Protecting Your Computer: Part 1 - Common Sense

January 9 2006

by Philip Dunn
Believe it or not, the most important defense for your computer is not an anti-virus program or a firewall, but your own brain. The way you use your computer determines how secure it is.

Web browsing on the Internet and email can be a dangerous, but thinking before you click can save you a world of hurt. Here are some tips to help you keep the hackers at bay.

Do not give out your principal email to everyone. Get a free web mail address for times when you need to give an email to access pages or open accounts. I recommend having three different email addresses. Use

one for family members only. Never give out this address to anyone and tell family members to do likewise.

Use another email for important mail, Paypal, work related stuff and good friends. Again, give out this address with caution. Avoid forwarding jokes, trivia and other junk mail to your friends. Tell them not to send junk to you, as well.

Set up a third account to type into web pages to read articles, get information from vendors and to receive junk mail. Use this account to forward witty jokes, questionable photos and mass mailings. This account can be cancelled when it gets overloaded with Spam or unwanted mail.

Why is all this necessary, you might well ask? Because your email is like your street address, but much more accessible. Once your email address makes it into a hacker's computer, he can attack your account at will, sending you all kinds of dangerous virus-ridden mail and annoying ads for things like Viagra and porn. Your only permanent escape from this, despite spam filters, is closing the account.

Web mail accounts have another advantage in that the mail stays on a remote server. It does not require downloading – you read it online. Good web mail providers scan all email giving you an added layer of protection. You can also read web mail from any computer making it handy when traveling.

Popular and reliable free web mail hosts are Google (Gmail) and Yahoo!(Yahoo! Mail). If you like a good, quick free web email account with no frills, try Fastmail (www.fastmail.fm).

When signing up for these accounts, they will invariably ask you all kinds of questions. Be smart and lie – yes, you heard me: Lie. Use any

information but your own. Why? Because they often sell this information to 3rd parties who then bombard you with junk mail, phone calls and Spam. If you cannot tell a lie, stick to regular email accounts.

As a matter of fact, lie on just about every web page that asks you for personal information. If they ask for an email account to verify, use your throw-away web mail account, not your principal account. Do the same when registering software.

Pornography is the single largest user of bandwidth on the Internet. Despite protests to the contrary, almost everyone looks at porn on the Internet. This is where people make their biggest mistakes. They can quickly end up with a virus ridden computer, get hundreds of nude pics every day in their email and have XXX pages popping up whenever they go online.

If you must look, do so safely. Set your browsers security level to high and do not allow pop-up windows. When asked if you wish to run ActiveX controls, click no.

Never, under any circumstances, download and install software from these sites no matter how enticing it may seem. These programs will take over your computer and your anti-virus program will not detect them. Always click no when offered the option to download any software from these sites.

Sometimes these porn sites will ask you if you would like to make them your home page. Don't do it unless you enjoy your boss/significant other/children seeing what you've been up to.

Never give your email address to a porn site.

File sharing is completely legal as long as you only share legal content.

However, it's often impossible to tell weather it's legal or not. Best bet; don't do it. Many file sharing programs come with loads of spyware – more on spyware later. Besides that, they can allow other users to see important files on your hard drive.

File sharing has been used to pass viruses, illegally copied music, pirated software and even child porn. Be extremely careful with what you download. Popular and relatively safe file sharing programs include Shareza, Limewire and EMule.

Spyware is software you inadvertently install when installing some other program. Spyware reports your online activities to a third party when you are connected to the Internet. Avoid spyware by paying careful attention when installing software and avoiding pirated programs and "free" utilities. Always look the program up on Google first before installing. If it has spyware, somebody has detected it.

Don't let other people use your computer or supervise their activity. They may not have read this article or decide to install "cool screen savers" or other virus ridden programs.

Be wary of using your credit card online. One good strategy is to have a credit card with a low limit just for online purchases. Never type your credit card number into a web page that is not secure – in should show a small lock in the bottom right side of your browser. Don't keep credit card numbers on your computer, either.

Flow these simple tips and remember: nothing is for free, if it sounds too good to be true, it is and will probably end up infecting your computer.

[Protecting Your Computer: Part 2 - Firewalls]

Copyright 2005 PhysOrg.com

Citation: Protecting Your Computer: Part 1 - Common Sense (2006, January 9) retrieved 18 September 2024 from https://phys.org/news/2006-01-common.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.