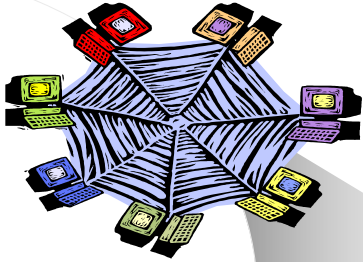


Home Computer Security

By: Cory Chrisinger
& Kevin Brinnehl



Topics

- Security
- Home Networking
- Wireless Networking
- Spyware
- Virus Protection
- Email Security
- Questions?



Security

- It is recommended that you use a firewall
- A Router Wired or Wireless is a Firewall
- Network Address Translation
- Windows XP Service Pack II Firewall Services
- Zone Alarm – Free

Networking Hardware

Routers

Wireless Access Points

Linksys WRT54G

Wireless NICs

<http://www.practicallynetworked.com/>

Wireless Networks

Wireless Encryption

WEP -- *Wired Equivalent Privacy*

WPA-PSK -- *Wi-Fi Protected Access*

Windows XP SP2 W/ Firewall

Free Firewalls – ZoneAlarm

Spyware

Free Software

- Adaware
- SpyBot
- Microsoft Defender

Spyware scan minimum once per month

Avoidance???

Virus Protection

- This is by far the most important piece of software you will install on your computer.
- We can not emphasize the above point enough. Without virus protection your computer is exposed to threats via email, web browsing, and in some cases by just having your computer on.

What type of virus software should I use?

- For all faculty and staff employed by UW Colleges, we have provided McAfee Anti-Virus software free of charge (<http://www.uwc.edu/downloads/mcafee>). We recommend taking advantage of this service because: 1) It's free, 2) You can get free support from McAfee, 3) It is utilized throughout the colleges so you may be able to get limited support from your peers.

Other Virus Scanners

- Symantec's Norton: <http://www.symantec.com>
- Trend Micro: <http://www.trendmicro.com>
- AVG: http://www.download.com/AVG-Anti-Virus-Free-Edition/3003-2239_4-10503939.html?tag=lst-0-2 (although there is a commercial version, this link is to the free personal edition). This is a great tool for students or anyone else who doesn't want to buy a yearly subscription from the other companies.

What Should I Do Once the Virus Software is Installed?

- Most of the newer corporate editions make configuration of the software very easy.
- At the least, you should scan your machine for viruses at least once a month.
- More importantly, you should ensure that your software is downloading virus software updates on a daily basis.
- If your program prompts you for an action, make sure that you read the text carefully and choose the appropriate option.

Email Security

- This is probably the number one growing threat for home computer use.
- There are really three different types of malicious email: SPAM, PHISHING, and virus attachments.
- SPAM can be classified as annoying but presents no immediate harm. An example of this would be a Viagra advertisement.
- PHISHING is much more invasive. A phishing email attempt to lure you to a website and provide personal information about yourself or your accounts. This has the potential to be devastating as it can lead to identity theft.

SPAM Management

- We'll begin with the less intrusive problem.
- There are a variety of commercial software products that focus on SPAM management. As with the virus software, these products are usually based on a yearly subscription.
 - McAfee: <http://www.mcafee.com>
 - Norton: <http://www.symantec.com>
 - I Hate Spam: <http://www.sunbelt-software.com/iHateSpam.cfm>
 - There is one free solution that we've seen fairly good results with and that will work with Outlook (but not Outlook Express): <http://spambayes.sourceforge.net/>

How to Protect Against Phishing

- Honestly, this is a tricky one to explain in full detail. The reason is that phishing attacks come in many different forms and you need to have a fairly good knowledgebase to identify if the email is legitimate or not.
- However, there are steps you can take to protect yourself.

How to Recognize Phishing Attempts

- The number one rule is that no legitimate business will send you an email telling you that your password has expired and you need to login to change it, or that you need to type in your credit card number, or to go to a website and provide your SSN. These are telltale signs that someone is up to no good. If you are worried that something might be legitimate then we recommend that you contact the business and ask them directly.
- Another telltale sign of a phishing attempt is grammatical and spelling mistakes in an email. The more mistakes, the greater the chance the email is not legitimate.

Don't Click on That Link!

- Don't click on any hyperlinks in emails.
- This may seem rather intrusive but it is the safest option available to you.
- Nearly all phishing attempts present you with a legitimate looking email that "redirects" to you a different server that attempts to collect your private information.
- If you don't click on the link, then you can't be redirected to the malicious website.

Don't Click on That Link! (cont.)

- Say, for example, you get an email from your bank asking you to login. Instead of clicking on the link, open up your web browser and go to your bank's website directory.
- Now, not every hyperlink is meant to cause you trouble. Emails from companies like Evites provide you with a link to click on that is perfectly safe.
- Use your best judgment that errors on the side of caution. If it looks like a duck, smells like a duck, and quacks like a duck then...you know the rest. Except that ducks aren't generally trying to steal your credit card number.

Software Solutions to Help Protect Against Phishing

- Unfortunately the industry has been a bit lagging in producing quality anti-phishing tools to date. We've tested a number of them and they all have problems to varying degrees.
- However, the good news is that most anti-spam software classifies phishing as SPAM, which will help protect you.
- The latest update for Office 2003 provide some phishing protection by utilizing the built-in junk email filter, which is the SPAM solution provide with Office 2003. If you use Office 2003 you can visit <http://officeupdate.microsoft.com> to obtain the latest update for your software.

Virus Attachments

- This was actually the first problem most people encountered as email became more widely used. Most of you have probably already seen examples of this throughout the years.
- Generally, the email tells you to open this very cool movie, or really funny joke, or really awesome game....

Example

- This is one of my personal favorites, mostly because I'm supposed to have sent it out.
- Needless to say, we did not send this out, your computer is not infected, and the sky is not falling. Without an anti-virus program, opening the link would most likely lead to an infection.

```
-----Original Message-----
From: Antivirus [mailto:Antivirus@practicalnetworked.com]
Date: Monday, April 03, 2006 12:17 PM
To:
Subject: Re:
Dear user of practicalnetworked.com,
We have received reports that your system has been used to send a large amount of spam messages during the last week.
Therefore, your computer has compromised and now contains a trojan virus.
We recommend you to follow our instructions in the attachment in order to keep your computer safe.
Best regards,
The anti-virus team.
```

How to Protect Yourself

- Anti-Virus, anti-virus, anti-virus.
- If you have an anti-virus software package installed you've taken the first step to protect yourself against this attack.
- Even more importantly than anti-virus, don't open attachments that look suspicious.
- Again, be on the lookout for spelling and grammatical errors. These generally are warning signs.
- If in doubt, email the person that you got the attachment from and ask them if they sent it.

Questions ??

Home Security Links
<http://www.practicalnetworked.com/> -- Home Networking Tips
<http://www.linksys.com> -- Hardware
<http://www.zonealarm.com/> -- Free Firewall
<http://www.lavasoft.com/> -- AdAware
<http://www.spybot.com/> -- Spybot
 Microsoft Defender -- AntiSpyware
