Security :: Spammers, Phishers, and How to Stop Them

Learn how to recognize spam and phishing [1] emails (yes, they are different), what their goal is, and how you can help keep them out of your - and everyone else's - inboxes. Read on for more about spam and phishing attacks. [2]

Email messages, however authentic they might look, may not be legitimate and may be spam or phishing [3]. What's the difference, and what can you do to keep them out of your inbox?

- **Spam emails** are usually trying to sell you something - products to improve your home, your sex life, your professional skills, your computer – or tempt you into some get-rich-quick scheme or store card worth $100. If no one ever responded, they would stop sending them, but because there's always someone who acts on these requests, they keep coming. It costs the spammer nothing to send the messages. The emails usually include a link to a website that may infect your machine with malware [4] and/or turn it into a “spambot”. This enables the spammer to use your machine to send their spam messages in the future. Spammers send spam because they get paid for every message they send.

- **Phishing emails** are far more serious, and often focused on specific targets (sometimes called spear phishing). Phishers are “fishing” for information – especially credit card and bank account numbers, user names and passwords, medical information, and the Holy Grail – Social Security numbers. Their primary goal is to trick you into revealing this information so that they can steal your identity, your money, your credit - or sell the information on the black market. Phishing emails usually masquerade as coming from somewhere familiar, like a bank or government agency, and lead you to a fake website that’s similar enough to the real thing so that you’ll trust it and volunteer information.

HSU users have been targeted by a number of phishing campaigns where the email claims to be from Information Technology Services or the Helpdesk or "webmail" group and requests that the recipient click on a link to update their information. These pages are hosted off-campus and can look almost identical to HSU's login pages. Sometimes, they claim that the recipient's information is out-of-date or that they have exceeded their email quota. HSU will never email you asking for your password.

If you have received a phishing message like this and entered your information, you need to call the Technology Help Desk. They will request that you change your password and personalized questions immediately to protect your identity. Contact information for the Technology Help Desk: 707-826-4357 (HELP).

Use this excellent step-by-step video [5] to assist in resetting your password (or HSU user name [6]) and personalized questions. Closed captioning is provided.

Learn more about spam and phishing. [7]

What you can do

Gmail [8] helps HSU to keep spam and phishing attempts off the network and out of everyone's inbox by

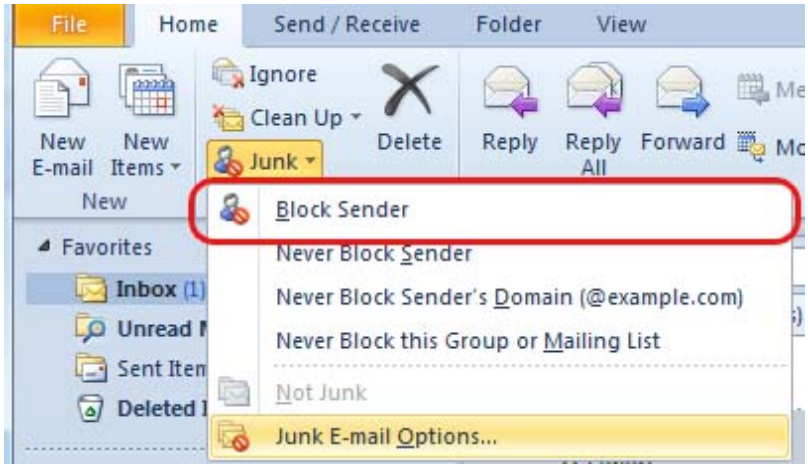
detecting and blocking most of it at the network perimeter, where the Internet meets the HSU network. But every so often, a particularly clever attempt will get past the filters. Here's what you should do if this happens:

1. If an offer looks too good to be true, it usually is. Never click on a link in one of these messages – including any Unsubscribe link (clicking on this just tells the spammer there's a live person at this email address).

2. If the message appears to come from someone you know, like your bank or the HSU helpdesk – call them and ask them. No reputable organization is going to request this kind of personally-identifiable information by email.

3. If you use Gmail as your email client, click on the reply down arrow (more) in the message and choose Report phishing [9] or Report spam [10]. You can also click on the exclamation point in the toolbar to report spam.

4. If you use Outlook as your email client, click on the Junk button in the toolbar (it's usually towards the left) and choose Block Sender.



Related Topics

Security [11]

Source URL: http://www2.humboldt.edu/its/security-spam

Links:
[1] http://www2.humboldt.edu/its/glossary/5#term202
[2] http://www.humboldt.edu/its/security-spam
[3] http://support.google.com/mail/bin/answer.py?answer=8253
[4] http://www2.humboldt.edu/its/glossary/5#term200
[5] http://www.humboldt.edu/its/resetting-your-password
[6] http://www2.humboldt.edu/its/glossary/5#term99
[7] https://www.humboldt.edu/its/security-phishing
[8] http://www2.humboldt.edu/its/glossary/5#term195
[9] http://support.google.com/mail/bin/answer.py?answer=184963
[10] http://support.google.com/mail/bin/answer.py?hl=en&answer=190737
[11] http://www2.humboldt.edu/its/category/quicklinks/security