HOW TO SPOT A PHISHING EMAIL

A MISMATCHED URL

Hover your mouse over the top of the URL. If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent or malicious.

TOO GOOD TO BE TRUE!

If you receive a message from someone unknown to you who is making big promises, it's probably a scam.

YOU'RE ASKED TO SEND 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 even pose as your boss requesting you pay a rather large bill! If this happens, it's a scam!

POOR SPELLING AND GRAMMAR

By sending an initial email that's obvious in its shortcomings, the scammers are purposefully isolating the most gullible targets. They don't want you, someone from whom there's virtually no chance of scamming. They want people who, faced with a ridiculous email, still don't recognize its illegitimacy.

CONTAINS UNREALISTIC THREATS

For example, the message says your account has been compromised and if you do not submit a form with your account number and personal information etc, your account will be canceled and assets seized.

URLS CONTAIN A MISLEADING DOMAIN NAME

People who launch phishing scams often depend on their victims not knowing how the DNS naming structure works. The last part of a domain name is the most telling. A phishing artist will create a child domain bearing the name Microsoft, for example.The resulting domain name looks something like this: Microsoft.com.maliciousdomainname.com

APPEARS TO BE FROM A GOVERNMENT AGENCY

Phishing artists sometimes send messages claiming to have come from organisations that might scare the average law-abiding citizen. These organisations usually follow certain protocols for sending emails, and don't engage in email-based extortion.

REQUESTS 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 already knows your account number. A reputable company would never email asking for passwords, credit card numbers, or answers to security questions.

YOU DIDN'T INITIATE AN ACTION

You probably haven't won the lottery! If you get a message informing you that you have won a prize, or a contest you did not enter, you can bet that the message is a scam.

BASICALLY, SOMETHING JUST DOESN'T LOOK RIGHT

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.