McCARTHY GRITTINGER
FINANCIAL GROUP LLC

How to Identify Malicious Emails

July 2019

1: The message contains a mismatched URL
One of the first things to check in a suspicious email message is the integrity of any embedded URLs. Oftentimes the URL (web address) in a phishing message will appear to be perfectly valid. However, if you hover your mouse over the top of the URL, you should see the actual hyperlinked address (at least in Outlook). If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent or malicious.

2: URLs contain a misleading domain name
People who launch phishing scams often depend on their victims not knowing how the DNS (Domain Name System) naming structure for domains works. The last part of a domain name is the most telling. For example, the domain name info.website.com would be a child domain of website.com because website.com appears at the end of the full domain name (on the right-hand side). Conversely, website.com.maliciousdomain.com would clearly not have originated from website.com because the reference to wesbite.com is on the left side of the domain name.

3: The message contains poor spelling and grammar
Whenever a large company sends out a message on behalf of the company as a whole, the message is usually reviewed for spelling, grammar, and legality, among other things. So if a message is filled with poor grammar or spelling mistakes, it probably didn't come from a major corporation's legal department.

4: The message asks for personal information
No matter how official an email message might look, it's always a bad sign if the message asks for personal information. Your bank doesn't need you to send your account number. It already knows what that is. Similarly, a reputable company should never send an email asking for your password, credit card number, or the answer to a security question.

5: The offer seems too good to be true
There is an old saying that if something seems too good to be true, it probably is. That holds especially true for email messages. If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.

6: You didn't initiate the action
Unless initiated by you as the user (forgot password), no system should or would initiate a password change via email. If you receive an email asking you to click to change a password due to various reasons (account was compromised, identify verification, etc.), rather than using the email link from your email, navigate to the website or service direct

web page and login directly through the page. You can initiate a password change from the web portal or follow the instructions of the email AFTER you have initiated the password change. The only problem is that I never bought a lottery ticket. If you get a message informing you that you have won a contest you did not enter, you can bet that the message is a scam.

7: Fake Display Name

One major advancement in the backend development of email clients, such as Microsoft Outlook, is that they are there to make our workday more efficient and convenient. One enhancement in particular is that incoming emails are often tagged with Display names vs. Email Addresses (John Smith vs. johnqsmith@yahoo.com). Though this is more convenient from a categorization perspective, this is also somewhat of a potential gateway for malicious exploitation. A would be attacker can easily use a free email service such as (Gmail, Hotmail, Yahoo, etc.) to create a new email account. Except instead of their name they would use the name of an employee (that they can obtain from the company website). Once the email account is created, they would send the email to other potential employees at the firm, which may have embedded malicious content. When the email shows up in your inbox, it would be listed under the real Display Name (John Smith), which may make the email seem legitimate. It is important to remember that if you suspect an email to be fake, to also hover over the email Display Name and confirm the legitimacy of the email address, as this may be another red flag when reviewing a suspicious email.

8: The message makes unrealistic threats

Although most of the phishing scams try to trick people into giving up cash or sensitive information by promising instant riches, some phishing artists use intimidation to scare victims into giving up information. If a message makes unrealistic threats, it's probably a Scam.

9: The message appears to be from a government agency

Phishing artists who want to use intimidation don't always pose as a bank. Sometimes they'll send messages claiming to have come from a law enforcement agency, the IRS, the FBI, or just about any other entity that might scare the average law-abiding citizen.

ACKNOWLEDGEMENT: This article was published by ITEGRIA, LLC. and is distributed with its permission.

This information is intended for educational purposes. McCarthy Grittinger Financial Group is not affiliated with ITEGRIA, LLC.