How to Recognize and Avoid a Phishing Scam

Phishing is an identity-theft scam that can use emails and websites to trick people into giving out personal information, such as credit card numbers, usernames and passwords, or Social Security numbers.

Phishing is usually done by hijacking the brand identity of a bank or an online store in a spoofed email that is distributed widely. The email usually contains a link to a login page designed to look like the organization's actual site. The scam uses the login page to capture the information you provide, then sells or uses it for malicious purposes.

Five ways to avoid falling victim to a phishing scam:

- **Always be suspicious of emails asking for sensitive information**. Email is not a secure form of communication. Organizations you do business with already know your account information and will never request it in an email. Phishers usually include false statements to create a sense of urgency for information, such as, "Your account will be terminated unless you respond immediately."

- **Never respond to an email request for personal information**. Err on the side of caution. Look at the "from" field of the email. If the organization name does not match the "reply to" organization name, the message is probably fake. (For example, a message from a local credit union or bank would not have a reply email address ending in yahoo.com.) If you ever need to provide personal information like a credit card number, be sure to use a secure, trusted website.

- **Beware of phone phishing scams**. If someone requests personal information on a phone call, be sure you initiated the call—not the other way around.

- **Never follow the links in an email you suspect might be phishing**. If you are unsure about a link you receive in an email, hover your cursor over it. If the link text doesn't match the link address, do NOT click it. Log directly onto the company's website, or call the company. Ask if the company is legitimately asking for the information in the email. Note that hovering on links often does not work on mobile devices, so it is best to use a computer when determining an email's legitimacy -- ignore the email until you can get to a computer to verify.

- **Make sure your operating system, antivirus software, and browser are up to date**. Malware exploits vulnerabilities in the security of operating systems (such as Windows and iOS) as well as web browsers (such as Internet Explorer, Firefox, etc.). Be sure you have the latest security updates installed on your computer. [FI - The ITS security information page has more information on keeping your computer and data protected.]

Think you received a phishing scam?

Trust your gut. If it seems off, it probably is and you can delete it. If you received a phishing message, but aren't sure, cross-check it with our current Phishing Examples page where we post current messages that are being reported on campus.

If you don't see your message on the current Phishing Examples page, you can report your message to our email security team at helpdesk@glendale.edu.

More tips to avoid being scammed

1. How to Spot Fake Email Addresses

   One of the best ways to defend against deception is to take a critical look at the internet address and/or email address and evaluate it for authenticity.

   Websites and the originating site of an email usually have an address based on the domain name – for example .com, .gov, or .edu. A list of common extensions is available in the article [FI - Understanding Web Site Names].

   Ask yourself whether the extension matches the purpose of the site. For instance, a governmental site or email would typically end in .gov. If the domain name associated with the site or message is .com, be suspicious.

   Sometimes, the site's name ends in a country code (e.g. .uk, ro, .ru or .ca). When you see this, judge whether it's being used in the correct context. For example, would your local bank email you from Romania or direct you to a website based there? It is unlikely they would.

   Even when the site name seems plausible, watch for these other red flags:

   Concealed web addresses – In web pages or emails, links might say one thing and link somewhere different.

   Deceptive addresses – Scammers often create deceptive web addresses that resemble legitimate ones.

   Forged email addresses – In emails, the "From" address field is very easy to fake.

2. Recognizing a Deceptive Link

   Deceptive links are a common trick used by scammers, both in emails and on web pages (especially advertisements). They will create a link that mimics a legitimate web address—but when you click it, it takes you to a completely different site than you expected.

   An example: A phishing email sent to individuals here at GCC included the link:

   www.glendale.edu/webmail
   Sounds legit, right? However, the underlying address was completely different, so when people clicked it, they were sent to something more like this:

   www.abc-bad-link.com/use/upgrade/form.html

What's the worst that could happen if you click one of those bad links?

Your computer could be infected with malware and an infected system can do just about anything, from stealing your personal information to spamming your unsuspecting contacts in an effort to infect their machines.

How can you tell if a link is deceptive?

BEFORE you click it, hover your mouse over the link. The link it actually leads to should pop up in a box or bubble (and it may even warn you of a mismatch). Look at the URLs closely to make sure they match.

Also, be cautious of any link that doesn't clearly indicate where it leads—particularly links that say "click here" or those that do not disclose where you go when you click them, such as those provided by URL shortening services (tinyURL, bitly, etc.).

3. Spotting a deceptive web address

Scammers are good at coming up with website names that seem legitimate but take you to a site you didn't intend to visit—often a troublesome one that could infect your computer with malware.

Their trick: include just enough recognizable words and phrases to confuse people. At first glance, when you see those familiar words, it seems real. But a closer look reveals that it's bogus.

An example:

These email messages claim to come from ITS, and you recognize phrases like GCC and outlook.

http: //gccoutlook.glendale.edu.ru/outlook.htm

http: //216.32.44.201/outlook.htm

But, both are bogus, and here's how you can tell. Look at the actual site name:

http: //gccoutlook.glendale.edu.ru/outlook.htm

The first example includes "glendale.edu," but ends with ".ru" The ".ru" indicates a site in Russia — a highly unlikely origin for a message about any GCC account.

The second example doesn't have the hostname, just the numeric address (IP address) that underlies a hostname. A URL that only includes an IP address should be treated with great suspicion.

http: //216.32.44.201/outlook.htm

One more clue

We'll wrap up this lesson with one last tip: Watch for letter substitutions.

You might see something like service@g1enda1e.edu, with the number 1 used in place of the lower case l. in "glendale."

Or, Helpdesk @its.gl3ndale.edu, with a three rather than the letter e.

4. ### How to identify a forged email address?

It is easy to fake what appears in the "from" or "reply-to" line of an email message. If you dig a little deeper, you can confirm the message's true origin.

When you receive an email, the message header includes standard information, like "to," "from," and "subject." But there's also a more detailed full email header that can help you trace the message back to its original source, to see if that matches up with what the more basic message header says.

If the "from" in the message header doesn't correspond with what you see in the full version of the email header, be suspicious of a scam.

Revealing the full header

The full header is not automatically visible, but it's easy to reveal it through your email software.

Here's a support article on how to view or forward message headers in Outlook. This Google support article offers instructions for revealing full message headers in other email services.

Wath the speling …

Did you happen to catch the misspelling of "incorporated" in the "from" line in the example? (From: Adobe Systems Incoporated)

Spelling and grammatical errors are good indicators that an email could potentially be bad.