

Don't be caught out by hoaxes

As much good stuff as there is on the Internet, unfortunately there is even more bad stuff such as spam, viruses, scams, porn, crackers, hackers etc. Another one of the annoying things found in abundance online are hoaxes.

WHAT IS A HOAX?

A hoax is usually an e-mail you receive with a supposedly very important message, urging you to pass this info on to as many people as possible to make them aware of this info. However, the message is bogus and passing it on will accomplish nothing else but create unnecessary junk e-mail messages, very similar to chain letters. The only purpose of hoaxes is to waste your time and make you help generate junk Internet traffic.

Over the past few years hoaxes have become increasingly smarter and appear to be more legitimate in terms of even using respective logos. We have all seen them, "Please confirm your banking details" or "My father is held captive by the government and we have funds that we need to transfer into a bank account. Please act as our partner"

Hoaxes are similar to a virus. Think about the similarities:

- a virus is a malicious piece of code camouflaged as a harmless program or file - a hoax is a falsified message camouflaged as a fabricated story.
- a virus can spread over the Internet via e-mail - so does a hoax
- a virus interrupts productivity by interfering with your computer - a hoax interrupts productivity by making you waste time reading it and forwarding it, as well as bogging down e-mail servers around the globe

HOW DOES A HOAX WORK?

Here's the big difference between a virus and a hoax. Some viruses are malicious programs that spread themselves without your knowledge by e-mailing themselves to some or all people in your address book. But a hoax is not a program or script and therefore cannot replicate and spread itself – it requires your intervention. It has to be a lot more enticing. The hoax has to be convincing enough to make you believe it's true so that you spread the hoax yourself. This means a hoax not only wastes your time by making you read it, it also tries to manipulate you into acting upon it - spread the hoax and breed the cycle.

HOW TO IDENTIFY A HOAX

Any e-mail that asks you to forward it to as many people as possible is a hoax - period. I am yet to see a single e-mail asked to be forwarded that was legit. Any time you see a request to spread an e-mail - don't! Assume it's a hoax, don't bother reading on, just delete it and put an end to the cycle.

Every hoax only works if it can convince you that it is legit. They usually do that by claiming that this message comes from some type of authority, some well-known or at least very legitimate sounding organization such as banks. If the message was not sent to you directly from said authority, be suspicious, assume it's nonsense until you have verified its authenticity by, for example, visiting said authority's web site to see if it's mentioned there.



The subject of a hoax is usually one of the following categories:

- **a virus warning** - it describes some horrible new virus that spreads like wildfire and does horrible things to computers. You can easily verify them first by visiting the web site of a reputable virus software manufacturer; they maintain searchable databases where you can look up every virus known to mankind.
- **a scam** - it asks you to send something back, whether it's money, your ISP user name and password, credit card number and even your banking details and passwords etc.
- **an urban legend** - some incredible story of something that happened. If it sounds unbelievable, it usually is.
- **a give-away** - it claims that some big well-known company is giving away something for free based on how many times the e-mail is forwarded as it keeps track of how often the e-mail is sent.
- **a tear-jerker** - a very common hoax is a story of a person on his/her deathbed with the last wish of receiving tons of e-mail or cards, or somebody donating money for each e-mail sent towards research to cure the illness.
- **a regular chain letter** - the most common one is to send it on, otherwise you'll have bad luck. No matter how superstitious you are, this is absolute nonsense.
- **a get-rich-quick scheme** - somebody has the secret to getting rich quick, and they are sharing it the formula with everyone on the Internet.
- **dating scheme** – this is an incredibly “evil” hoax. These are people that create enormous, well thought through schemes using various dating sites to develop trust and entice an online romance. Once this has been achieved they will use various mechanisms to entice you to assist them financially.

WHAT TO DO WITH A HOAX E-MAIL

If you receive an e-mail that looks like a hoax, the best thing to do is to delete the message. Often a very simple verification can be done by checking the content against the senders email address. As an example if a bank sends you a mail asking you to confirm some details and it appears authentic with logo's and so on, beware, first they would not ask you to verify your details via mail and second the email address will not be that of the bank.

Another verification method is to simply Google the subject line of the email. Also take note that often public email addresses are used such as Gmail, Yahoo, Hotmail and Webmail. Naturally if you get a mail from a bank and the senders email address is hotmail.com; it is a hoax.

If none of the above methods reveals anything about the message you received, visit one of the hoax info web sites listed below. They maintain a searchable database where you can see if the message is bogus and report it too.

If all else fails, delete the message and move on. You have already wasted an hour.

Always ensure you have an Anti Virus tool that incorporates a SPAM function, this will reduce the volume of hoaxes you receive.

ANTI-HOAX LINKS

<http://www.hoaxbusters.org/>
<http://www.snopes.com/>
<http://www.hoax-slayer.com>
<http://www.truthorfiction.com>
<http://www.internethoaxes.info>

Written by: **Brian Smith, Managing Director, IN 2 IT**