

E-mail Lingo

A glossary of terms and concepts

attachment -- An attachment is a file sent by e-mail. The contents usually aren't part of the original e-mail, but can be accessed by clicking an icon. In GroupWise the icon is a paperclip. Attachments can include word-processed documents, spreadsheets, music clips and slide presentations.

bounced -- When an e-mail message you have sent is returned to you without reaching the recipient. Often it will be returned with the message "user unknown" or "host unknown." A hard bounce occurs most often because of an error in a subscriber's e-mail address (misspelled, wrong host).

emoticons -- When speaking one-on-one, you can usually gauge a person's emotions and mood from tone of voice and facial expressions. E-mail offers no visual or aural clues, which makes communicating tricky. One solution is to use emoticons, glyphs constructed with keyboard characters such as the colon and parentheses: :-) is happy : (is sad or angry.

glurge -- This term describes human-interest stories, usually circulated by e-mail, that often are untrue or have been exaggerated so as to make them untrue. Glurge stories often seek to inspire or outrage recipients with stories that are overly sentimental, sweet, tear-jerking or heart-tugging. They usually are based on inaccurate information or exaggerated facts or were made up and passed off as true.

harvesting -- Also called scraping, e-mail harvesting is an automated process in which an address collector uses a robot program to search the Internet for exposed e-mail addresses. The program collects the address into a database, which the collector sells to anyone who wants to send mass e-mails. Harvesting helped spawn today's great tide of junk e-mail.

HTML mail -- HyperText Markup Language (HTML) e-mail can use different fonts, styles, sizes, and colors, plus inline graphics. A well-constructed HTML message resembles a web page.

Joe Job -- A spam-industry term for forging an e-mail address to hide the sender's identity.

mail bomb -- Malicious persons send large amounts of mail to the same mailbox in an attempt to overload the mail system. A successful mail bomb may cause the victim's disk quota to be exhausted, the disk holding his mailbox to fill up, or his computer to spend a large proportion of its time processing mail.

phishing -- Scammers send out millions of fake e-mails designed to trick unwary recipients into disclosing sensitive and valuable information, such as Social Security, credit-card and bank-account numbers, which they can then use to open online accounts, make online purchases or wreak other financial havoc. In one version of the scheme, scammers send bogus e-mails that look like messages from legitimate online companies, warning recipients that they must disclose financial information in order to maintain their accounts. The messages usually refer recipients to phony Web sites set up to look like their legitimate counterparts.

plain text e-mail -- E-mail messages that do not contain formatting such as larger font-size headings, colored text, bold text, italicized text and graphics.

shorthand – This refers to using uppercase letters, representing the initial letters of words, to create a shortcut version of a common phrase. BTW is “by the way”, TTFN is “ta-ta for now”, FYI is “for your information” and IMHO is in “in my humble opinion”. Shorthand is also known as Internet slang or Internet acronyms. Shorthand is only useful if the recipient understands it.

shouting – An e-mail message with uppercase text is perceived as raising one’s voice above a respectable level. Shouting with capital letters should be avoided. Also, long passages of uppercase text are hard to read.

signature – This is the text placed at the end of a mail message to provide the reader with the author's contact information, favorite quote, special of the month, web site address and the like. The signature line is composed and placed into the e-mail software's signature file for automatic appending. In GroupWise click *Tools/Options/Environment/Signature* to create a signature.

spam – This is the unsolicited bulk e-mail or unsolicited commercial e-mail that clogs mailboxes and e-mail systems. It is the e-mail version of the junk mail you receive in your postal mailbox. Out of respect for Hormel’s canned pork product, SPAM, it is sometimes called UCE (unsolicited commercial e-mail).

spoofing -- The practice of changing the sender's name in an e-mail message so that it looks as if it came from another address. The most effective kind of spoofing uses addresses of people you know.

subscribe -- To join an e-mail list, either via a Web form or e-mail commands sent to a list server.

virus -- A malicious program or piece of code that disrupts workstations, servers and networks. Viruses are often delivered via an e-mail attachment.

Web-based e-mail -- Web-based e-mail lets you read your e-mail within a browser such as Internet Explorer. GroupWise WebAccess is Web-based e-mail, as is Hotmail and Yahoo! Mail.

worm -- A piece of malicious code, often delivered via an attachment in e-mail or over a computer network. Unlike a virus, a worm has the ability to infect other computers without human assistance. Two worms, naive and blaster, infected our network in December 2003.

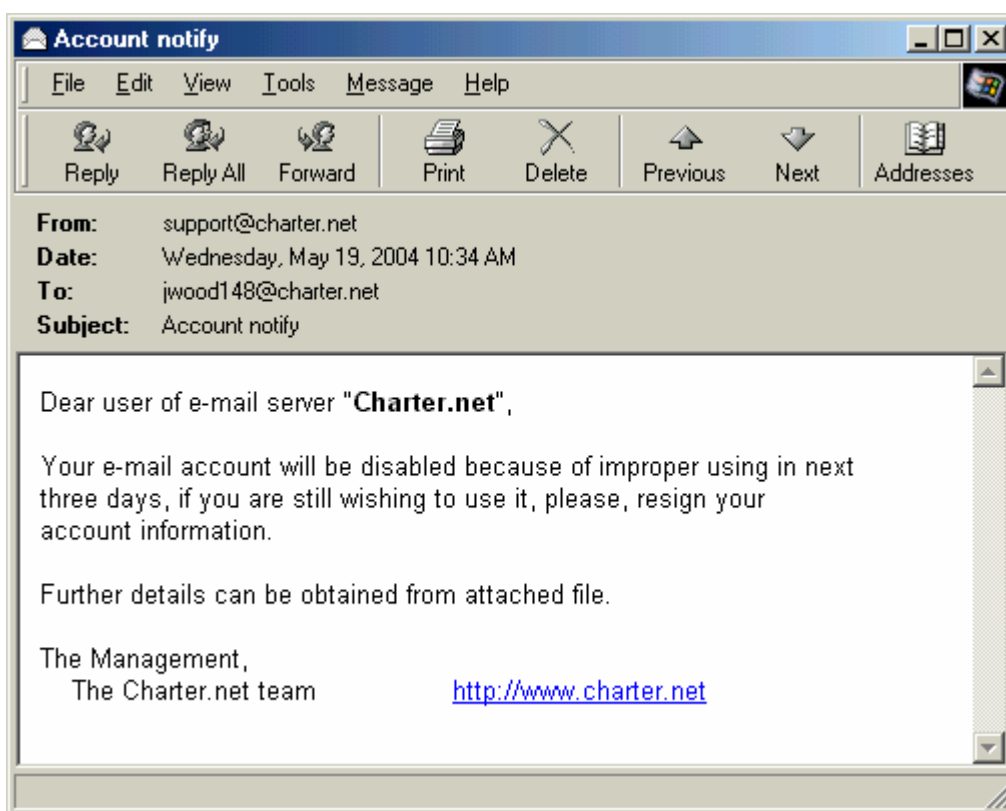
Below are examples of malicious e-mail

Spoof

This spoof targets people who have e-mail accounts with Charter Communications. The sender's goal is to persuade you to open the attached file, which contains a worm. Note the use of the www.charter.net web address, the legitimate web site for St. Louis-based Charter Communications. Also, notice the sender claims to be e-mailing from support@charter.net.

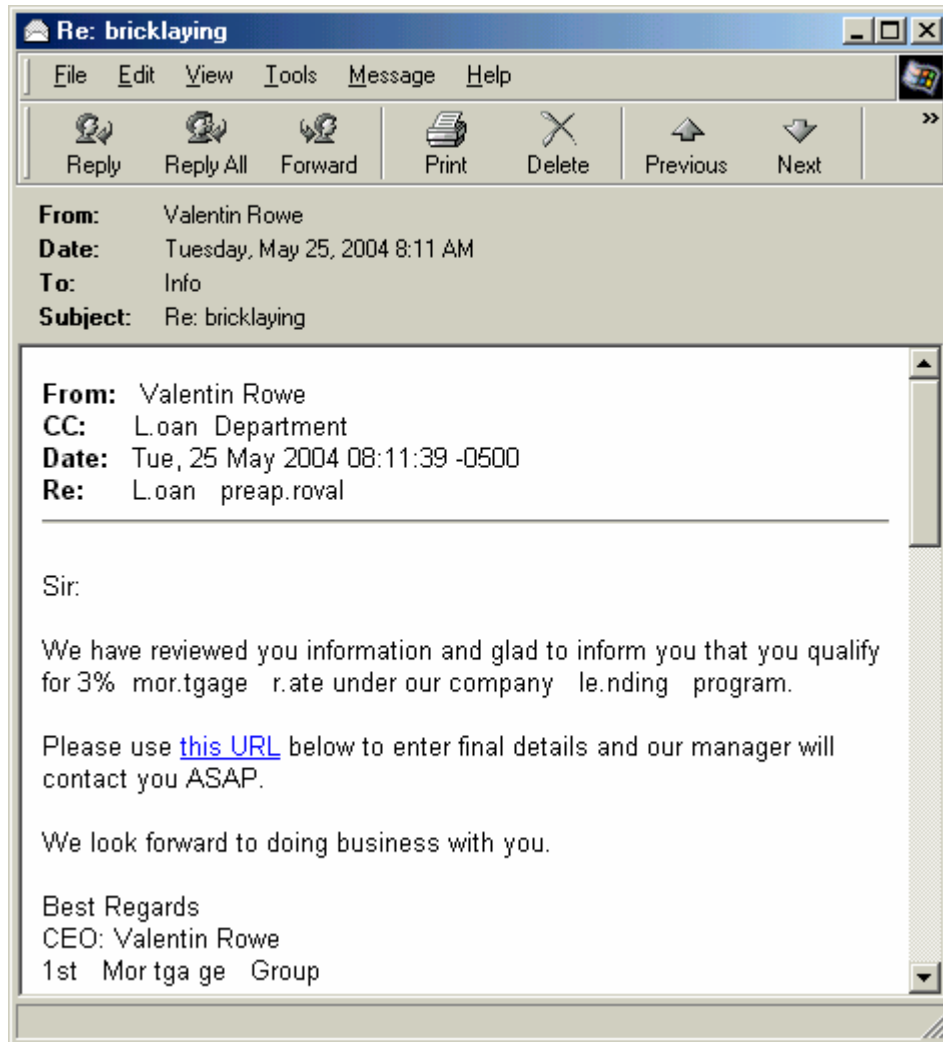
So, how do we know it's a spoof? The bad grammar and poor sentence structure in the body of the message are clear signs of spoofing. Multi-billion dollar corporations do not send e-mail this poorly written. The best evidence is from Charter, however. On 3/3/04 Charter disavowed all e-mail purporting to come from support@charter.net, explaining that the address was being used to spread the Bagle.k and/or Beagle.k worms.

Lesson: If you receive "official looking" e-mail asking you to do something, check the company's web site for spoof alerts or hoax alerts before acting.



Spam

Unscrupulous e-mail marketers work vigorously to stay a step ahead of anti-spam software. In the example below, the spammer inserts periods and spaces into words likely to cause the message to be blocked. The periods and spaces may be enough to slip past the anti-spam software, but not enough to obscure the meaning of the message.

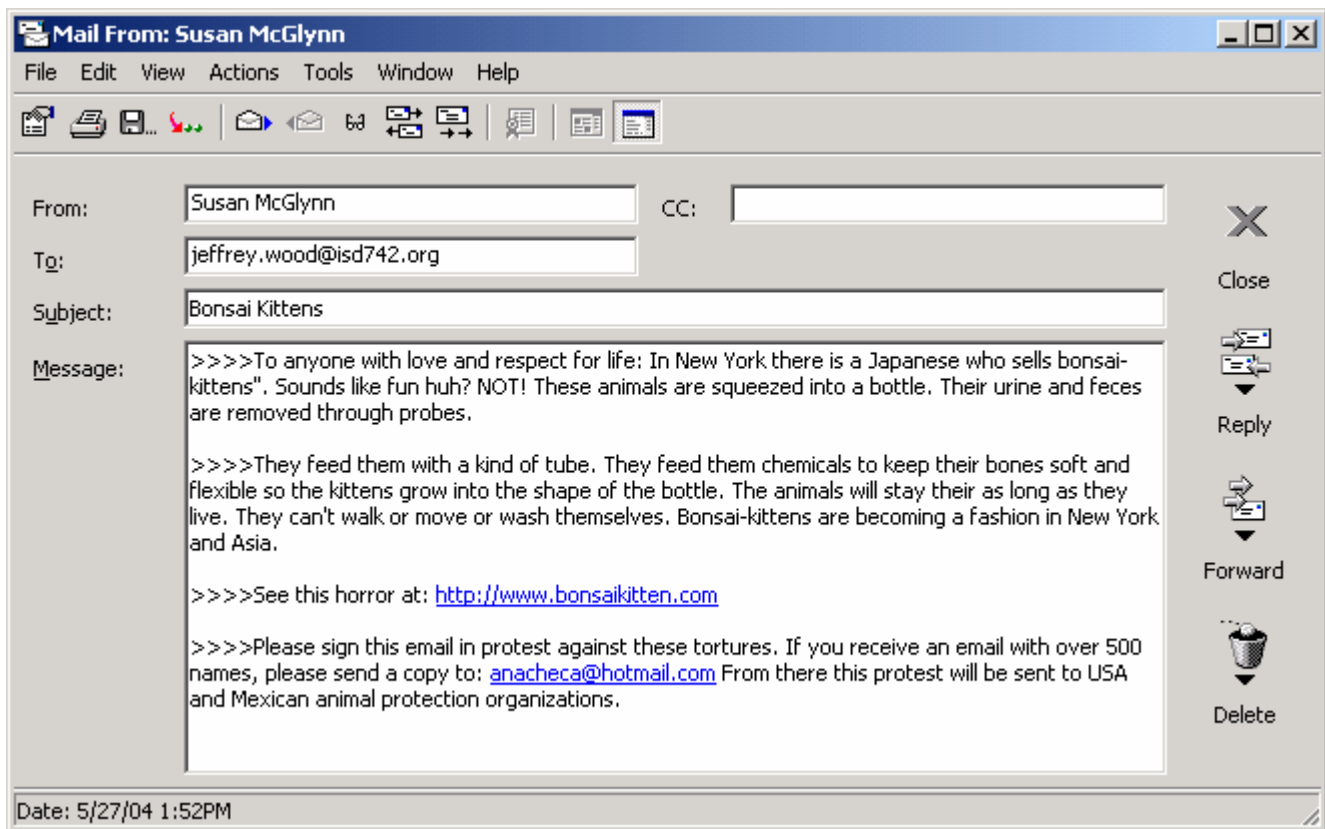


Glurge

Glurge – those forwarded e-mail that inspire or outrage us with distorted or false information – can appear amazingly authentic. The Bonsai Kittens glurge, below, describes how people stuff kittens into glass containers to warp their bodies into the shape of the container, training the kittens' bodies much like a gardener trains a bonsai tree. Lending authenticity to this glurge is an associated web site with photos of kittens stuffed into bottles. The photos are accompanied by detailed, technical descriptions.

Telltale signs of glurge:

- e-mail is unsigned but a cryptic e-mail address is provided
- emphatic language in upper-case text
- an associated hoax web site



This glurge warns us of the danger of boiling water in a microwave.

Hallmarks of glurge:

- the phrase “please pass this information on to friends and family”
- the e-mail is not signed
- the son, the doctor and the hospital are not named

