



E-mail Scams 101

by Sheriff Ted Mink

No one is immune from receiving e-mail scams. Scammers seem to think that if they cast a wide enough net, they will catch some unlucky victims ... and they do. E-mail scamming itself isn't new, but scammers are constantly thinking up new ways to trick victims out of their money or their identities. Here are some hard and fast rules for e-mail use that can help you stay safe.

1. Don't give an e-mail a second glance if you didn't contact the sender first.

Do not respond to any e-mails that you did not initiate. Some will pull at your heartstrings with pleas for help for someone who is ill. Some will tell you you've got a prize to collect. Others will go so far as to threaten your life and ask for ransom money. But unless the e-mail is personal and comes from someone you know, you can bet that hundreds of other people received the same e-mail, and that they're hoping you're going to take the bait. If you want to find out more about a business or nonprofit to see if they are legitimate, research them via the Better Business Bureau or the National Fraud Information Center.

2. Don't be fooled by a logo or professional looking graphics.

It might look like your bank's logo, and the e-mail might contain graphics that give it an "official" appearance, but the truth is, these elements can be easily copied or created by an amateur. Your bank will not contact you via e-mail to discuss "problems" with your account, nor will it request information from you via e-mail. If you distrust an e-mail you receive from your financial institution, contact your financial institution at the telephone number provided on your statement.

3. Do not give out any personal financial information via e-mail.

Whether you're communicating with a seller on Craigslist or eBay, or trying to respond to an "inquiry" from your bank or credit union, never provide financial information via e-mail. Never give bank account numbers, credit card numbers, social security numbers or any other financial information out over e-mail. Using your credit card to purchase via a reputable online store, like Amazon.com, is fine. Paying for something via PayPal or other secured transaction services is fine. E-mailing someone account numbers is never okay.

4. When in doubt, delete.

If you're still not sure whether an e-mail you've received is from a legitimate source, delete it. What's the worst thing that could happen if you delete a questionable e-mail? If the sender is a true associate of yours, they will have other means of contacting you, like mail or telephone.

5. Signs that an e-mail is probably a scam:

- You don't know the sender
- There are misspellings or grammatical errors
- The greeting is generic and does not use your name ("Hello, friend," "Dearest," etc.)
- The tone is urgent
- The e-mail contains a business proposal or suggests a transaction of some kind

If You Become a Victim

The reality is, many e-mail scams are extremely difficult to investigate, as many scam artists operate from outside the United States where our state and local laws do not apply. Many fraudulent online sites and e-mail addresses operate for only a few days before the operator packs up and moves on to a different site.

The best solution is prevention. Avoid scams through proper Internet safety practices. Should you fall victim to an Internet crime or have your identity stolen, report it to your local law enforcement agency right away. In addition, report Internet-related crimes to the Internet Crime Complaint Center (IC3).