

Making sure your e-mail does not compromise your computer's safety

Hackers, phishers, viruses, worms...simply having your computer online can expose your data and personal information to all kinds of malicious and worrisome problems. If you're somewhat new to the 'net' or to computers in general, these four tips could help protect you from identity theft, credit card fraud, or a complete computer takeover – all of which can happen without you even knowing about it!

1. What's in Your Inbox? – If your e-mail program allows you to preview the entire message before or while it is being downloaded, turn this setting off. Some e-mails can contain dangerous code that could unknowingly compromise your computer and leave you vulnerable to viruses, worms or worse! Check the options in your e-mail program for a way to disable the message preview pane.

2. Scrutinize Your Messages – Don't ever respond to messages claiming to be from your bank, credit card company, or other financial institution, which ask for personally identifiable information such as card or account numbers, passwords, or other private information – even if the e-mail looks to have come from the actual company. It may be a hoax designed to get you to unknowingly part with crucial financial or private contact information, leaving you vulnerable to credit card fraud, identity theft or credit card theft. Contact the institution or company that claims to be sending the e-mail and verify the contents of the message with them. Chances are – they never sent it. Only use the number on your statement though, and not the number that appears in the e-mail message. It may direct you right to the scammer, who will do everything they can to assure you that nothing is wrong!

3. If it's From a Friend, it must be Safe, Right? – It's logical to assume that a message from your friend or colleague is safe, but that isn't always the case! If you receive an email from a friend or colleague which contains an attachment (could be a media clip, a screensaver, a picture or anything else), call them up to check and see if they really did send it. Many viruses and worms can hijack your computer and blast out a virus-ridden email to everyone in your address book, making it appear that it came from you and therefore, making it appear trustworthy.

4. Read Your Messages in Plain Text – Some e-mails written in HTML (the coding language that makes up many web pages) can be harmless. Others can contain malicious code that can hijack your e-mail program, browser, or your entire computer – and send your personal and financial information out to a hacker or scammer without you even knowing about it! Stay safe by setting your e-mail program to only show messages in plain text format (often in the options or settings section of the software). This will prevent threatening code from installing itself and compromising your system and private information.

Possibly one of the best ways to protect your e-mail is simply by exercising common sense. The Internet is a lot like a crowded plaza. Would your banker or credit card lender walk out into the middle of the throng of people and shout out to you to ask for your account information? Would you tell him where everyone could hear? Definitely not! The same caution should be exercised when checking your e-mail. These tips can help you stop scammers dead in their tracks while keeping you from becoming another victim of fraud or theft.

About the Author

Did you find this article useful? For more useful tips and hints, points to ponder and keep in mind, techniques, and insights pertaining to computer tips, do please browse for more information at our websites. www.infozabout.com www.internet.infozabout.com

Source: <http://www.zogol.com>