem you should install a firewall, or activate the existing Windows Firewall on your machine.

You can also purchase special Internet Security software to protect your PC from attacks, should you come into contact with malware. Try known, affordable products such as AVG, which will recognise and remove common malware; as well as providing an up-to-date virus scanner you can run yourself.

ABOUT CAROLYN HOLGATE

Carolyn Holgate is a part-time tech guru and general manager at leading internet service provider MWEB. She is responsible for the strategic focus of the consumer division that offers Internet access to the consumer and SOHO/SME markets. Follow @MWEBGuy on Twitter.

- Be proactive in your online safety - 4 Apr 2013
- Taking your small business social - 25 Feb 2013
- Demystifying the cloud - 5 Nov 2012
- Be a start-up success story! - 18 Oct 2012

View my profile and articles...