Anti-Virus Overview and Online Safety

Erik Svenson - Microsoft

Definitions

- Malware
  - consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.
- Virus
  - A program that copies itself from one computer to another; used to corrupt files on a computer network
- Worm
  - Unlike a computer virus, it does not need to attach itself to an existing program
- Payload
  - Code in a worm used to do damage
- Trojan horse
  - A destructive program masquerading as a benign program
- Spyware
  - Used typically to collect personal info; can also install keylogger programs
- Rootkit
  - A program that enables privileged access to do bad stuff
- Adware
  - Usually harmless, generates popups of ads, but can also contain keyloggers and spyware
- False-positive
  - When an AV program identifies a valid program as malware
- False-negative
  - When an AV program fails to identify malware

Anti-Virus/Malware Options

Manufacturer	Product Name	Plusses	Minuses
Symantec	Norton Antivirus 2011	• Excellent malware detection & removal • Fast install • Minimal impact on system performance	• Scans slowish • Hard to read interface
Kaspersky	Anti-Virus 2011	• PCWorld top pick • Very good tech support • Very high malware detection	• Finds less scareware and rootkits, many false positives
ZoneAlarm	Security Suite		
Avast	AntiVirus 5	• Free • Very effective malware detection • Intuitive interface • Free phone support	• Adds for software • Some scans require user input
Sophos	Anti-Virus	• Free • Very good detection performance • Quick install • No ads • Scans for Mac and Windows	• No phone or email support
Microsoft	Security Essentials	• Free	
McAfee	VirusScan		

How to remove malware

1. Make sure AV program’s signature file is current
2. Disconnect the computer from the network
3. Run an AV scan
4. Back up your files
5. Boot the computer into Safe Mode
6. Remove any adware from your programs list in Control Panel | Add/Remove
7. Empty Recycle Bin
8. Reboot into “normal mode”
9. Re-run AV scan

Things to be aware of

- Online persona
- Phishing emails
- Phishing links

Be Wary of Identifiable Information

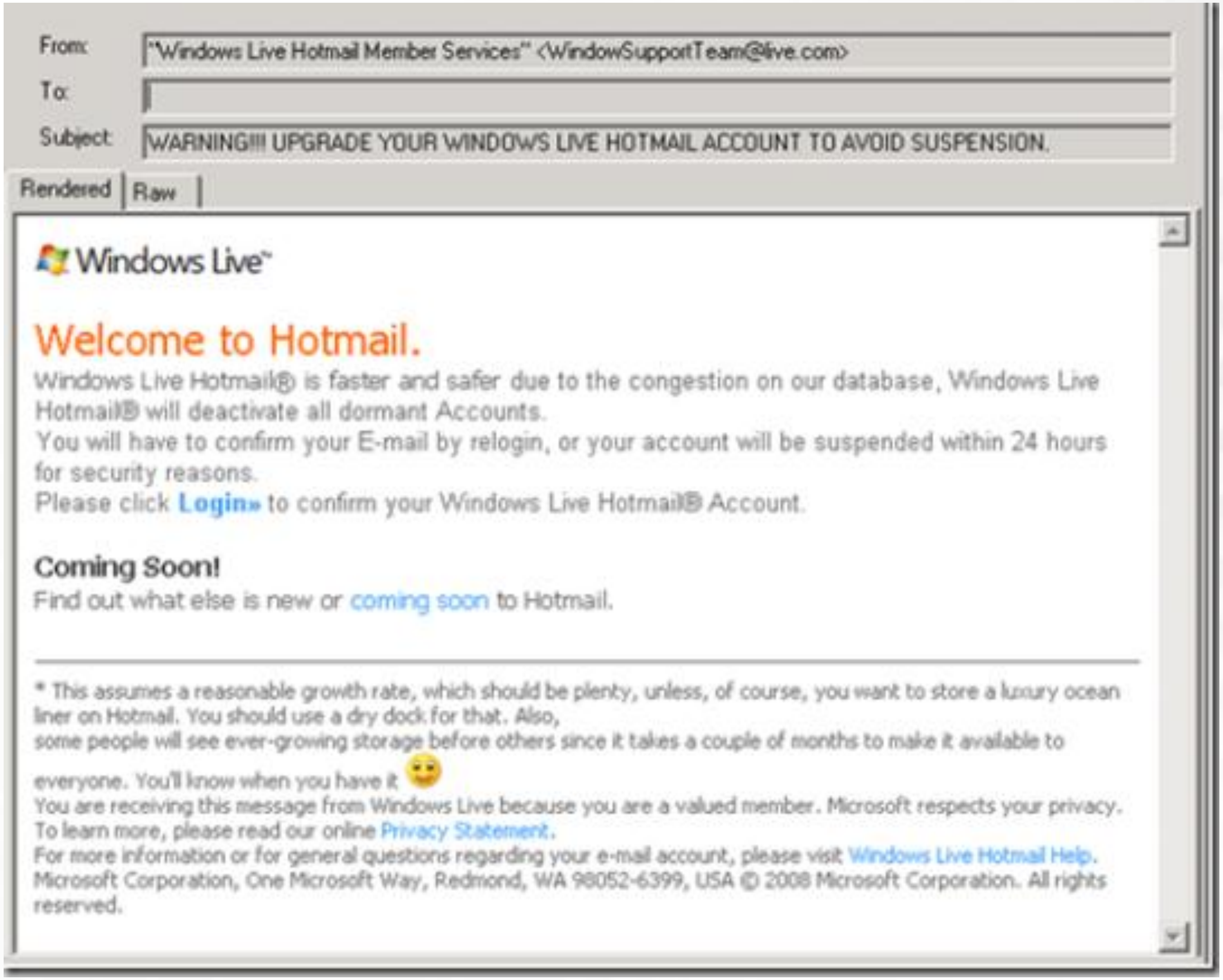
"Minimum information given with maximum politeness."

Many social websites allow people to join public groups that include everyone who goes to a certain school. Be careful when you reveal this and other information that could be used to identify yourself, such as workplaces, or the name of the towns they live in. Too much information can make you vulnerable to Internet predators, fraud, or identity theft.

Recognizing phishing email or links

- They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.
- They might appear to be from someone in your email address book.
- They might ask you to make a phone call. Phone phishing scams direct you to call a phone number where a person or an audio response unit waits to take your account number, personal identification number, password, or other valuable personal data.
- They might include official-looking logos and other identifying information taken directly from legitimate websites, and they might include convincing details about your personal history that scammers found on your social networking pages.
- They might include links to spoofed websites where you are asked to enter personal information.

Phishing example



From: "Windows Live Hotmail Member Services" <WindowSupportTeam@live.com>

To:

Subject: WARNING!!! UPGRADE YOUR WINDOWS LIVE HOTMAIL ACCOUNT TO AVOID SUSPENSION.

Windows Live™

Welcome to Hotmail.

Windows Live Hotmail® is faster and safer due to the congestion on our database, Windows Live Hotmail® will deactivate all dormant Accounts.
You will have to confirm your E-mail by relogin, or your account will be suspended within 24 hours for security reasons.
Please click **Login»** to confirm your Windows Live Hotmail® Account.

Coming Soon!

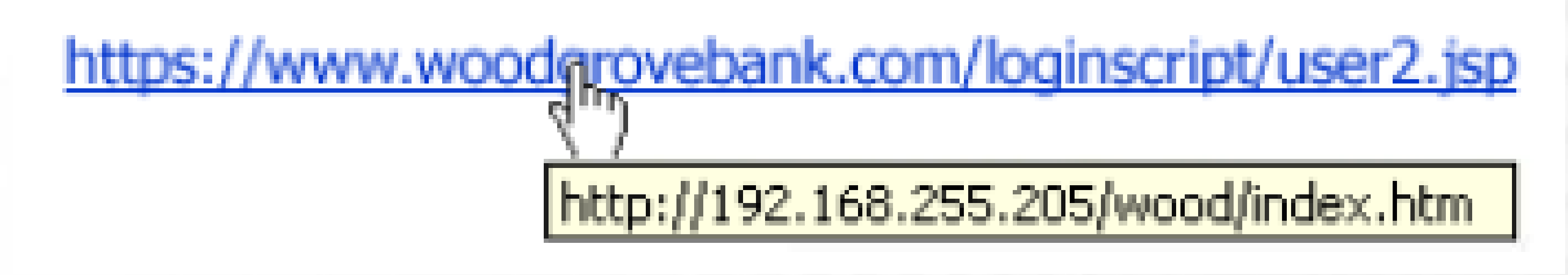
Find out what else is new or coming soon to Hotmail.

* This assumes a reasonable growth rate, which should be plenty, unless, of course, you want to store a luxury ocean liner on Hotmail. You should use a dry dock for that. Also,
some people will see ever-growing storage before others since it takes a couple of months to make it available to everyone. You'll know when you have it 😊
You are receiving this message from Windows Live because you are a valued member. Microsoft respects your privacy. To learn more, please read our online Privacy Statement.
For more information or for general questions regarding your e-mail account, please visit Windows Live Hotmail Help.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA © 2008 Microsoft Corporation. All rights reserved.

Phishing links

- Email can direct you to spoofed websites
- HTML-formatted messages can contain links or forms that you can fill out just as you would fill out a form on a legitimate website.
- Phishing links that you are urged to click in email messages, on websites, or even in instant messages, may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate website.

Phishing link example



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

Increase Security and Privacy

- In addition to blocking inappropriate content, it's a good idea to block sites and downloads that might be a risk to your security and privacy.
- **Use antivirus and antispyware** software like Microsoft Security Essentials. These can help you detect, disable, or remove viruses, spyware and other potentially unwanted software.
- **Create different user accounts** on your home computer. Each user logs on with a unique profile and his or her own Desktop and My Documents folder. You can give yourself an Administrator account and give your children Limited User accounts. Administrator accounts have full control over the computer. Limited Users cannot change system settings or install new hardware or software, including most games, media players, and chat programs.
- **Adjust web browser security settings**. You can help protect yourself through your web browser. Internet Explorer helps you control your security and privacy preferences by allowing you to assign security levels to websites.
- **Make sure Windows Update is on "Auto"**
- **Make sure your AV signature is up to date and that it is scanning**
- **Don't click on any email link that says it's from a bank, or the government**

Help! Where Do I Go?

The Federal Trade Commission maintains a rich site of information specifically addressing the impact of fraud and what to do if victimized. http://www.ftc.gov/bcp/edu/microsites/idtheft

The Internet Crime Complaint Center (IC3) gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. Link to report a cyber crime here: http://www.ic3.gov/complaint/default.aspx

Comparing Anti Virus Programs

http://www.av-comparatives.org/

The Microsoft Malicious Software Removal Tool checks Windows based computers for infections by specific, prevalent malicious and helps remove any infection found.
http://www.microsoft.com/security/pc-security/malware-removal.aspx

Individual Social Networking Sites have mechanisms in place to report abuse
Facebook: http://www.facebook.com/report#!/help/?page=843
MySpace: http://www.myspace.com/index.cfm?fuseaction=help.reportabuse
YouTube: ttp://www.google.com/support/youtube/bin/request.py?contact_type=contact_us
Bebo: http://www.bebo.com/Safety.jsp

Microsoft®