

IDENTIFYING DANGEROUS EMAIL

by

Robert Drum, CISSP

You've heard of spam, the electronic equivalent of junk mail. You've heard news stories about destructive Internet worms and computer viruses. But did you know that your mother had the best advice for dealing with both of these problems? "Don't talk to strangers." It's a simple phrase meant to keep children safe from the unknown. Well cyberspace isn't so different from real-life that your mother's sage advice doesn't apply.

Think about your email inbox. Surely you get messages from people you've never heard of, with subject lines that cover everything from sexual enhancement products to random gibberish. Well your mother's admonition, "Don't talk to strangers," is particularly useful when dealing with such emails. Take a close look at the name and

subject line; if either seems odd, just go ahead and delete the email without reading it.

But sometimes it isn't easy to identify which emails belong in the trash, especially when you recognize the sender. There are common clues that can help you spot problem emails from simple spam to destructive viruses. The first, best clue is that such messages always arrive unexpectedly. But just being unexpected doesn't make an email dangerous, there are other clues to look for.

Who is that from?

Any emails that appear to be from you are suspicious. Unless you actually do send yourself emails, you shouldn't ever see your address in the From: line of a message in your inbox.

Usually, only folks with multiple email accounts send themselves messages. Most people can just assume that messages from their own address are bogus and just delete them. Be careful though, emails in your sent items folder will say they are from your address because they really are, you might want to keep them.

What does that say?

Another good clue to a potentially dangerous message is bad grammar. You should be suspicious of any message that is poorly written. Nigerian fraud messages are one common type of email that exhibit bad grammar. The basic Nigerian fraud scam is to promise a large sum of money to a potential victim who must first establish a bank account, with a substantial opening balance, where the ultimate jackpot will wind up. Unfortunately, the con artist who sent the message only makes withdrawals, leaving the victim with an empty account.

Another new trend is for spammers to put random words in the subject line of their emails. "Encomia grit danube fjord nosebag," is a subject line I found in my inbox not long ago that turned out to be an ad for a breast augmentation product. Just remember, gibberish means junk, and junk belongs in the trash.

What do you want?

If an email asks you for something: money, personal information, passwords, or other sensitive information, it is almost always a fake. If you think the email is genuine, contact the sender by phone. If you don't have a phone number for the sender you shouldn't be sending them sensitive information anyway.

Some emails that request information are designed to panic us into action. The most common form of this is a fake message supposedly from your Internet Service Provider (ISP) saying, "Your account has been used to send spam and will be disabled in three days." The email will then ask you to reply with your user name and password, or go to a web site where you can change your password.

Let's be clear, these messages are absolutely fake.

Your service provider will never ask you for your user name or password in an email. The folks sending these messages are just trying to get your credentials so they can hijack your account and use it to send spam or run some other scam.

Ooh, a picture!

The last thing to watch for is if the email suggests you open an attachment. Maybe it's a picture of Anna Kournikova, or a cute cartoon, or a document from a co-worker, it's probably a virus. Even up-to-date virus software won't protect you from a brand new virus, but deleting the message without opening the attachment will.

If you're concerned that the message is genuine, contact the sender and ask before you act. But even if you do delete a valid message it can always be re-sent.

Handling dangerous emails.

The basic course of action when dealing with emails you're not sure about is to delete them without opening them. Of course you can also contact the sender to check first.

But there is more that you can, and should, be doing. Run anti-virus software and keep it updated. Apply software patches for your operating system, email software, and Internet browser. And check your email software settings for attachments and previewing messages.

Anti-virus software isn't perfect but it does help. Try to find anti-virus software that works with your email software and make sure you download the virus definition updates religiously. Most companies release updates weekly, if you can, have your software get these updates automatically.

Operating system and browser vendors release security updates for their software frequently. Most current PC operating systems like Mac OS and Windows let you check for these updates automatically. For a personal PC this is usually a good idea, for a business PC you should check with your system administrator or IT guy first.

Finally, check your email software settings. Make sure it doesn't automatically open attachments. Saving attachments is OK if you scan them for viruses before you use them. And think twice about using a preview pane; emails containing malicious web content (embedded HTML) can damage your computer, even from a preview pane.