Bank of Tucson
Email Phishing Tips

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 things that you can look for. This article lists 10 of them.

1: The message contains a mismatched URL

One of the first things I recommend checking in a suspicious email message is the integrity of any embedded URLs. Oftentimes the URL 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. 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 naming structure for domains works. The last part of a domain name 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.maliciousdomain.com would clearly not have originated from brienposey.com because the reference to brienposey.com is on the left side of the domain name.

I have seen this trick 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, 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 it 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

Just yesterday I received an email message informing me I had won the lottery!!!! 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: You're asked to send money to cover expenses

One telltale sign of a phishing email 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, phishing artists will likely ask for money to cover expenses, taxes, fees, or something similar. If that happens, you can bet that it's a scam.

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. Let me give you an example.

About 10 years ago, I received an official-looking letter that was allegedly from US Bank. Everything in the letter seemed completely legit except for one thing. The letter said my account had been compromised and that if I did not submit a form (which asked for my account number) along with two picture IDs, my account would be canceled and my assets seized.

I'm not a lawyer, but I'm pretty sure that it's illegal for a bank to close your account and seize your assets simply because you didn't respond to an email message. Not only that, but the only account I had with US Bank was a car lease. There were no deposits to seize because I did not have a checking or savings account with the bank.

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.

I can't tell you how government agencies work outside the United States. But here, government agencies don't normally use email as an initial point of contact. That isn't to say that law enforcement and other government agencies don't use email. However, law enforcement agencies follow certain protocols. They don't engage in email-based extortion—at least, not in my experience.

10: Something just doesn't look right

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