

Here is a great KnowBe4 resource that outlines 22 social engineering red flags commonly seen in phishing emails. We recommend printing out this PDF to pass along to family, friends, and coworkers.

Travis
1e 25.11.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micosoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com — the "n" is really two characters — "r" and "n".

DATE

- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4
Human error. Conquered.

Prevent Phishing Attacks:

Though hackers are constantly coming up with new techniques, there are some things that you can do to protect yourself and your organization:

- To protect against spam mails, spam filters can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it's spam. Occasionally, spam filters may even block emails from legitimate sources, so it isn't always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message is shown. The settings of the browser should only allow reliable websites to open up.
- Many websites require users to enter login information while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis, and never use the same password for multiple accounts. It's also a good idea for websites to use a CAPTCHA system for added security.