How to spot an Email Hoax - Guide to Recognizing Hoaxes

Spotting the latest email hoaxes may be easier than you think!

There are thousands of email hoaxes moving around the Internet at any given time. Some may be the latest email hoaxes around. Others may be mutated versions of hoax messages that have travelled the Internet for years. These email hoaxes cover a range of subject matter, including:

Supposedly free giveaways in exchange for forwarding emails.
Bogus virus alerts.
False appeals to help sick children.
Pointless petitions that lead nowhere and accomplish nothing.
Dire, and completely fictional, warnings about products, companies, government policies or coming events.

The good news is that, with a little bit of foreknowledge, email hoaxes are easy to detect. Hidden within the colorful prose of your average email hoax often lurk telling indicators of the email's veracity.

Probably the most obvious of these indicators is a line such as "Send this email to everyone in your address book". Hoax writers want their material to spread as far and as fast as possible, so almost every hoax email will in some way exhort you to send it to other people. Some email hoaxes take a more targeted approach and suggest that you send the email to a specified number of people in order to collect a prize or realize a benefit.

Another indicator is that hoaxes tend not to provide checkable references to back up their spurious claims. Genuine competitions, promotions, giveaways or charity drives will usually provide a link to a company website or publication. Real virus warnings are likely to include a link to a reputable virus information website. Emails containing Government or company policy information are likely to include references to checkable sources such as news articles, websites or other publications.

A third indicator is often the actual language used. Email hoax writers have a tendency to use an emotive, "over-the-top" style of writing peppered with words and phrases such as "Urgent", "Danger", "worst ever virus!!", "sign now before it's too late" and so on, often rendered in ALL CAPITAL LETTERS for added emphasis. Paragraphs dripping with pathos speak of dying children; others "shout" with almost rabid excitement about free air travel or mobile phones. As well, some email hoaxes try to add credibility by using highly technical language.

Before forwarding an email, ask yourself these questions:

1. Does the email ask you to send it to a lot of other people?
2. Does the email fail to provide confirmation sources?
3. Is the language used overly emotive or highly technical?

A "yes" answer to one or more of the above questions, should start some alarm bells ringing. These indicators do not offer conclusive evidence that the email is a hoax but they are certainly enough to warrant further investigation before you hit the "Forward" Button.

Common Internet Scams - An Overview

Email and the Internet is a wonderful resource that has revolutionized the way humans communicate and access information. Unfortunately, it has also proved to be a fertile medium for the unscrupulous and the morally challenged. Scammers regularly use email in attempts to steal money or personal information from unsuspecting victims. Those inexperienced in the ways of the Internet are especially vulnerable to current Internet scams.

The good news is that it is not difficult to learn how to recognize current Internet scams that arrive via email. Included below are descriptions of three of the most common types of email driven scams as well as some general indicators that should help you recognize scam emails.

Phishing Scams:

You may receive an email from a bank/online service provider/ financial institution that asks you to click a link and visit a website in order to provide personal information. Such an email is more than likely the type of Internet scam known as "phishing".

A phishing scam is one in which victims are tricked into providing personal information such as account numbers and passwords to what they believe to be a legitimate company or organization. In order to carry out this trick, the scammers often create a "look-a-like" website that is designed to resemble the target company's official website. Typically, emails are used as "bait" in order to get the potential victim to visit the bogus website. Be wary of any email that asks you to click on a link and provide sensitive personal information such as banking details. Information submitted on these bogus websites is harvested by the scammers and may then be used to steal funds from the user's accounts and/or steal the victim's identity.

Most legitimate companies would not request sensitive information from customers via email. **DO NOT** click on the links in these emails. **DO NOT** provide any information about yourself. If you have any doubts at all about the veracity of an email, contact the company directly.

Nigerian Scams:

You may receive an email/letter/fax that asks for your help to access a large sum of money in a foreign bank account. The message says that you will get a percentage of the funds in exchange for your help.

In all probability, the message is an example of the type of scam known as a Nigerian or "419" scam. The "large sum of money" does not exist. The messages are an opening gambit designed to draw potential victims deeper into the scam. Those who initiate a dialogue with the scammers by replying to the scam messages will eventually be asked for advance fees supposedly required to allow the deal to proceed. They may also become the victims of identity theft. The scammers use a variety of stories to explain why they need your help to access the funds.

For example:

> They may claim that political climate or legal issues preclude them from accessing funds in a foreign bank account.
> They may claim that your last name is the same as that of the deceased person who owned the account and suggest that you act as the Next of Kin of this person in order to gain access to the funds.
> They may claim that a rich merchant, who has a terminal illness, needs your help to distribute his or her wealth to charity.

If you receive one of these scam emails, it is important that you do not respond to it in any way. The scammers are likely to act upon any response from those they see as potential victims.

Lottery Scams:

You may receive an email/letter/fax that claims that you have won a great deal of money in an international lottery even though you have never bought a ticket. The email may claim that your email address was randomly chosen out of a large pool of addresses as a "winning entry". Such emails are almost certainly fraudulent. In some cases, the emails claim to be endorsed by well-known companies such as Microsoft or include links to legitimate lottery organization websites. Any relationships implied by these endorsements and links will be completely bogus.

There is no lottery and no prize. Those who initiate a dialogue with the scammers by replying to the messages will be first asked to provide a great deal of personal information. Eventually, they will be asked to send money, ostensibly to cover expenses associated with delivery of the supposed "winnings". They may also become the victims of identity theft. DO NOT respond to these messages. DO NOT supply any personal information whatsoever to the scammers.

General Scam Indicators:

The current Internet scams described above are some of the most common types of Internet fraud. However, these fraudsters are clever people who may use many variations of the above scams to achieve their nefarious ends.

In general, be wary of unsolicited emails that:

Promise you money, jobs or prizes
Ask for donations
Propose lucrative business deals
Ask you to provide sensitive personal information
Ask you to follow a link to a website and log on to an account.

By taking the time to educate yourself about these common types of scam, and/or by sharing this information with others, you can make a valuable contribution to the war against Internet fraud.
