Don't Get Caught by the Newest Twists in E-Mail Scams

By FoolProof's Information Edge

Has your e-mail inbox had more spam in it lately? If so, you're not alone. In their never-ending siege on protective anti-spam filters, spammers are now using PDF (portable document format), Excel, and Word documents to try to scam you and steal your personal and financial information. And there are more new tricks. Your best defense is knowledge of their tactics. This month's report, looks at the latest scams now showing up in inboxes across the country.

More Sophisticated Phishing Scams

Phishing scams are getting more sophisticated. These scams directly target stealing your financial information by faking a legitimate site, such as a financial institution or retailer you might do business with. The newest phish emails appear very business-like without spelling or grammatical errors and may include the recipient's correct name within the subject line or the body of the message. Examples of these phish include fake Better Business Bureau complaint messages, IRS audit warnings, and false business invoices—by faking organizations you would normally trust, the thieves are trying to sneak by your defenses. They also avoid a popular phishing tactic many people have learned to avoid: Instead of directing the recipient to a fake website in order to steal personal and financial information, these messages may have a Word document that contains a link. Clicking on the link may cause malware to be installed on your computer which will attempt to steal personal and financial data.

In another twist, phishers are using electronic greeting cards to steal personal and financial information. The e-greeting may have malware as an attachment or a link to a site that will try to install malware on your computer. The malware will attempt to steal personal and financial data. These greetings are usually easy to spot because the message is generic – the sender's name is not mentioned in the subject line or in the body of the message. Legitimate e-greetings mention the sender by name and greet the recipient by name.

Pump-and-Dump Scams

This classic "get-rich-quick " investment scam has moved online with scammers using e-mail messages to tout a "hot stock." Many people act on the so-called tip and buy the stock, thus pumping up the price. But when the scammers sell their shares (dump) and stop hyping the stock, the price plummets and many of the people who bought shares lose their money. Spam using images has been the most popular method for these scammers. But spam filters have gotten better at filtering out image spam, so scammers are now using PDF and Excel documents. Most spam filters can't read a PDF file.

Charitable Contribution Scams

These scams usually appear whenever a disaster or tragedy occurs. These messages ask for donations to help the victims or their families. Legitimate charities don't ask for donations by unsolicited e-mail. Always check out a charity before donating.

Another Twist

Some scammers try to make you think the message is real by borrowing pictures, logos, seals, and banners from legitimate organizations, businesses, and groups. For example, a number of fake FBI scam e-mails are using the picture of the director of the FBI.

Tips for Avoiding These and Other Scams:

Don't open attachments unless you are expecting them. Even if you know the sender but weren't expecting the attachment, check that they sent it before opening it.

Don't click on links in suspect e-mail messages. Don't click on links in e-mails that ask for personal information, account numbers, user names or passwords. These links may take you to fake sites to collect your personal or financial information or to sites that will try to install malware on your computer. Even if you think the e-mail is legitimate, don't click on the link in the message, go to the site using a bookmark or by typing in the address yourself. Remember financial institutions and most businesses never use unsolicited email to request or “verify” this type of information.

Make sure the full file name is displayed for attachments. Some malicious messages take advantage of hidden file extensions. For example, a fake Word document may have a full filename of name.doc.exe. The .exe makes the file a program not a text document. Opening the file will cause it to run, possibly installing malware on your computer.

Protect your computer. Install and keep updated antivirus and antispyware programs. Use a firewall and spam filters. For even more security, turn off your computer when not in use. Keep your browser and operating system updated.

Don't download software – especially free software – without thoroughly checking it out. Don't automatically click Ok, if a site asks to install software on your computer. Make sure you understand exact what the software is supposed to do. Read the entire end-user-license agreement (EULA) because sometimes the most important disclosures are at the very end of the agreement.

For More Information

Botnet and Hackers and Spam (Oh, My!) from the FTC provides tips on protecting your computer and your personal information from hackers and spammers.
[http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm]

Pump&Dump.com: Tips for Avoiding Stock Scams on the Internet from the U.S. Securities and Exchange Commission
[http://www.sec.gov/investor/pubs/pump.htm]

New spam alert: PDF attachments from the Credit Union National Association
[http://www.creditunion.coop/news/story.php?id=32165]

LooksTooGoodToBeTrue.com
This site is maintained by a joint federal law enforcement and industry task force including the U.S. Postal Inspection Service and the FBI.
[http://www.lookstoogoodtobetrue.com/]

Spyware from the FTC
[http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.shtm]