How to tell if an e-mail is a scam

E-mails come in many forms, and it sometimes can be difficult to tell the difference between a genuine message and a scam. Here are some of the many indicators that the e-mail you've received is fraudulent.

Incomplete/misspelled words

One of the indications of a scam e-mail is poor spelling, grammar, or punctuation. E-mails coming from professional organizations and companies are highly unlikely to contain any of these mistakes. Scam e-mails, on the other hand, are often written by individuals who may not have strong spelling or grammatical skills, or are writing in a rushed fashion. If you receive an e-mail that appears to be from a legitimate company, but has spelling or grammar mistakes, it is probably a scam and should be deleted.

Requires immediate action

If the e-mail requires immediate action, a good practice is to call the company directly and inquire whether or not the message is legitimate. The customer service department should be able to look up your account and determine if any action is required, especially action related to the e-mail you received.

Request to enter personal information

Some e-mails are designed to capture, or steal, a user's login credentials for a particular website. These e-mails often include a request for a user to submit some sort of personal information or login credentials via e-mail to access or verify an issue with their account. If an e-mail you receive asks for any of this information, be wary as it can be a sign of a scam.

Tip: Most legitimate businesses will ask you to visit their site and log in to your account, rather than requesting the information by e-mail.

Addressed to a username

Writers of fraudulent e-mail have varying degrees of information about the recipient, sometimes none aside from their e-mail address and username. Legitimate companies generally start an e-mail by addressing the recipient by their full name. Many times point of a scam e-mails is to gain personal information about the user, so it may use something more generic, like "Dear Sir" or "Dear Madam."

Tip: Any e-mail that does not give specifics is one sign of a phishing e-mail.

Check the web page link

One of the most commonly used tools of scammers is a web page link. A deceptive e-mail may contain a link to a bogus website that they'll use to capture whatever you type on that web page, allow them access to your account or information. To combat this, you can check the link in your e-mail before clicking it.

One way to inspect a link is to place your mouse cursor over the link, but refrain from clicking on it. At the bottom of your e-mail program or browser in the status bar, you should be able to see the actual website address. Inspection of the link should indicate whether or not the like is to the companies actual website.

You can also right-click on the link in the e-mail, choose the "Copy Link Location" or similar option in the pop-up menu, and then paste that link in a program like Microsoft Word. Copying the link allows you to view the entire

address for that link. Compare that link to the company's real website address and verify if they match or not.

In any of the above cases, if you feel the e-mail you have received is a scam, do not attempt to click on any links in the e-mail. Aside from trying to send you to a fraudulent website, it may also contain spyware which could be designed to capture and steal further information from your computer after the fact.