
Spam

“As more people use email, marketers are increasingly using email messages to pitch their products and services. Some consumers find unsolicited commercial email - also known as "spam" - annoying and time consuming; others have lost money to bogus offers that arrived in their email in-box. Typically, an email spammer buys a list of email addresses from a list broker, who compiles it by "harvesting" addresses from the Internet. The marketer then uses special software that can send hundreds of thousands - even millions - of email messages to the addresses at the click of a mouse.”

—From <http://www.ftc.gov/spam> — a source of tips on email scams/deceptive spam.

At CCSF, our GroupWise administrator filters out about 70% of all email before it reaches you. At present she also spends hours each day checking on the legitimacy (or the opposite) of individual email messages. During the workshop for which this handout was designed you will hear about other measures that we might be able to take at CCSF.

FTC Research

- FTC Anti-Spam advice (Adobe Acrobat Format):
<http://www.ftc.gov/bcp/online/pubs/online/inbox.pdf>
- FTC Report on false claims in SPAM (Adobe Acrobat Format):
<http://www.ftc.gov/reports/spam/030429spamreport.pdf>

Fraud updates & advice

- <http://www.pcworld.com/resource/browse/0,cat,1513,sortIdx,1,00.asp>
- http://www.mailfrontier.com/fraud_alerts.html and
http://www.mailfrontier.com/fraud_index.html
- <http://antispam.yahoo.com/tips#1>
- <http://spam.abuse.net/>
- <http://antispam.yahoo.com/faqs>

Avoiding SPAM (from <http://antispam.yahoo.com/tips#2>)

- Protect your email address - treat it like your phone number.
- Use an email service that offers spam-fighting tools.
- Never email your password, credit card numbers, or other personal information.
- Don't post your email address in public places where spammers mine for emails.
- Use a Disposable Email Address when posting.
- Never respond to unsolicited email or click on a URL or web site listed in spam - this can alert the sender that your email address is valid.
- Never forward spam chain letters

Phishing

Phishing attacks involve the mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. These fraudulent messages are designed to fool the recipients into divulging personal authentication data such as account usernames and passwords, credit card numbers, social security numbers, etc. Because these emails look “official”, up to 5% of recipients may respond to them, resulting in financial losses, identity theft, and other fraudulent activity. From <http://www.antiphishing.org/>

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.

- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.

CAN-SPAM Law

The CAN-SPAM Law 'Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003' (passed Jan 1, 2004):

<http://www.spamlaws.com/federal/108s877.html>

According to CAN-SPAM legislation, e-mail must meet five basic requirements to avoid being labeled "unsolicited commercial" e-mail:

- The e-mail message must have correct header information.
- The message must have an accurate subject line.
- The message must contain a functioning return e-mail address.
- Senders must not send e-mail more than 10 business days after receiving a request to be removed from a mailing list.
- Commercial e-mail must contain a clear identification that the message is an advertisement, must contain a conspicuous notice of opportunity to decline further e-mail and must display the physical postal address of the sender.

Some reactions: <http://www.ohio.com/mld/ohio/business/7591414.htm>

http://www.pcmag.com/print_article/0,3048,a=119423,00.asp

"Identifying spam is really quite easy—the senders are unknown and the subjects are typically short like, "Hey You"—but keeping it out of your mailbox is another matter entirely. ... The bill states that there must be a "return address or comparable mechanism in unsolicited commercial electronic mail." Most junk e-mail does have a return address, information for opting out, or both. Unfortunately, the info is almost never valid, and following the opt-out procedure usually cements your status as a real e-mail target."

From PC Magazine: http://www.pcmag.com/print_article/0,3048,a=41369,00.asp

"... unsubscribe links are typically dead or invalid. The suggestion that a spam recipient would open the spam mail, let alone click on a link within it, makes some industry veterans apoplectic.

"Spammers ... take the required snail-mail address and place hidden characters between letters. "Houston, TX" might appear on screen as "H o u s t o n, T X" where each space is filled with, say, a white, invisible x. In this case, the text filter, which some anti-spam engines employ, sees ""Hxoxuxsxtxoxn, TxX." The filter sees only nonsensical words, but the address still looks real on your PC. The result: There's no way for the filters to capture a traceable address, but end-users still think they're seeing a real mailing address. The use of hidden characters has long been a common practice for hiding pornographic phrases...."

-“Keeping up with CAN-SPAM” (eWeek magazine): <http://www.eweek.com/article2/0,1759,1472742,00.asp>