

Email SPAM & Email Internet Security

Greenspring Village

November 10, 2009

Mark Leymaster

What's This About

- The topic this afternoon is email SPAM, which gets a little creepy sometimes. **Don't Panic.**
- This excludes comment-SPAM on blogs or list-SPAM, Twitter-SPAM or other non-email SPAM
- Sorry, but I want to leave time for questions.
- We're also not going to spend much time on Internet Security generally, but mostly as it is compromised by email SPAM
- There's a pdf of this slideshow, so you don't need to take notes unless you like to.

Who am I

- I'm Mark Leymaster, Internet Services Director for CPCUG, the Capital PC User Group, of which the Greenspring meeting today is a Special Interest Group (SIG). I'm at ISD@cpcug.org
- No one is honestly an anti-SPAM "expert," least of all me. I have too much experience dealing with it to think there are easy answers. I'm happy to offer some serious advice, but I'm generalizing.
- Be skeptical of anyone trying to sell you an anti-SPAM "solution," especially if it's easy and comprehensive. Snake Oil is so last century.
- As we'll see *you* are the best & easiest solution.

Plan for This Presentation

- Brief overview of Toxic email-SPAM, and the email delivery system on your desktop.
- How spammers get your address and how to reduce that risk (since you can't stop it).
- Show & Tell on other ways to manage or divert SPAM, such as common sense and filtering.
- Best “tool” to manage SPAM and improve your internet security is between your ears. Really.
- If others share your computer, everyone one of you has to behave to avoid toxic SPAM.

What is Email SPAM

- You probably know it when you read it.
- For those who like definitions, a good definition for today is SPAM is any **unsolicited email you get, whether or not it is really addressed to you.**
- An ugly subset of this is unsolicited “toxic” email that messes with your time, money, data, computer or identity unless you manage it.
- There’s a trick here: these definitions exclude other kinds of SPAM (and may change next year).
- What’s SPAM to me may not be SPAM to you.

Are you Worried Yet ?

- Opening unfamiliar email attachments is the best single way to infect a healthy computer with a virus or spyware or identity-theft tools.
- Second best is clicking on an unfamiliar email link that infects your browser and from there you might get viruses and mal-ware.
- Crooks make a lot of money from toxic-email, chiefly from those who fall for it or click unwisely
- Remember, anti-virus and anti-spyware will diagnose the problem **after** you've got it, and may only sometime be able to help you get rid of it.

Low-Tech Scams by Email

- Spam is also a quick and cheap way to run all kinds of scams and frauds, such as
- Fake winnings such as a lottery or a gift,
- Fake inheritance or easy money making,
- Identity theft by misrepresentation, such as false requests to reset bank or ebay accounts that use fake websites that look real, or
- “Insider” investment tips and opportunities.
- As with phone or paper mail frauds, you have to think it through. **Never** act without investigating.

Toxic SPAM plays to curiosity, greed and guilty pleasures too.

- Offer from a stranger to acquire something at an absurdly low price such as drugs or software or self-improvement, often from a foreign country.
- A stranger praying for your help in transferring a large sum from overseas, with a profit to you.
- An intriguing (fake) message to someone else, with a link or attachment to click to eavesdrop.
- Promised access to pornography or quick riches,
- An electronic greeting card from a “friend” or a fun-seeming invitation with a link or attachment.

Where does SPAM come from

- Everywhere. Most SPAM is from the US, because skill, greed & easy access are here.
- SPAM truths are ever changing. Early SPAM was playful, later anarchistic, now for-profit
- It comes to you because your address has been compromised: harvested from websites or honest mailing lists, stolen from a careless correspondent's address book or taken from an insecure online database, copied from your ISP's server, sold from a once secure list by a successor company dumping assets or because you replied to bad email in the past.

Visible Signs of SPAM

- Subject is missing, a foreign language unknown to you, nonsense or inflammatory.
- Sender is you or unknown to you.
- Misspellings, grammar or gross layout errors in the subject or body text.
- Illegal or improper offers such as bootleg software or deeply discounted drugs.
- Addresses in the wrong places or duplicated

False SPAM (a moderate pain)

- False SPAM, as used here, is email that looks like it could be toxic but *after the fact* turns out it isn't.
- Some unwanted email is non-threatening but still SPAM. Thinking of it as “good SPAM” is unwise.
- Common false SPAM for me includes an e-greeting card from a real friend, with a link or attachment that comes from a sender I don't know. There are a lot of genuine toxic SPAM of exactly this type, so
- I have to contact my friend first, confirm they ordered this message before I dare click through. I actually wish they wouldn't send this kind of thing.
- What if my younger correspondents use unfamiliar addresses, no signature and attach photos?

Bear Down: Think before Clicking on that Alien Email

- Treat all probable SPAM as if it might be toxic: click and move it gingerly from the beginning, like you might a possibly stinging insect nearby.
- If you suspect it's SPAM from the email subject line, and it is not from an address you know, I recommend you don't open it. Why risk it?
- Make a JUNK or SPAM folder if you must collect this stuff, to hold suspect SPAM.
- Most of the time you should **delete** it the first time, so you don't waste time analyzing it repeatedly.

Bad Ideas Involving SPAM

- Never, never, never reply or respond to SPAM.
- Don't believe what you read in SPAM.
- Don't unsubscribe using a provided link in the email unless you are absolutely sure it is legit. Most unsubscribe links are toxic.
- Don't send the SPAM back, as it will never reach the spammer, and just clog the system for others.
- Don't try to read the SPAM unless you know how.
- Avoid Outlook Express or any other Windows Email program that automatically opens the email.

Basic Thoughts on Toxic SPAM

- Don't Panic. You can drive defensively. Just pay attention to the warning signs.
- Regular backups of your entire computer *before it gets compromised* is the best action you can take. Do it weekly if you can, so you can restore you computer after an attack. Accept no substitutes.
- Not all malfunctions are your fault: a lot of this difficulty is from badly written software and insecure websites, e.g. But there will be still fewer problems if you think first and click less.

Prevention Beats Cleanup

- Preventing SPAM avoids most of the trouble I've described and more. But preventing is work.
- We've already covered toxic-spam avoidance.
- Guard your address, share with the trustworthy.
- Additional email addresses are affordable.
- Substitute temporary addresses when you signup in risky places. Many email hosts allow aliases.
- Don't use cc when bcc will do. The latter hides your associate's email addresses from others.
- Never send to lists in the clear, use bcc;

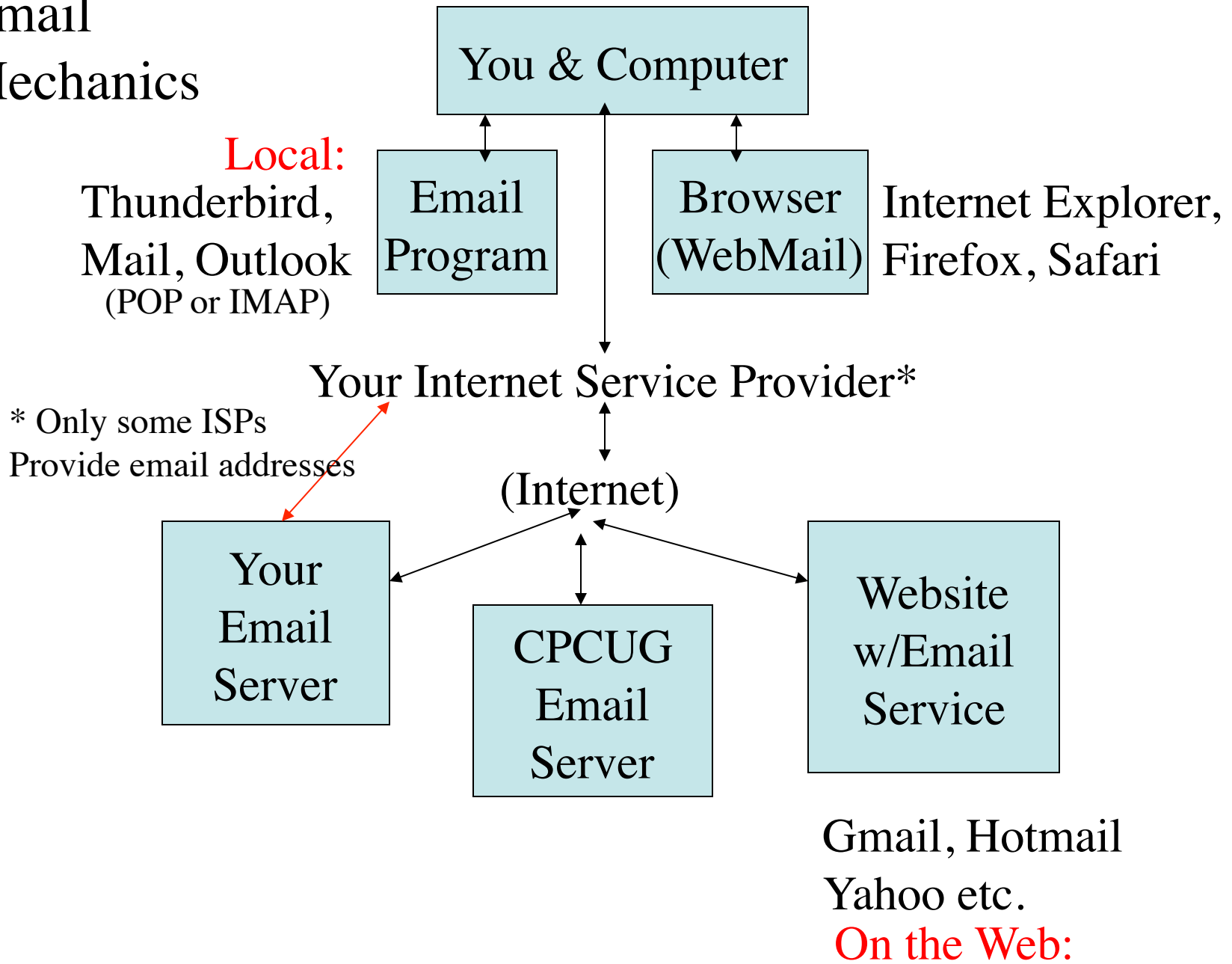
More on Address Protection

- Don't post addresses in the clear on web pages if you can substitute graphics with it instead. If you can't do that use a crippled address such as [ISD@\[omit-this\]cpcug.org](mailto:ISD@[omit-this]cpcug.org). The idea is to defeat harvester internet robots who use the whole thing.
- Don't use mail to links on personal web pages, instead use a form that hides your address. If you can't do that, consider not posting your address.
- Generally, social media web sites are resources for SPAMMERS. Participate responsibly.

More on Prevention & Security

- Remember that your email address is often linked to various private information, your identity and your money if you shop or move money on line.
- **Never send sensitive information in email**, like credit card numbers, passwords or PINs, and only use secure web pages (https) for places you trust. When in doubt, use the US mail or a phone.
- You protect your money and ID as well as your email address with good, frequently changed **strong** passwords. Yes, I know it is a pain.
- Keep your computer and its anti-virus, firewall, anti-malware and other Security tools up to date. *And use them.* Please spend time setting them up too, as default installations can be problematic.

Email Mechanics



Email Mechanics in Words

- Your email program, if you use one, is independent of your browser's webmail access. Both need to be kept updated.
- Messages in your email program are local, that is, on your hard drive (for backup, which you should)
- Messages in webmail are “in the cloud,” that is, out on the internet and less private; you can download webmail messages to your hard drive for backing up, but it takes extra steps. Don't leave important email unbacked up in some form.
- If you don't erase messages on any email server, it may refuse new messages if your mail box is full.

Email Addresses > Mailboxes

- Each email mailbox has one “primary” address, which is pretty hard to change. Doing so will permanently disable future receipts under it.
- Many email boxes allow “secondary” addresses or aliases, that are delivered to your primary address. These are easy for the user to change, and provide **disposable** email addresses if you want.
- Some email accounts actually provide multiple independent email boxes & other features.
- If you own your own domain-name, you can use that domain to create unlimited email usernames.

About Webmail

- Toxic attachments are less risky but links are not.
- Webmail usually gives you anti-SPAM and message sorting (“filtering”), which can be smarter than your ISP’s mail server or your Email program, though with less user control. Use it.
- Webmail usually deletes suspected SPAM after 30 days; with your own Email program you can keep it as long as you want. Decide if you can ignore it.
- Webmail is accessible from any browser you trust with your email account password. Generally I suggest you **change** your password after using public browsers if you care about privacy.
- Attachments maybe limited, harder to store & use.

About Laptop/Desk Email

- Not all webmail allows you to maintain many separate folders as you prefer, Email programs do.
- This permits selective backup, since email folders on your computer are data files like most others.
- Older Email program help & support are limited.
- Email programs suffer less connection delay when used to compose, revise or manage messages.
- Email programs allow multiple mailboxes to be managed from one place.
- Size or types of permitted attachments are up to your ISP, and incoming restrictions are few. If outgoing attachments are restricted, use webmail.

AntiSpam Measures I

- Most email hosts have automatic anti-SPAM measures, a few will let you tune or turn them off. When working the SPAM never reaches you.
- Spam Assassin, used by CPCUG and many others, has a multistage process of “scoring” all messages that relies on updated black-lists of bad domains used by spammers. White lists can override this.
- Usually, suspected SPAM, that gets a bad score, is put in a Junk or SPAM folder on the user’s account, so it can be reviewed by you. Messages over 30 days old maybe deleted automatically.
- If you can’t or don’t turn it off, you *must* check that folder monthly to recover **false positives**.

White Lists and Black Lists

- From here we're talking measures against SPAM that has already got into your email box once.
- Most email boxes permit you to use both "Black lists" of address you never want to see (You can auto delete too if you're sure you've not included any future friends, see also "Filters" hereafter) &
- "White lists" that you always want to have delivered, ignoring any anti-spam rating.
- Setting up these lists and maintaining them can be tedious. Not all email providers make this easy.

Anti-SPAM Measures II

- Most think false positives are the biggest problem in automated SPAM filtering, that is automatic diverting or deleting of your non-SPAM emails. Some webmail allows you to reduce your protection in order to adjust for this. White lists are often better if you've the option and the time.
- The false negative you see in your inbox, but you are likely to overlook the false positives.
- This is the reason that a minority of CPCUG members refuse automated anti-SPAM services.
- Instead they manage it all in their Email Program. That's a lot more work for a lot more control.

Spoofing Complicates Things

- It is not hard to “spooft” an email address, that is to make mail appear to be from you that is not. This makes for no end of trouble.
- Spammers spoof as matter of course, so no one can back-track to the true sender.
- If your address is spoofed as sender do not assume your system has been compromised. Most of the time it is just a misuse of your address.
- Hasty or ill-informed reporting of spoofed addresses as abusers causes ISPs to refuse legitimate mail if they black list that domain.

Filters: Anti-Spam Measures III

- After your email host is done SPAM scanning, if you use an Email program like Thunderbird, you have some more options. Filtering is the main one.
- Once the messages are delivered, you can run your own black or white lists, search for offending terms or syntax and more, see “Signs of SPAM”
- Spoofed address may result in false negatives and can distort white lists and black list effectiveness.
- Filtering needs understanding of the program and filtering logic, which can vary from Gmail to Thunderbird. We’ll take a look at this in a minute.

Anti-Spam Measures IV

- If you're really into SPAM killing you've further more complex options.
- You can install dedicated anti-spam tools on your desktop that may or may not work well with your system and your Email program.
- Usually they cost money, they can slow your computer noticeably, require updates if not a constant internet connection, and they maybe incompatible with other software you like.
- CPCUG has a big program free to a member who asks, but it is hard to install, harder to maintain and so is not commonly recommended.

Anti-SPAM Measures V

- If provided in your application, you may be able to mark individual offensive messages as SPAM while you read the email subject line listed within your webmail or Email Program. (It is smarter to review possible spam by subject lines rather than opening the email.) In time your software learns what you consider to be SPAM and diverts it, or so the applications say.
- Typically you select the line and click a SPAM button. You can usually undo that click too.
- Great idea, though my experience with this last stage is not objectively very productive.

Show & Tell

- I prefer Email Programs to web mail, though the latter is a good backup and key for travel and emergencies. Your mileage may vary, as your tolerance for risk probably differs from mine.
- I use Thunderbird, just as I use Firefox instead of Internet Explorer; both kept updated
- I also use Apple Macintosh, as you'll see. Backup regularly, not just Apple's TimeMachine.
- Let's look at CPCUG Webmail, then my Email Program on my laptop.

Human Factors and SPAM

- What about other people who borrow your computer to get to the internet?
- If anyone else who uses your system clicks on toxic-SPAM (or downloads malware), you could be stuck with the cleanup. Who do you trust?
- At least make them use a Guest Account that does not permit installing software. You can back it up before it's messed up, and then restore if needed.
- If you've a big problem with this, try Deep Freeze <http://www.faronics.com/html/Deepfreeze.asp>

Ideas on Stronger Passwords

- Never use a real phrase or familiar name. Sequences like ABC or 123 stink too.
- You want passwords that you can remember but that your best friend or your nephew can't guess.
- For example, pick an old nickname *not* in current use, then substitute one or more punctuation marks (@ for A, e.g.), a number (3 for e) and capitalized a letter other than the first.
- You can customize passwords for websites by using the short name without vowels for the site as a prefix, such as "mcys" as a prefix for Macy's

URLS for Window Security

- Dennis Courtney, CPCU President, suggests
- Avg Antivirus <http://free.avg.com>
- Microsoft Security Antivirus (one URL)
http://www.microsoft.com/security_essentials/default.aspx
- Commodo Firewall
<http://www.personalfirewall.comodo.com/>
- ZoneAlarm Firewall (one URL)
http://www.zonealarm.com/store/content/catalog/products/zonealarm_free_firewall.jsp
- SpamBytes for Outlook <http://spambayes.sourceforge.net>
- Advanced WindowsCare PE
<http://www.iobit.com/advancedwindowscareper.html?Str=download>

Human Behavior is Important

- What's important here depends on your situation.
- Despite risks in casual SPAM behavior, it *can* be managed so **Don't Panic** if you get some: move it to quarantine, investigate deliberately then delete.
- Fear, like Greed, impedes your Judgment. Toxic SPAM is designed to do just that. Think before clicking on links or opening attachments.
- Use/Get tools to (a) secure your computer, and your mail, and (b) segregate SPAM. **Backup your computer monthly, personal files weekly.**
- If others “play” on your computer or just share it, give them a *separate* account. You're only as safe as the most careless user with access to your PC.

Questions ?

- I can be reached at ISD@cpcug.org. Ask your question in the subject line & be specific, please.
- If you're a current CPCUG Member you can also ask questions at Support@cpcug.org
- Thanks for asking questions in advance. If you didn't get the answer already, please ask again if it's about email-SPAM.
- I'll leave a PDF of these slides with Ann.
- So ... Questions anyone?