10 Tips for spotting a phishing email

Every day countless phishing emails are sent to unsuspecting victims all over the world. While some of these messages are so outlandish that they are obvious frauds, others can be a bit more convincing. So how do you tell the difference between a phishing message and a legitimate message? Unfortunately, there is no one single technique that works in every situation, but there are a number of different things that you can look for.

1. The message contains a mismatched URL

One of the first things that we recommend checking in a suspicious email message is the integrity of any embedded URLs. Often times the URL in a phishing message will appear to be perfectly valid. However, if you hover your mouse over top of the URL, you will see the actual hyperlinked address (at least that's how it works in Outlook). If the hyperlinked address is different from the address that is displayed then the message is probably fraudulent or malicious.

2. URLs contain a misleading domain name

Often times people that launch phishing scams depend on their victims not knowing how the DNS naming structure for domains works. It is the last part of a domain name that is the most telling. For example, the domain name info.brienposey.com would be a child domain of brienposey.com because brienposey.com appears at the end of the full domain name (on the right hand side). Conversely, brienposey.com.maliciousdomai.com would clearly not have originated from brienposey.com because the reference to brienposey.com is on the left side of the domain name, not the right. This trick has been used countless times by phishing artists as a way of trying to convince victims that a message came from a company like Microsoft or Apple. The phishing artist simply creates a child domain bearing the name Microsoft, Apple, or whatever. The resulting domain name looks something like this: Microsoft.maliciousdomainname.com.

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, legality, and a number of other things. As such, 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 is always a bad sign if the message asks for personal information. Your bank doesn't need you to send them your account number. They already know what it 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 saying holds especially true for email messages. If you receive a message from someone unknown to you who is

making big promises, then the message is probably a scam. After all, why would a Nigerian prince that you have never heard of contact you to help him smuggle money out of his country?

6. You didn't initiate the action

If you get a message informing you that you have won a contest that you did not enter then you can bet that the message is a scam.

7. You are asked to send money to cover expenses

One telltale sign of a phishing E-mail is that you will eventually be asked for money. You might not get hit up for cash in the initial message, but sooner or later a phishing artist will likely ask for money to cover expenses, taxes, fees, or something like that. If that happens, then you can bet that it's a scam.

8. The message makes unrealistic threats

Although most of the phishing scams seem to try to trick people into giving up cash or sensitive information by promising the victim instant riches, other phishing artists try to use intimidation to scare the victim into giving up information. If a message makes unrealistic threats then the message is 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 phishing artists will send messages claiming to have come from a law enforcement agency, the IRS, the FBI, or just about anything else that could scare the average law abiding citizen.

10. Something just doesn't look right

In Las Vegas casino security teams are taught to look for anything that JDLR (as they call it). The idea is that if something just doesn't look right, then there is probably a good reason why. This same principle almost always applies to email messages. If you receive a message that seems suspicious then it is usually in your best interest to avoid acting on the message.