Scams and hoaxes

1. Introduction

Online scams and hoaxes are a common occurrence in our digital lives. They can be spread in multiple ways including email, social media, phone call or text message. Spotting a scam quickly will keep your personal data safe, save you time and protect you against fraud.

This activity will focus on how to quickly spot email scams. The same skills can be applied to phone calls and text messages.

Learning outcomes

This activity will show you how to spot an email scam and how to deal with it.

2. Can you spot a scam

How good are you at spotting scams and hoaxes? Read the following email. Think about what you would do if you received it and then answer the multiple choice question.

Email

Dear Sir,

My name is Mr. Thomas Richard, a Fund Manager with Fidelity Investment, United Kingdom. I have been the personal Fund Manager for the late Libyan President Muammar Gaddafi for many years. To confirm visit link (http://www.guardian.co.uk/world/2011/oct/)

The Total sum of 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 to us only. 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.

Sincerely, Thomas Richard

Question

If you received this email what would be the best action to take?

1. Click on the link.
2. Forward the message to all my friends.
3. Delete the message and ensure that I have a good spam filter installed in my email client.
4. Reply to the sender asking them not to send me any more emails like this.

Feedback option 1

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.

Your answer is incorrect

Feedback option 2

Sharing hoaxes in this manner allows others to be taken in.

Your answer is incorrect

Feedback option 3

That's great. Removing the message removes the immediate threat. A good spam filter will help protect you against future attacks. Some companies ask that employees report phishing emails in a particular manner - you may wish to check if this is true of your workplace.

These types of emails have been ridiculed in much comedy in recent times. So it’s likely that you spotted this email as a spoof quickly. Others are harder to spot.

Your answer is correct!

Feedback option 4

By replying you are identifying yourself to whoever is responsible and potentially opening yourself up to further deception and fraud.

Your answer is incorrect

3. Can you spot a scam part 2

You have received this email. Do you think it’s genuine? Spend some time reflecting on why you feel that way. Read "our thoughts" when ready.

Email

From: PayPal pay.pal@notice-access-123.com

Subject: Urgent update action required

Dear PayPal Customer

We have noticed unexpected shopping activity from your account. We want to protect you, so we have temporarily restricted available account functionality for your peace of mind and security.

Don’t worry though restoring your Pay Pal account to its full glory is easy, it will take no time at all. To lift the restriction applied to your account go to https://paypaly.com/account-rupture, to avoid future disruption.

The PayPal team

Our thoughts

This email is not genuine. Seeing any of the following in an email should make you question the authenticity of the email.

- The email of the sender has the domain name “notice-access-123”. If the email was genuinely from PayPal the domain name (the text that appears after @) would feature the word PayPal i.e. @mail.PayPal or @PayPal.
- The email starts with an impersonal generic greeting, rather than the name of the account holder. This should make you question this email. If you already have a genuine email from a company, you can compare the greeting and format of the genuine email to one that you are unsure of.
- The company name is not formatted consistently in the email. If this email was genuine the company name would appear as one word throughout.
- The URL in this email has a couple of odd features. It starts PayPaly.com, this is similar to the legitimate PayPal web address but crucially it is not the same. The url ends with “account-rupture”, this is an odd phrase. “Account breach” is a common expression in English but not “account rupture”, even though rupture and breach can have a similar meaning. Not all scam emails are poorly written, but many are.
- You may have spotted that the url starts https. It is a misconception that all http: web address are unsafe and all https: addresses are safe. When you provide data to a https site the data is encrypted and therefore harder for a third party to intercept. Hence your data is more secure. However there is nothing to prevent a cybercriminal from registering their website for an SSL certificate and getting a https web address. An https link in this case simply means you can securely transfer your data to a cybercriminal without anyone else being able to get to your data.
- Scam emails will often have an urgent tone to them. Their aim is to get you to panic and act without thinking. This email has urgent in the subject, even though the text of the email is not urgent.

Scam emails can be hard to spot. If you are unsure an email has come from the company it pertains to be from, you can always check by contacting the company directly. The proliferation of scam emails does mean that legitimate companies will want to assist you in determining if a communication is genuine.

4. Scam spot Checklist

Hoax emails are annoying and can potentially lead to viruses or malware installing themselves on your computer if you click on any links.

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

- Who is the email really from? Check ‘from’ address, greeting, contact details and branding.
- Are you being asked to click on a link? Check if it is legitimate website. You can always use a search engine to look up part of the address.

- Does the email have poor or unusual spelling or grammar? Is the tone unusually official? Compare the email you have received with others from the same company. Ask yourself again who is this email really from?
- Are you being asked to do something quickly? Scam emails often try to cause panic to make the recipient act before thinking through their actions.
- Are you being asked for personal or bank details? Never provide usernames and passwords to an individual either by phone or email. This is simple, if anyone asks this it is a scam.
- Remember you can contact a company directly to check if a communication is genuine. (Which, 2020)

5. Capture and prevention

Once you have realised an email is a scam you need to remove it from your computer as soon as possible. Either delete from your computer or use the report message option if available in your email client. Using the report option will block the sender's email address from your inbox.

Prevention

To reduce the number of scam emails you receive ensure your antivirus, spam filter and malware software is up to date. If you have not already you may want to think about anti-virus software for your phone and or tablet.

5. Summary

Summary

We have looked at:

- Example scams
- How you can spot a scam
- What to do when you have spotted one
- How to reduce the number of scam emails you receive

Next Steps

This activity has concentrated on email scams. Sadly other media for scams are available. For more information check out these websites:

- The website Hoax Slayer reports on scams originating in email, Facebook and other media.
- Scam watch regularly reports on large scams.

- Who called me allows you to look up the phone number that called or sent you a text message. You are then given a rating which reflects the experience of others from said mobile phone number. If you have received a scam call or text message you can share your experience on this site to help others from becoming a victim to it.

References

Which (2020) How to spot an email scam. Available at:

https://www.which.co.uk/consumer-rights/advice/how-to-spot-an-email-scam (Accessed: 01 July 2020)