Video 4: Phishing Scams

Topics in this Module
Module 4 – Phishing Scams

Welcome to NAU's Information Security Essentials training. This module includes the following topics:

- What is Phishing
- Purposes of Phishing
- How to Spot a Phishing Scam
- Indicators of Phishing Scam
- Examples of Phishing Scams
- What to do if you suspect a phishing scam

To learn more about these topics, click "continue. To jump straight to the tutorial quiz, click "jump to quiz".

What is Phishing?
Phishing is the process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email or other electronic communication.

Purpose of Phishing Attacks
The purpose of a phishing attack is to trick you into providing personally identifiable information such as your username and password, bank account information, social security number, or credit card information. In most cases, phishing scams are after something of monetary value or they are trying to commandeer your account.

Purpose of Phishing Attacks
If you respond to a phishing scam with your personal information, this could result in identity theft, whereby someone else may be able to apply for and get credit in your name, empty your bank account, or change the direct deposit account for your paycheck.

How to Spot a Phishing Scam
It is not always easy to spot a phishing scam right away. Sometimes phishing scams appear legitimate or like webpages or services you recognize. For example, take a look at this webpage. Many of you may recognize this as the CAS login page that we use to log in to NAU services. However, this is not the CAS login page. This is the CAS login page. Can you spot the difference? Take a closer look at the URLs. Notice how they are different. Some phishing scams can be really convincing, such as this CAS page, but we'll go over ways to determine whether an email or electronic communication is a phishing scam or not.

Unfortunately, there is not always a definitive way of determining whether you are looking at a scam or not. NAU will never request your NAU password in an email and

you should be suspicious of any request for personal information in an email or other electronic communication. In addition there are characteristics we should always look for when someone is requesting our personal information.

Again, NAU will never ask for your password in an email. If you receive an email asking for this information, it is a phishing scam. It is important to know, not all phishing scams will ask you for your username and password. For these cases, there are some clues that you can check for. Not all of these clues are definitive of a phishing scam and may even be present in legitimate emails. So, we've divided these clues into two categories, strong and weak. The strong category contains elements that will be highly suggestive of a phishing scam, whereas the weak category are clues that might be present in a phishing scam, and should make you suspicious, but on their own are not strong indicators of a scam.

Strong Indicators
Strong clues to look for in a phishing email are an untrusted reply address or a suspicious URL.

Let's take a look at an example that has these strong indicators. Here's the bait. Let's start at the top.

Reply Address
Take a look at the Reply Address that will appear next to **From:** at the top of the email. In this example, it reads Gary Saunders with a return email address of gsaunder@bw.edu. This is not a name or email that I recognize. And, because I don't recognize it, this is not someone I really trust, especially in regards to my NAU password. Email addresses may not always be the most dependable way of determining a scam. For example, would this email be more trustworthy if it came from an NAU email address that ended with @nau.edu? Not necessarily. If a phishing attack successfully obtains someone's NAU username and password, they could then use that account to send you phishing scams and those scams could come from an @nau.edu email address. Therefore, the email address alone is not enough to determine if the email is a phishing scam.

It is important to note, if NAU needs to contact you regarding your NAU account, that email will usually come from the email address Ask-ITS@nau.edu.

URL
Next take a look at the URL in this email. http://systemadminmailboxupgrade.jimdo.com. This email is addressing concerns over an NAU account, shouldn't it have nau.edu in the URL? Let's return to the example of the CAS page that we saw earlier to help us understand this URL.

There are two things we can look at to help us determine if this is a trusted URL. If a URL is asking you to log in or enter personal information, it should have an https:// at the beginning of the URL, which indicates the page is using encryption (computer code

that protects data from outside third parties), in a web browser this is symbolized by a lock symbol. And, the URL should have a familiar domain.

The domain is a word or series of words that defines a site location on the Internet. The domain is always at the beginning of the URL following the https:// and ends before the first slash. It is not enough to have nau.edu in the URL, it must be located at the end of the domain. This means that nau.edu must immediately be followed by the first slash. For example, I've highlighted the domain in the two URLs below. Notice how nau.edu is only at the end of the highlighted domain in the real CAS page, but in the fake CAS page it appears after the first slash? That is because the fake CAS page is not a real NAU website.

Let's take a look at a few more examples. Identify which URL is a trustworthy NAU website.

Examples for activity
https://iris.nau.edu/OWA/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2firis.nau.edu%2fOWA%2f
This is the correct answer. Even though the URL does not begin with nau.edu, nau.edu appears right before this first slash signaling that this is a legitimate NAU webpage.

http://nau.edu.freewebs.com/15689/logon.php
While nau.edu appears at the beginning of the URL, we really only care about this area right before that first slash. This does not have an NAU domain, but is instead a webpage on the freewebs.com domain. In addition, there is only an http:// at the beginning of this URL, and we need to look for an https:// to indicate a secure website.

https://docs.google.com/forms/nau.edu/d/1SF03ASeVqjzgD-z9Qs2BrDmXK5xpRnYEBK-u0zzwirY/viewform?usp=send_form
While nau.edu does appear in this URL, it is not in the right spot. It needs to be before the first slash in the URL. Anything after that slash does not indicate that this is truly an NAU website.

URLs
Returning back to our email, let's take another look at the domain of this URL. In this case, the domain of the URL is jimdo.com, and it does not begin with https:// which would indicate that this is a secure website. This URL is not to be trusted.

Hidden URLs
Sometimes, links appear in an email as text, such as Click Here. To determine whether these links are trustworthy, hover over the link with your mouse and you will see the actual URL. From here, you can look at the domain to determine if this is a trustworthy URL.

Weak Indicators

We've learned that the strongest indication of a phishing scam is a request for personal information, especially your NAU username and password. We've also learned that strong indicators of a phishing scam can be found in a reply address and a URL. Now, let's examine some characteristics that are weaker indicators of a phishing scam. Or, they should make you suspicious if you notice them. They may not be present in all phishing scams and they may even be present in legitimate activity. Weak indicators include strange terminology, language errors, and a sense of urgency. Let's look at another example.

Strange Terminology

Take a look at the terminology in this email. Web-mail Account User, Technical Support, Web-mail Account Service Team Management. Legitimate communications tend to be a little more specific in their terminology. For example, at NAU, our support teams are called the Solution Center and the Student Technology Center. And, our email accounts are Iris/Exchange accounts and Gmail accounts. We will refer to these services with the correct names. Keep in mind, just because you see the correct names, doesn't mean that the communication is legitimate. These names are public information and a smart phishing scam might use the correct names to appear more legitimate.

Language Errors

Now, take a second to read over the content of the email. Notice that some of the language does not make sense. Let's take a look at the second paragraph as an example. "Failure to update will process your Web-mail account being temporarily blocked or suspended from our network and may not be able to receive or send e-mail due to the update" That sentence is difficult to read and doesn't make a lot of sense. Language errors such as grammar, spelling, and punctuation can be an indicator that this is not a legitimate message. While not everyone is perfect, official communications from NAU are proofed before being sent and obvious errors should not be present. Sometimes phishing scams are also proofread, so a lack of language errors does not rule out an email as a scam.

Sense of Urgency

Notice how this email has a sense of urgency. It wants you to respond so your account can be updated immediately and it reminds you at the end that you have to reply to this email. Phishing messages will create a sense of urgency so that you immediately respond without thinking. But, a sense of urgency is a weak indicator; therefore it may not be present in all phishing scams.

Review

In review, if you ever receive an email or electronic request asking for your NAU password or other sensitive personal information, this is most likely a phishing scam. Not all phishing scams will ask for this information so we can use strong and weak indicators to help us spot them. Strong indicators are the reply address and URLs. Weak indicators are strange terminology, language errors, and a sense of urgency. If

you are ever unsure, you can always contact the Solution Center and they will help you determine if you have a phishing scam or not.

What if You Suspect a Phishing Scam?
If you ever receive an email or electronic communication that you suspect to be a phishing scam, there are several important steps that you can take to not only protect yourself, but also the entire NAU community.

Never respond to a phishing scam! Not even to tell them to leave you alone. Responding to these emails will confirm that your email address is a valid and active account and you may start receiving more scams.

Never click on any links within a phishing email or open any attachments. Doing so could take you to dangerous websites, or install dangerous files, such as Malware, on your computer.

If you feel the email MIGHT be valid but are suspicious of clicking or responding to it (good for you – be suspicious!), remember "phone-first" is a good practice! If it is coming from your supervisor, call him or her or walk down the hall to confirm – they will appreciate your diligence in verifying. If it is your bank or some other account, "phone-first" or login as you normally would – do not use the email link or phone number.

Remember, if you See Something – Say Something! Don't just click it, report it! Once our Information Security team is aware of these phishing emails, they can protect other NAU users from receiving them. To learn more about how to report phishing scams, please see http://nau.edu/its/learn/emailphishing.