Spam

SPAM

Email spam, also known as unsolicited commercial email (UCE) or unsolicited bulk email (UBE), is unwanted email messages usually urging the recipient to commercially benefit the sender in some way. It is a common and frustrating side effect to using email; the electronic version of the "junk mail" delivered by the post service. Often the spam links to sites attempting to sell goods of questionable legality or push unwise investment opportunities.

First of all, the biggest security risk from spam comes from actually doing what the message suggests. Do not purchase products pushed by spam. Often the goods are not of the quality implied by the message and sometimes can be dangerous. Especially beware of pharmaceuticals or other medical products that can cause serious injury or even death. When you get a spam message, delete it. Providing spammers with your personal information puts you at risks covered in our phishing section [1]. Certainly, spam and phishing are related issues.

UNI employs an email filter, commonly referred to as IronMail [2], that deletes computer-harming virus content and quarantines messages suspected of being spam. Typically, an insignificant number of spam messages get through IronMail. If a message that is spam or UCE gets through IronMail, it is usually best to simply ignore it and delete it.

Best Practice

- If the sender of a message is unknown to you (unverified) and/or the subject line of the email is offensive or unknown, immediately delete the email message. Opening the email may prove more offensive then the subject line.
- Do not respond or unsubscribe to an "opt-out" email address and/or link or sender asking to be removed from the list UNLESS the message comes from a company or organization you recognize and trust. Responding or asking to unsubscribe from a list is often a ploy by the spammers to verify your email address. Once email addresses are verified the spammers generate a known list of users that they sell for profit or for further spamming activities.
- Do not click links in unsolicited email nor trust their content to make any decision whatsoever.
- Avoid unnecessarily publicizing your UNI email address. You increase your chances of being spammed the more your email is seen on public bulletin boards, newsgroups, and chat rooms.
- Finally, and most importantly, if you receive email that is threatening or could potentially cause physical harm immediately contact your local law enforcement agency to file a report with the information that you have, including the email message and email header. Information on how to locate header information of an email message can be found in your client email help file.

Frequently Asked Questions Regarding Spam

What should I do when I get a spam message?

Delete the message. Do not click any links or reply to the message. This can only make things worse and expose you and your computer to untold danger.

How did they get my email address?

Spammers have computers programs that search the Internet for addresses listed on web pages. They purchase lists from less-reputable companies you may have done business with. They monitor as many web communications as they can. Sometimes, they even try every common email address that is possible. Spammers are very cleaver at getting your email address, so it is best to assume that the spammers will get your email address and send you unwanted messages.

What if I'm receiving email I do not want from a reputable source?

If you receive email that you do not want that appears to come from a reputable source, it should contain a link towards the bottom of the message containing instructions to unsubscribe from the email list. Be careful, some spammers also include unsubscribe links to help determine if an address is being actively used and checked. The best practice is to only unsubscribe from email lists originating from sources to which you believe you provided your email address.

Do email spam filters work?

Yes. No system is perfect and inevitably some spam will get past the filter and some rare emails that are not spam may be filtered. IronMail typically filters out 90-95% of the messages that are presented for delivery on any given day.

Who provides spam filters?

Most free email address accounts now offer some sort of spam filtering. Many Internet service providers also provide email spam filtering for their addresses. While products to deal with excess spam do exist, its probably easier for the average user to switch to a free email address that provides spam filtering then to purchase a commercial product to integrate into their email client.

How do I limit my exposure to spam?

The best way to limit spam is to limit the exposure of your email address. Do not post your email addresses needlessly on the Internet and do not share them with companies without a justifiable reason. Consider opening a second email account at a free email provider to post on the Internet and to provide to businesses so unwanted email does not clog up your primary inbox. Additionally, when submitting your email address online, look for default options or settings that might sign you up for unwanted email. Disable those options and consider not doing business with such entities. Further, do not click links in spam messages. In many cases, this confirms to the spammers that your email address is live and actively checked.

Are the products and services touted by spam really dangerous?

Often yes. Investment opportunities received via spam are often attempting to temporarily inflate the value of a given stock in order for the spammers to sell their stock at a higher value then it was purchased at. The stock will than typically recover and the investors who purchased at the request of the spam will loose money. Anything requesting you pay up front in order to receive additional money is a scam and you will certainly lose money. Products sold by the spammers are often counterfeit or stolen goods. Providing the spammers with your credit card or bank account details can often lead to fraudulent charges on your accounts. Pharmaceuticals sold by spammers may not contain any useful drug or may contain dangerous drugs not even approved for use in humans!

Remember:

- If it sounds too good to be true, it probably is.

- Few things in life are really free. Be suspicious of any unsolicited email offering you "free" goods or services. There is always a catch.
- Nothing in a bottle will safely make any part of your anatomy, male or female, larger or more attractive to the opposite sex.
- You did not win that contest or lottery you never entered.
- There is no person at this unusual site who wants to show you their "hot" pics.
- It's probably a bad idea to view porn touted by spam messages. Remember, you cannot "un-see" anything.
- No foreign prince has randomly chosen you to protect his money. This is an advance-fee fraud [3].
- You should not have to pay up front to receive an inheritance. Further, such notices should be delivered by regular mail, not email. This is another advance-fee fraud [3].
- There is no easy way to make money from home that is going to arrive unannounced in your email.
- Consolidating your debt may be a good idea for you, but never trust a source that arrives in email to provide you with such services.
- You really cannot settle your IRS debt for pennies on the dollar.
- If you do not know the sender, should you really trust them?

Why is unwanted email called spam?

Spam is a slang term for unsolicited commercial email. A popular theory is that the term originates from a 1970's Monty Python skit. The word "SPAM" constantly drowned out other conversation in the skit. Hormel foods, the maker of the SPAM food product, wishes the food SPAM to be in all uppercase and the email spam in all lowercase. SPAM is still a trademark of Hormel foods, so when referring to the unwanted email, it should not be in all uppercase. See http://www.spam.com/about/internet.aspx [4] for more information.

If email is blocked by the IronMail can it be retrieved?

If the message contained dangerous viral content, it was immediately discarded. Most other emails still exist. Contact the help desk for questions at 3-5555.

How does IronMail handle viruses and worms in email?

It deletes them immediately. No matter what the settings on an individual account, emails known to contain malicious code are deleted by IronMail and cannot be recovered.

I have not received an email I am expecting. How can I check for it?

Check your quarantined message notifications for the message. However, messages from individuals are rarely quarantined. Keep in mind the system only sends out notifications once daily.

If not quarantined, there are still plenty of other possibilities. Often the sender made a mistake typing your address or there is a problem with their email sending server. Sometimes servers do not send out the message promptly or it could be queued for delivery somewhere. There may be a general problem on the Internet. Sometimes emails just disappear without the intervention of any of our systems.

Source URL: http://www.uni.edu/its/support/article/575

Links:

[1] http://www.uni.edu/its/services/security/phishing
[2] http://www.uni.edu/its/support/article/574
[3] http://en.wikipedia.org/wiki/Advance_fee_fraud
[4] http://www.spam.com/about/internet.aspx