IDENTIFYING RED FLAGS

SOCIAL ENGINEERING

Think before you click

91% of successful breaches start with a phishing email. Human beings can become an organization's last layer of defense only when security awareness training demonstrates to them how susceptible they are to social engineering.

What to do

Always report any suspicious emails to your IT help desk and reach out to LMT for more information on our Security Awareness Training program to help you build your "human firewall."

From

- I don't recognize the sender's email address as someone I normally communicate with.
- This email is from someone outside my organization and is not related to my job responsibilities.
- This email is very unusual or out of character.
- The sender's email address is from a suspicious and misspelled domain (like micorsoft-support.com).
- 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.

Date

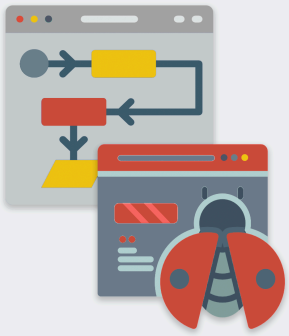
- I received an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.

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 well known site. For example, www.bankofarnerica.com – the "m" is really two characters – "r" and "n."

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, and does it have a sense of urgency?
- Top 5 Phishing Email Subjects:
  1. Password Check Required Immediately
  2. Your Order with Amazon.com/Your Amazon Order Receipt
  3. You Have Received 2 New Fax Messages
  4. UPS Label Deliver 1ZBE312TNIU1148452
  5. Last Reminder: Please Respond Immediately



Attachments

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message.
- The sender doesn't ordinarily send me this type of attachment or link, this could be a dropbox link, zip file, etc.
- I see an attachment with a possibly dangerous file type. Do NOT open any email attachments that end with: .exe, .scr, .bat, .com, or other executable files you do not recognize. The only file type that is 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 grammatical 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?

Key Takeway: The potential of something being wrong and/or at risk plays into the human psyche, leaving the individual to think that he/she must act immediately to resolve the issue. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

LMT TECHNOLOGY SOLUTIONS

4 Commercial St. Floor 4 | Rochester, NY 14614

(585) 784-7470
LMTnet.com