NAME: Chidinma B. Aniekwena

BUFF ID: 1108372

COURSE: Current Issues in Cybersecurity

WEEK 3: Assignment

ASSIGNMENT TOPIC: Phishing

1. WHAT DID I DO

I did a phishing quiz on Sonicwall and OpenDNS to determine and decide if the e-mail (or website) is a "Phish" or "Legitimate."

Phishing is a form of cybercrime in which criminals use fake emails, websites, and other forms of communication to trick individuals into revealing sensitive information such as passwords, credit card numbers, and other personal data.

Phishing emails often appear to come from a legitimate source, such as a bank, social media site, or e-commerce platform. The emails usually contain a sense of urgency and ask the recipient to click on a link or provide information to "verify" their account or resolve a supposed problem.

Phishing websites are designed to look like the real thing and often use a similar domain name or URL to the legitimate site, but with slight variations. For example, a phishing website might use a URL like "[www.paypa1.com](http://www.paypa1.com/" \t "_new)" instead of "[www.paypal.com](http://www.paypal.com/" \t "_new)." When users enter their login credentials or other sensitive information into these fake sites, the criminals behind the phishing scheme can use that information for their own purposes.

To protect yourself from phishing attacks, be cautious of emails or websites that ask for personal information, even if they appear to be from a legitimate source. Don't click on links or download attachments from suspicious emails. Instead, type the URL for the website you want to visit directly into your web browser's address bar. Additionally, keep your antivirus software and web browser up to date, and enable two-factor authentication on your accounts when possible.

1. WHAT WERE MY RESULTS

Out of the 10 questions quiz I did on Sonicwall, I got 8 correctly. One of the questions failed was the credit card payment due, maybe I was over cautious or I have a previous knowledge that one can login to the credit card app and make due payment and not via an email sent to a customer to click a link to make payment.

Out of the 14 sites I tried identifying on OpenDNS, I was able to identify 13 correctly, which I think qualifies me for a phish-spotting ninja!. However, I will not neglect the fact that cyber criminals are more clever than ever at creating sites that fool even the most experienced phishing detectives.

1. WHAT DID I LEARN

I learnt that one can never be to spot a phishing website or email at all times, but the most important question to ask oneself before opening an email of licking on an unsure site is to first hover round the url and ask oneself if they are expecting any email of such. Any email not recognized or unsure of, the best approach is to delete immediately for the system.