

TECH TALK & PIZZA

Presented by the
Technology Committee
of the
**Greater Delray Beach
Chamber of Commerce**

July 20, 2004

Tech Tricks to Minimize
Spam, Pop-Ups & Spyware



SPAM

Todd L'Herrou

Electronic Village Systems

(561) 272-3200

www.electronic-village.com



Tech Tricks to Minimize Spam, Pop-Ups & Spyware

Canning Spam

- What is Spam?
- What can I do about Spam?
 - Personal Actions
 - Email Programs
 - Spam Filters
 - Legislative “solutions”

What is Spam?

- Unsolicited Bulk Email
 - Usually commercial
 - Can include other bulk email: advocacy, chain letters, viruses, etc.

What Can I Do About Spam?

Personal Actions:

- Never reply to spam!
- Do not buy from any solicitation received via a spam email
- Strategic use of your email address(s)
 - Websites, chatrooms, dictionary attacks, shopping, etc.

What Can I Do About Spam?

Email Programs:

- The problem with preview...
- Mail Programs
 - Eudora (www.eudora.com)
 - Netscape (www.netscape.com)
 - Outlook (installed on Windows)
 - Pegasus (www.pmail.com)
 - others... (Pine, IncrediMail, etc.)

What Can I Do About Spam?

Spam Filters:

- Filter Types
 - Keyword / Heuristic filtering
 - Bayesian filtering
 - Whitelisting (accept only registered addresses)
 - Blacklisting (block certain “bad” addresses)
- Filter Problems
 - False Negatives (letting spam through)
 - False Positives (blocking “good” mail as spam)

What Can I Do About Spam?

Spam Filters:

- SAProxy www.statalabs.com \$30/\$40
- **SpamCatcher** www.aladdinsys.com \$30/\$30+s
- SpamSleuth www.bluesquirrel.com \$30/\$30+s
- Norton AntiSpam www.symantec.com \$40/\$40+s
- SpamBayes (spambayes.sourceforge.net) free

What Can I Do About Spam?

Legislative “solutions”:

- The nature of the problem
- CAN-SPAM act of 2003
- Ongoing efforts

SPAM

For more information contact:

Todd L'Herrou

Electronic Village Systems

(561) 272-3200

lherrou@electronic-village.com



POP-UPS

Anthony Vocaturo

E.CollectMD

(561) 953-2000

www.ecollectmd.com



Tech Tricks to Minimize Spam, Pop-Ups & Spyware

Pop-ups

Those advertising windows that pop up over or under other windows while we use the Internet — have become more and more ubiquitous as the Web has grown. For Macintosh computers, the Safari browser has pop-up blocking capability already included. But Internet Explorer, the most popular browser, does not yet include pop-up blocking, though Microsoft has recently said it will be included in its next Internet Explorer service pack. Many people believe the problem of pop-ups will disappear if pop-up blocking becomes a default component of Web browsers.

- The Web sites that sold or disseminated the most pop-up ads in the month of April include CNN.com, ESPN.com, Excite.com, Weather.com, and The New York Times.



Pop-ups

Pop-up purveyors are finding ways around popular new filters that aim to stomp them out, the latest sign of an Internet arms race over one of the most controversial online ad formats around.

- Google, America Online, Yahoo, EarthLink, Microsoft and a slew of niche software developers have begun offering consumers easy-to-install, free blocking software. As much as 30 percent of the Internet population uses a pop-up guard, according to estimates from ad technology companies. That number is set to soar when Microsoft releases an update to its Windows XP operating system later this summer that is expected to include a pop-up blocker for its Internet Explorer Web browser, which serves about nine in 10 people who surf the Web.
- Because IE so thoroughly dominates the browser market, ad executives and Internet watchers believe the changes could finally burst the bubble for pop-ups.

Pop-ups

- Marketers intent on preserving and extending the lucrative format have already developed workarounds that are duping existing blockers, setting the stage for a major battle for control over consumer PC screens.
- Click rates, or the number of times people click on an ad, could explain the growth of pop-up ads. Marketers say between 2 percent and 5 percent of the people who receive them will respond with a click. That compares with less than 0.35 percent for the most widely used ad on the Net today, static banners, according to an ad server report from DoubleClick.
- Pop-unders still yield the best performance.
- Blocking software typically suppresses a new window. It detects a command known as "openwin" for opening a new window, which would be written into the HTML (Hypertext Markup Language) of a Web page. That command calls on a third-party server to deliver the pop-up or pop-under.



Pop-Ups Bottom Line:

- At stake is the future of a lucrative form of online advertising that many ad executives say is among the highest performers for Internet marketers--despite severe negative reactions from a majority of Web users.

Pop-ups are of three kinds:

1. General browser pop-ups
2. Messenger Service Ads
3. Pop-ups generated by adware and spyware

General browser pop-ups

These pop-ups can be prevented by installing a pop-up blocker [say, Google Toolbar] The pop-up blocker in the Google Toolbar prevents new windows from automatically opening when you visit a website. Often times, these new windows display advertising that can interfere with your ability to see the content on the page you're trying to read. Many people use pop-ups killers which can aggressively block pop-ups and cause problems opening New browser window [Clicking a Hyperlink in a browser window or email client].



Messenger Service Advertisements

If the title bar reads as "MESSENGER SERVICE" with gray ADs, then it is the famous Messenger SPAM. This is applicable only for Windows 2000 and Windows XP. The "Messenger Service" [different from Windows Messenger IM] is responsible for transmitting these text-based messages. While disabling the Messenger Service can stop the pop-up Ads, it's not sufficient in the security point of view. These messages arrive to your system because there is a way for someone to transmit data to your computer via TCP and UDP ports. This means, some intruder can do nasty things on your computer with this port open. The BEST and HIGHLY RECOMMENDED method to prevent these type of pop-up and to harden the security of your computer is to enable the Windows XP's Internet Connection Firewall and upgrade to Windows XP SP1. This blocks the ports required for Messenger Service data transmission.



Pop-ups generated by Ad-ware & Spyware

- Spyware cause the same effect as general Browser pop-ups but they are usually powered by malware Browser Helper Objects, ActiveX controls which attaches to Internet Explorer and contacts the respective AD servers to fetch ADs through internet. This not only means waste of Internet bandwidth, but your private information may also be sent to someone. You need to treat any outgoing connection without your permission, as a 'security threat'
- Spyware are equally dangerous as Viruses / Trojans and your Anti-virus software may not be fully capable of detecting Spyware and Trojans. Therefore, it's a good idea to scan your system using a good Anti-virus package and also with a spyware removal utility such as Ad-Aware [www.lavasoftusa.com]. You **must** update the pattern files before scanning, this ensures good detection.
- Third-party Pop-ups killers might not help you much in case of browser hijackers, Data-miners and malware ActiveX controls. They only block pop-ups ADs generated by spyware.

Some options for dealing with pop-ups.

- **Commercial Products:** Software can be purchased to block pop-ups. Products such as Pop-Up Stopper (www.panicware.com/product_psprofessional.html), Ad-aware Plus (www.lavasoftusa.com), and PopUpCop (www.popupcop.com) offer pop-up blocking, in addition to other abilities. Ad-aware Plus, for example, checks your computer for spyware, and Pop-Up Stopper provides browser cleaning to erase your surfing history, browser history, cache, and cookies.
- **Toolbars:** The free Google and Yahoo! Companion toolbars, which can be added on to Internet Explorer for search functionality, also provide optional pop-up blocking. These are easy to turn on, and if you'd like to track how many pop-ups have been blocked, they include a counter on the toolbar.

Some options for dealing with pop-ups.

- **ISP-Provided Pop-Up Blocking:** Some Internet service providers, such as AOL and Earthlink, have added pop-up blocking to their software. In addition to blocking pop-ups, Earthlink offers additional functionality for your money by giving you the option of viewing thumbnail versions of blocked pop-up windows and blocking Flash and Shockwave content.
- **Freeware and Shareware:** Check your favorite shareware site (such as shareware.com) to download pop-up blocking products such as Pop-Up Stopper Free and Pop-Up Defender.

What is Microsoft doing to combat this problem?

SERVICE PACK 2 for Windows XP.

- SP2 turns off the Windows Messenger service by default. Spammers have latched onto Windows Messenger--which is supposed to be primarily used by systems staff to send administrative messages to computers on a network--as a way to deliver unsolicited pop-up ads.
- In addition, the update tweaks the Internet Explorer Web browser to block pop-up ads on Web sites and to prevent inadvertent downloads of software.
- Microsoft has said it expects to have a final version of SP2 ready by mid-2004 for all Windows XP users



Warning POP-UPS

For more information contact:

Anthony Vocaturo

E.CollectMD

(561) 953-2000

aev@ecollectmd.com



SPYWARE

Steve Weingart

Gulfstream Technologies, Inc.

(561) 394-5086

www.gulf-stream.net



Tech Tricks to Minimize Spam, Pop-Ups & Spyware

Spyware

What is it? How do we get it?

What does it do? And...

HOW DO WE GET RID OF IT!!!???

Spyware: What is it?

- Also known as Malware, Scumware, Ratware, Hijackers and other less kind names.
- They are a class of programs, cookies & Windows registry keys that give your information or resources to others.
- Most are non-targeted and harmless, even if they are annoying, like pop-ups.
- Others are malicious and can use your PC for other purposes, like sending Spam for others or redirecting your searches to a specific place.

Spyware: What is it? (cont.)

- Some Spyware is worse than that!
- There are keystroke loggers.
 - Some of these install themselves and send your info to someone else, this is BAD!
- There are recording programs that capture **EVERYTHING** on your screen.
 - These are typically commercial programs that someone installs.

So, how do we get Spyware?

- Typically a program or cookie gets into your PC on the coat-tail of something else, most often a web page or an email with links/programs attached or embedded.
- Often you are asked to click 'Yes' for something, but others don't even ask.
- Some hide in the installation of a legitimate program (one example is a Weather reporting program, which brings along several spies/actions).

How do we get Spyware? (cont.)

- Some came on your PC (usually tracking cookies).
- It may have been installed by an employer, family member or thief.

What does Spyware do?

- Most often, it's an anonymous tracking cookie that vendors use for statistics.
- Almost as often, it causes pop-ups. Some can be different from the usual kind and are not stopped by pop-up blockers.
- Worse.. It can hijack your connection to the Internet and redirect your traffic through places that you don't know about. This is most common with searches where the hijacker puts in their own results.

What does Spyware do? (cont.)

- Now the bad stuff: Spyware/Hijackers can record your keystrokes and send the info to others.
- Spyware/Hijackers can use your PC as a source of Spam, Viruses and other Malware.
- They can even make your PC a source of a Distributed Denial of Service attack (DDOS).
- But usually what spyware does that makes most people *crazy*, is that it uses so much of your PC and causes so many pop-ups, that the PC becomes practically unusable.

So, what do you do about Spyware?

- There is not a lot you can do to avoid exposure (besides not using the Internet).
- Do install antivirus software and keep it updated (weekly). Norton, McAfee, Trend, AVG, Panda are fine.
- As in avoiding viruses, don't open attachments from unknown senders and turn off the preview pane.
- Do install pop-up blockers (Google Tool bar is our favorite, it's free).
- Do use Spyware removal tools.
- Professional Spyware packages hide themselves very well, some essentially can't be found.
- When all else fails, call a professional.



Spyware Removal Tools

- Run Spyware removal tools monthly to weekly.
- If you are a heavy web surfer maybe daily.
- Two very good tools are: Spybot Search & Destroy 1.3 (older versions are no longer updated, so you must get the current version), and AdAware 6.
- Check for updates *EVERY* time that you run the tool!!!
- These tools are fairly easy to use and reasonably safe. But...read the instructions!

Spyware Removal Tools (cont.)

- Sometimes you have to use 'Heavy Duty' tools to remove the new or difficult ones.
- MSCONFIG can be used to remove programs that automatically start at boot.
- HiJackThis is a more powerful version of MSCONFIG aimed specifically at network connections.
- Regedit can be used to look for/correct/erase bad registry keys.
- These tools can wreck Windows if you don't know how to use them. If you have to ask yourself if you have the needed skills, you probably don't. **BE CAREFUL!!**

Spyware Removal Tools (cont.)

- Almost the last resort, and the most difficult, is manual removal.
- This usually requires a special boot disk so that you are not running from the hard disk with the problem (Win98 boot floppy or WinPE boot CD).
- The bad files are identified and erased.
- Needless to say, this can be VERY tricky and a mistake can damage your applications or Windows.

Spyware Removal Tools (cont.)

- Last resorts:
 - In XP, try a system restore to before the problem started.
 - Or, back up the data only, format the hard disk and reinstall Windows.
 - Or, wait a few days or weeks for the removal tools to identify the problem Spy/Hijacker (this often works if you can live with the problem).

Spyware Conclusions

- If you use the Internet, you are exposed.
- Don't:
 - Open unknown attachments.
 - Follow web links in unsolicited email.
 - Surf known bad Websites.
- Do:
 - Close windows that pop-up and offer things by using the X in the upper right corner.
 - Turn off the preview pane in Outlook/Outlook Express.
 - Install and update antivirus.
 - Install, update and use Spyware removal tools.
 - Call for help if you are in over your head.

Good Spyware Tools

- Spybot Search and Destroy 1.3
 - www.safer-networking.org/en/index.html
- AdAware 6
 - www.lavasoftusa.com
- HiJackThis (and CoolWebShredder)
 - www.spywareinfo.com/~merijn
- Free Antivirus (for personal use)
 - www.grisoft.com/us/us_index.php

SPYWARE

For more information contact:

Steve Weingart

Gulfstream Technologies, Inc.

(561) 394-5086

shw@gulf-stream.net



Questions?

Spam
Pop-Ups
Spyware

With many thanks to...

- **Bill Wood**, President & CEO
- **Beth Johnston**, Membership Development
- **Tony Newbold**, Technology Committee Chairman
- **Todd L'Herrou, Anthony Vocaturo and Steve Weingart**

PowerPoint Presentation by:

Tom Kriete

ComputerWorX, Inc.

Software, Solutions & Services

(561) 417-6680

For a PowerPoint file containing this presentation, send e-mail to

TechTalk@myComputerWorX.com

