June 2018
Volume 13, Issue 6

How to Spot Phishing Messages Like a Pro

From the desk of Thomas F. Duffy, MS-ISAC Chair

The Federal Trade Commission’s definition of phishing is “when a scammer uses fraudulent emails or texts, or copycat websites, to get you to share valuable personal information.”[1] When a user falls for a phishing message, the malicious actor achieves their purpose of getting the victim to hand over sensitive information such as login names and passwords. Though we count on technologies and controls to minimize threats, phishing exploits users through social engineering, which allows the malicious actors to side step these protections. This is why it is important that everyone learn to spot these fraudulent messages. Let’s take a look at some example emails of phishing messages.

Message #1

Subject: Low Cost Dream Vacation loans!!!

Dear John,

We understand that money can be tight and you may not be able to afford to go on vacation this year. However, we have a solution. My company, World Bank and Trust is willing to offer low cost loans to get your through the vacation season. Interest rates are as low at 3% for 2 years. If you are interested in getting a loan, please fill out the attached contact form and send it back to us. We contact you within 2 days to arrange a deposit into your checking account.

Please email your completed form to VacationLoans@worldbankandtrust.com.
Your dream vacation is just a few clicks away!

Dr. Stephen Strange
World Bank and Trust
177a Bleecker Street, New York, NY10012

What did you notice in message #1?

In this message, you can see that the phisher wants to give us a low cost loan with no credit check. They say we just need to send them our information and they will give us money, right? Not only does it seem too good to be true, but also when you hover the cursor over the email address to examine it further, you see that the link actually has a different destination. It is the email address of the attacker. Lastly, as much as you might like Dr. Strange, he’s probably not working for a bank part-time.

Message #2

Subject**:** Free Amazon Gift Card!!!
Dear Sally,

You name has been randomly selected to win a $1000 Amazon gift card. In order to collect you prize, you need to log in with your Amazon account at the link below and update your contact information so we can put your prize in the mail. This is a limited time offer, so please respond to the request within 2 business days. Failure to respond will forfeit your prize and we will select another winner.
www.amozan.com/giftredemption2321

[1] https://www.consumer.ftc.gov/articles/0003-phishing

What did you notice in message #2?

Aside from this seeming too good to be true, you can see that “Amazon” is misspelled as “Amozan” on the link provided. If you read this quickly, you may think you are responding to the real company to get your gift certificate. In reality, you are providing your information to the attacker. For the purposes of this example, the link actually navigates to the Center for Internet Security, which is a trustworthy site.

Message #3

Subject: Urgent – Take Action Before Your Email Account is Deactivated

Dear User,

Following changes to our Microsoft email systems, each user must authenticate their account to prevent it from being deactivated. You can accomplish this by heading to the link below and entering your Microsoft Outlook email account credentials, and then we will know your account is active and should remain so.
http://www.microsoft.com/

Thank you,
Information Technology
Helpdesk Support Team

What did you notice in message #3?

This email is fairly well crafted without errors. Note that it establishes a sense of urgency that the malicious actor hopes will cloud your judgement and threatens the deactivation of your email account. Additionally the link at the bottom looks like a link to Microsoft, yet it is in fact heading somewhere else! Luckily, for the purposes of this example, that link simply leads to the Center for Internet Security, which is a legitimate site.

With these three examples considered, here are some basic recommendations to help protect you from becoming a phishing victim:

- If it seems too good to be true, it probably is;
- Hover your cursor over links in messages to find where the link is actually going;
- Look for misspellings and poor grammar, which can be good signs a message is a fraud;
- And, never respond to an email requesting sensitive personal information (birthday, Social Security Number, username/password, etc.).

Additional information and a phishing game can be found on the FTC’s website, https://www.ftc.gov/.

MS-ISAC
Multi-State Information
Sharing & Analysis Center

STOP | THINK
CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.