

# Avoiding Email Scams

**Tuesday, April 15 2008 @ 06:43 AM EDT**

Unsolicited commercial email, or "spam," is the starting point for many email scams. Before the advent of email, scammers had to contact each potential victim individually by post, fax, telephone, or through direct personal contact. These methods would often require a significant investment in time and money. To improve the chances of contacting susceptible victims, the scammer might have had to do advance research on the "marks" he or she targeted.

Email has changed the game for scammers. The convenience and anonymity of email, along with the capability it provides for easily contacting thousands of people at once, enables scammers to work in volume. Scammers only need to fool a small percentage of the tens of thousands of people they email for their ruse to pay off.

The following recommendations can minimize your chances of falling victim to an email scam:

- Filter spam.
- Don't trust unsolicited email.
- Treat email attachments with caution.
- Install anti-virus software and keep it up to date.
- Install a personal firewall and keep it up to date.
- Configure your email client for security.

## **Filter Spam**

Because most email scams begin with unsolicited commercial email, you should take measures to prevent spam from getting into your mailbox. Most email applications and web mail services include spam-filtering features, or ways in which you can configure your email applications to filter spam. Consult the help file for your email application or service to find out what you must do to filter spam.

You may not be able to eliminate all spam, but filtering will keep a great deal of it from reaching your mailbox. You should be aware that spammers monitor spam filtering tools and software and take measures to elude them. For instance, spammers may use subtle spelling mistakes to subvert spam filters, changing "Potency Pills" to "Potençy Pills."

## **Don't Trust Unsolicited Email**

Don't automatically trust any email sent to you by an unknown individual or organization. Never open an attachment to unsolicited email. Most importantly, never click on a link sent to you in an email. Cleverly crafted links can take you to forged web sites set up to trick you into divulging private information or downloading viruses, spyware, and other malicious software.

Spammers may also use a technique in which they send unique links in each individual spam email. Victim 1 may receive an email with the link 'http://dfnasdunf.exemple.org/', while victim 2 may receive the same spam email with the link 'http://vnbnnasd.exaple.org/'. By watching which links are requested on their web servers, spammers can figure out which email addresses are valid and more precisely target victims for repeat spam attempts.

Remember that even email sent from a familiar address may create problems. Many viruses spread themselves by scanning the victim computer for email addresses and sending themselves to these addresses in the guise of an email from the owner of the infected computer.

## **Treat Email Attachments With Caution**

Email attachments are commonly used by online scammers to sneak a virus on to your computer. These viruses can help the scammer steal important information from your computer, compromise your computer so that it is open to further attack and abuse, and convert your computer into a 'bot' for use in denial-of-service attacks and other online crimes. A familiar "from" address is no guarantee of safety because some viruses spread by first searching for all email

addresses on an infected computer and then sending itself to these addresses. It could be your friend's computer is infected with just such a virus.

### **Install Anti-virus Software and Keep It Up To Date**

If you haven't done so by now, you should install anti-virus software on your computer. If possible, you should install an anti-virus program that has an automatic update feature. This will help ensure you always have the most up-to-date protection possible against viruses. In addition, you should make sure the anti-virus software you choose includes an email scanning feature. This will help keep your computer free of email-born viruses.

### **Install a Personal Firewall and Keep It Up To Date**

A firewall will not prevent scam email from making its way in to your mailbox. However, it may help protect you should you inadvertently open a virus-bearing attachment or otherwise introduce malware to your computer by following the instructions in the email. The firewall, among other things, will help prevent outbound traffic from your computer to the attacker. When your personal firewall detects suspicious outbound communications from your computer, it could be a sign you have inadvertently installed malicious programs on your computer.

### **Configure Your Email Client for Security**

There are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as "text only" will help protect you from scams that misuse HTML in email.

Beyond the above recommendations, you need to use plain old common sense. When email arrives in your mailbox promising you big money for little effort, accusing you of violating the Patriot Act, or inviting you to join a plot to grab unclaimed funds involving persons you don't know in a country on the other side of the world, take a moment to consider the likelihood that the email is legitimate.

---

Note: This article was produced and copyrighted by the US-CERT. This article was used with permission as stated in Terms of Use, Copyright Permission.

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

---

Posted by:  
Bobbette Fagel, CISA, CISM  
Vice President  
infotex

[0 comments](#)

---

<https://my.infotex.com/article.php?story=20080415064322856>