Fraud and Scam Series
#4- Phishing and Spoofing

It is good to be familiar with spoofing and phishing techniques used by scammers so you can easily identify when they may be being used against you. These methods are employed to take advantage of an individual's vulnerabilities to gain access to personal information.

Spoofing is when someone masks themselves as someone else. Spoofing can be used digitally on emails or website URLs, or over the phone. The scammer wants the individual being targeted to assume they are interacting with a trusted source.

Furthermore, these defrauders need the victim to believe they are dealing with a legitimate company or person so they can get them to send money, download malicious software or reveal personal information to be used elsewhere.

Phishing uses spoofing to trick the person into giving up the information they want.

Phishing has evolved and now has several variations that use similar techniques:

- *Vishing* scams happen over the phone, voice email, or VoIP (voice over Internet Protocol) calls.
- *Smishing* scams happen through SMS (text) messages.
- *Pharming* scams happen when malicious code is installed on your computer to redirect you to fake websites.

(SOURCE)

Examples of Phishing and Spoofing:

- You get a call from a number that looks local, the person on the other line identifies as being from your bank's fraud department and needs to verify your identity to stop fraudulent activities on your account. *Know that if a financial institution calls you, they will NOT ask for sensitive information.*
- You receive an email that looks to be from an energy company, there is an attachment to the email that contains a bill or invoice for work rendered. If the sender's email address looks questionable or you didn't have service from such company, this attachment could contain malicious software than can harm your device or steal information from the hard drive. *Do NOT open it*.

What to do when you feel uncertain:

- Never open an email or click on a link or attachment is questioning an email or text message. Instead contact the company directly either by phone or signing into your account.
- If you receive a questionable call, never give out personal information. Hang up and call the company back on a phone number you know to be certain.
- Never send money to an uncertain source. Scammers will try to frighten you by threatening with arrest or jail time, further action, or fines. Legitimate companies will give you some time before taking extreme action, therefore take a moment to do your due diligence and try not to have a knee jerk reaction.