SUMMER 2004 NEWSLETTER

SPECIAL ISSUE ON PESTS AND THREATS

VIRUSES/WORMS – By far the most common viruses are "mass-mailing worms". Once they infect a computer, they mail themselves to everyone in the address book. The "From" address is usually faked, so you should not blame the apparent sender, and you should not open an attachment just because it appears to come from someone you know. If you are in the address book on an infected computer, you may receive complaints blaming you incorrectly for sending out infected emails.

Some worms exploit vulnerabilities in Windows, but the majority use "social engineering", which means tricking you into opening the attached file. Some viruses spread via P2P filesharing, disks, instant messaging, and directly across LANs or the Internet. Precautions against viruses and worms include:

- Install anti-virus software (e.g. Norton AntiVirus or McAfee VirusScan)
- Update virus definitions and run a full scan weekly
- Enable scanning of incoming mail
- Renew the virus update subscription (e.g. LiveUpdate) when it expires
- Run Windows Update monthly (from Start menu, or http://windowsupdate.microsoft.com)
- Don't run filesharing programs like KaZaA
- Be extremely suspicious of attached files with extensions of .exe, .com, .bat, .scr, .pif, or .zip
- Don't open email attachments just because you recognize the sender
- Watch out for files with double extensions (e.g. "filename.txt.scr")
- Disable the Preview Pane in Outlook Express (Message Window in Netscape)
- Be suspicious of links or programs sent via Instant Messaging

Note that some email worms use the trick of faking the sender as support@<recipientdomain> or support@microsoft.com, to make the email sound genuine and important. So you may get an email apparently from support@kwom.com claiming your email service has been suspended because of unauthorized access and telling you to click on the attached, password-protected zip file. This email is not from KWOM or Microsoft! Don't click on the attachment!

ADWARE/SPYWARE – These are programs that install themselves on your computer to show you ads, change your homepage, redirect you to different websites, track your activities or keystrokes, steal passwords, etc. Or they may simply leave "tracking cookies" on your computer. Adware and spyware programs, collectively known as "malware", are typically installed when you download a free utility like Gator or Comet Cursor or Free Smileys, or click on an innocent looking button on a website.

Anti-virus software does not detect or remove malware, because in theory you agreed to install these programs. Typical symptoms include:

- slow computer performance
- your homepage has changed
- popup ads on sites that normally don't have popups
- X-rated popups

Some malware can be uninstalled, but most people find they need a spyware removal tool such as:

- AdAware (freeware or $39.95 Pro version, from www.lavasoftusa.com)
- Spybot Search & Destroy (freeware from www.safer-networking.org)
- Bazooka (freeware from www.kephyr.com/spywarescanner)
- Pest Patrol ($39.95 from www.pestpatrol.com)

It is often necessary to run more than one of these removal tools to find and remove all the pests.

SPAM – Spammers typically buy lists of email addresses. How does yours get on the list? Online retailers and even some ISPs sell their customer lists (KWOM does not do this). Some spammers "harvest" email addresses from websites, discussion groups, newsgroups, etc., or they may use a "dictionary attack" (combine popular names and a domain name, and hope it results in a valid email

address). If you get more than 5-10 junk emails per day, consider either changing your email address, or subscribing to our Postini email filtering service. Other suggestions for minimizing spam:

- If you must use your email address to buy or register something online, look for checkboxes to "opt out" of receiving email solicitations
- Avoid using your email address on websites, discussion groups and newsgroups, where it can be automatically harvested by a software robot
- Consider getting a second "throwaway" email address for online purchases and registrations
- NEVER follow unsubscribe instructions unless you know and trust the sender, otherwise you are just confirming that your email address is active, and you will get even more spam
- Don't bother with blocked sender lists, they don't work because spammers use fake, random sender addresses
- Our Postini filtering service will typically block about 95% of spam

EMAIL SCAMS – Email scams have become more serious than chain letters and money-smuggling Nigerian royalty. "Phishing" scams try to steal credit card or other account information by directing you to realistic looking fake websites and claiming that your bank, credit card company, PayPal, eBay, or an online retailer needs you to re-enter your account and password.

- Always go directly to your bank or credit card company website, don't click on links in emails
- Run Windows Update to patch vulnerabilities that help fake websites masquerade as real ones
- If you have already been tricked, contact your bank or credit card company immediately
- For more information on phishing scams, check out www.anti-phishing.org

POPUPS – Many websites advertise their products or pay for their operation with popup ads. Variations include ads that pop up after you leave the site (sometimes after a delay), and ads that hide underneath the current window. Some popups however are not ads but a necessary part of the site. The most annoying popups are from sites like DoubleClick that pay the website owner for each click. Free pop-up blockers like the one in the Google toolbar (http://toolbar.google.com) can automatically block popup ads, with configurable options for allowing popups when and where you want them.

If you are getting popups on sites that shouldn't have popup ads, especially if they are X-rated and your homepage has changed, your computer is probably infected with adware or spyware (see above).

Another type of popup is not a webpage but a Windows Messenger Service alert window. This service is supposed to be used by a printer, UPS, or network administrator on your local network, but some spammers are using it. We block Windows networking ports 135, 137-139 and 445 which are not really intended to traverse the Internet, but some spammers are sending Messenger Service alerts on UDP port 1026 which we are reluctant to block because it may have legitimate uses. You may want to turn off Messenger Service, see www.mynetwatchman.com/kb/security/articles/popupspam for instructions.

HACKERS – Despite all the media attention and hype from firewall vendors, the threat from hackers is overblown, unless you are running a server. Many software firewalls will warn you of dangerous portscans, when in reality this is probably just some kid seeing if your computer has already been infected with a backdoor program, or a filesharing server trying to contact the last person who dialed up and got the IP address now assigned to you. Email viruses infecting your computer and opening up a backdoor for relaying spam are a much more serious concern than actual hackers.

We recommend:

- Install anti-virus software, and do regular updates and scans
- Regularly run Windows Update and install all critical or security updates
- If you have Windows XP, enable the built-in firewall for your Internet connection
- If you have DSL or a cable modem, make sure your router includes Network Address Translation (NAT) which provides adequate firewall protection for most individuals and small businesses
- If you have Windows XP firewall or a NAT router, you don't need an additional software firewall

HOAXES – We still get reports of the grey teddybear hoax. Someone warns you of a virus which is not detected by anti-virus programs, saying you should look for and delete a file "jdbgmgr.exe" with a grey teddy bear icon. Sure enough, you find the program yet it is not detected by your anti-virus program. Why? Because it is part of Windows and not a virus. There are many other virus hoaxes floating around, check a hoax website such as www.symantec.com/avcenter/hoax before taking any action.