WHAT IS PHISHING?

August 2020
Bonsor 55+ Computer Group

What Is Phishing?

Attempt to obtain sensitive information, such as usernames, passwords and credit card details by someone posing as a person of authority or a legitimate institution.

Typically carried out over email, telephone (*vishing*) or text message (*smishing*).

Example of Email Phishing

Email from bank warning of suspicious card activity, asks you to click on a link in the message so as to verify your account.

The link in the message will connect you to a fraudulent website posing as the actual bank's site.

Bank of America

Security Alert
Debit card ending in xxx

Unusual debit card activity detected

Dear Customer,

We're letting you know that we detected unusual activity on your Bank of America debit card on 08/09/2018. For your protection, we need you to review this activity immediately.

Please sign in to Online Banking at www,bankofamerica,com/update to verify and updte your account activity After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

If you do not contact us, certain limitations may be placed on your debit card.

Please disregard this notice if you have already contacted us.

🔒 Your last sign-in

To verify that this email is from Bank of America, confirm your last sign-in date is correct. To access Online or Mobile Banking, go directly to bankofamerica.com or use our Mobile Banking App.

Example of PhoneText Phishing

Text message from income tax asking you to claim a refund. The link in message will connect you to a fake IRS website.

Your IRS tax refund is pending acceptance. Must accept within 24 hours: http://bit.ly/sdfsdf.

Example of Phone Call Phishing

Phone call from person claiming to be from a government agency, threatening you and asking for personal information.

DO NOT RELY ON CALLER ID!
Phone numbers can currently be spoofed easily!

Phishing Email Red Flags

Let us take a look at a typical phishing email and some of the common red flags associated with such an email.

PDF of image can viewed at:

https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf

Reference:

https://www.phishing.org/what-is-phishing
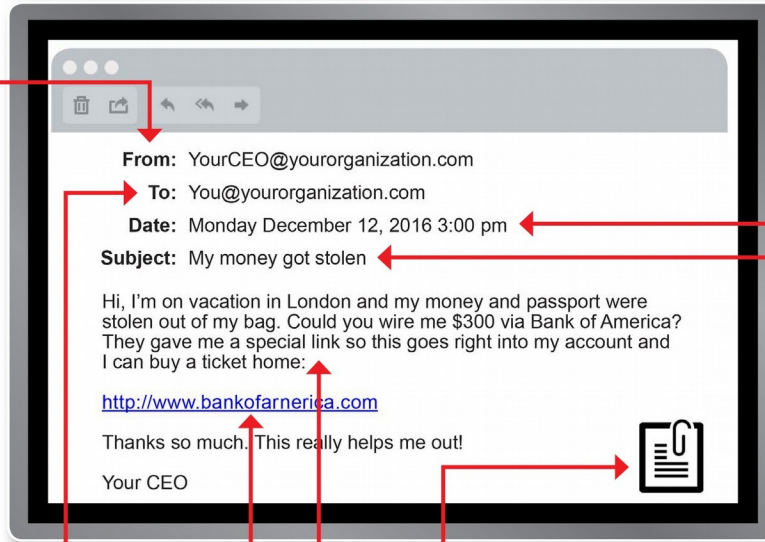
Social Engineering ▷ Red Flags

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 micorsoft-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.bankofarnerica.com — the "m" is really two characters — "r" and "n."

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

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?

KnowBe4
Human error. Conquered.

Finally ...

Any questions???