Being digital

Scams and hoaxes

1: Introduction

Smith: I had an email the other day - it said if I click on the link I will get 3 million pounds.

Jones: Ooooh - what did you do?

Smith: Well, it was sent from someone important in the Russian government so I thought it was OK and followed the link.

Jones: So did you get your money?

Smith: No, unfortunately it took me to a website with dodgy software which planted a virus on my computer and sent emails to all my friends asking them to click on the same link.

Jones: Yes I know, I was one of the friends ...

Has anything like this ever happened to you? How can you know what is genuine and what is bogus?

Learning outcome

By the end of this activity you should be able to avoid getting taken in by email scams and hoaxes.

2: What do scams and hoaxes look like?

Read the message below, and think about what you would do if you received it.

"Dear Sir,

My name is Mr. Thomas Richard, a Fund Manager with Fidelity Investment, United Kingdom. One of the world's largest investment company. I have been the personal Fund Manager for the late Libyan President Muammar Gaddafi for many years. You may wish to visit the link to confirm. (http://www.guardian.co.uk/world/2011/oct/20/muammar-gaddafi-dies-city-birth-FI) Total sum of Fifteen Million, Seven Hundred and Forty Five Thousand British Pounds (15,745,000.00) GBP was invested on behalf of the late president of LIBYA under a SECRET CODE INVESTMENT where none of his personal information's was used for the investment. This is known between only both of us and not even the investment company has information's about the owner of the investment. Now that President Muammar Gaddafi is DEAD, I need a reliable and trustworthy person with whom I can work this deal out so that we can claim the funds as mentioned above. There is no risk attached and the funds in question can never be dictated or traced.

Sincerely,

Thomas Richard"

What would you do with this message?

a) I would click on the link

b) I would forward the message to all my friends to see if they would like a share of the money

c) I would delete the message, and ensure that I have a good spam filter installed in my email programme

d) I would reply to the sender asking them not to send me any more emails like this

(You will find the answer to this question, and feedback on all the options, in Appendix 1 on page 5.)

3: Be alert – ask the right questions

So far we have looked at an example of a hoax email. As well as being annoying, this kind of message can potentially lead to viruses or malware installing themselves on your computer if you click on any links. Replying to the message could open you up to further scams.

You may come across hoaxes on Facebook as well. For example, anything claiming that Facebook will donate $1 for each share of a post about a sick baby or similar is not true.

How can you spot a hoax? In the example you have just looked at, you may have had a gut instinct that something was wrong. Here are some of the signs:

- The **style of writing may be stilted**, with bad spelling and grammar and use of capitals or exclamation marks.
- The message may be **emotive and sensationalist**.
- It **may make demands** on you that you do not want to comply with - for example, following a link, forwarding the message on to others or providing your bank details.
- You **may have come across something like it before** that you know to be untrustworthy.

4: Staying safe

Steps to take

- Ensure your antivirus and spam filtering software is up-to-date.
- Next time someone forwards you a message you are not sure about, run it past your mental 'spam filter' to decide if it is trustworthy or not. This applies even if it comes from a friend - they may not have realised they are dealing with a hoax.
- Always be sceptical of any messages sent from individuals you do not know. Never click on links in messages where you do not know the sender.

For more advice on antivirus software and online security in general, visit either of these BBC Webwise sites: Five tips for avoiding email scams and How to stay secure on the web.

For a comprehensive overview of many different kinds of email and online hoaxes, visit the Hoax Slayer website. You might find it interesting to browse some of the different kinds of scams and hoaxes to see which you have come across. Did you realise they were not true at the time?

References

Being digital activity

Scams and hoaxes

Appendix 1: Answers and feedback

What do scams and hoaxes look like?

What would you do with the message you read on page 2?

The correct answer is c) "I would delete the message, and ensure that I have a good spam filter installed in my email programme".

Feedback on all the options is provided below.

a) I would click on the link

Feedback: This is a bad idea because links in hoax emails may take you to websites with viruses or malware, which can lodge themselves on your computer. It can also identify you and leave you vulnerable to future approaches.

b) I would forward the message to all my friends to see if they would like a share of the money

Feedback: This is a bad idea because if they are not aware it is a hoax they may get taken in, and if they are aware, they are likely to feel annoyed at having their time wasted with untrue information.

c) I would delete the message, and ensure that I have a good spam filter installed in my email programme

Feedback: Yes, this is the best thing to do. If you have good spam filtering, this kind of message may not get through to your inbox in the first place.

d) I would reply to the sender asking them not to send me any more emails like this

Feedback: This is not recommended. By replying you are identifying yourself to whoever is responsible and potentially opening yourself up to further deception and fraud.