How to Spot Malicious Emails

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

Spammers send out billions of spam messages every day. These messages often get flagged by spam filters, and many users routinely discard these annoying messages on a regular basis. Malicious emails can still get by even the most advanced spam filter systems, however. It is these malicious emails that you should be concerned about.

Malicious emails are one way that hackers try to get access to your private information. If you receive a spam email, you should delete it immediately—do not open any attachments or click any links. It only takes one wrong click, and hackers can gain access to your entire computer. The tips below will help you better protect yourself when using email.

Phishing emails are one type of email scam. Phishing emails appear to come from legitimate sources and aim to get you to download a malicious file, click a malicious link, or provide your personal information. These messages often use alarming, outrageous, or tempting language designed to get you to respond quickly without thinking.

Tips to Avoid Malicious Emails

Check Email Sender

Scammers often send emails from email addresses that appear to be legitimate. Spammers sometimes create email addresses where numbers have been substituted for letters (for example, "*irs-service@IRS.GOV*" compared to "*irs-service@IRS.G0V*", where the letter "O" has been substituted with the number "0"). You should always review the sender email address to ensure it is valid. In the example above, you should never expect to receive email notifications from the Internal Revenue Service about tax refunds. Pay close attention to messages that come from unknown senders.

Review Hyperlinks

Hyperlinks or links allow users to click and navigate to specific websites. There are two parts to a link—(1) what is displayed and (2) where the link actually takes you. Spammers often make links appear legitimate. But the links can take you to malicious websites. To avoid accessing a malicious site, know where the link will take you before clicking. To do this, move your mouse over the link. Your screen will show you where the link will actually take you when you click it. Use caution with links that contain numbers, misspellings, or odd text. For example, the link "*www.website.com/1482197/pl2mia8hw573nzzbv71i0f29y3uxj9.zip*" points to a file that contains malware. When in doubt, perform your own search, or contact the company directly, instead of clicking the link.

Look for Grammar and Spelling Errors

Spammers are getting smarter when crafting malicious emails. But many messages are still riddled with grammar and spelling mistakes. Read the subject line and first few sentences of the email to determine if the email uses broken language or text not related to the purpose of the email. Here is an example of misspellings in a real malicious email: "Confrm your email by filling out your Login Infromation below or your account will be suspended within 24 hours for security reasons." Other examples of messages with broken language include "Verify your account now to avoid it closed!!!" and "Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently." You should delete these messages immediately and avoid clicking links and downloading files that are attached to them.

Enable Two-Factor Authentication

Usernames and passwords are hacked every day and sold in underground cyber markets. To strengthen your accounts, you should enable two-factor authentication for all your financial and email accounts. In addition to your username and password, you will also be required to provide a PIN, which is typically valid for one minute. This added layer helps protect your account in the event your username and password are stolen by hackers. This is not enabled by default on your accounts. Most companies allow you to enable this feature through your account settings. If not, contact the company directly to determine if two-factor authentication is available.