Don't Get Reeled In by Phishing

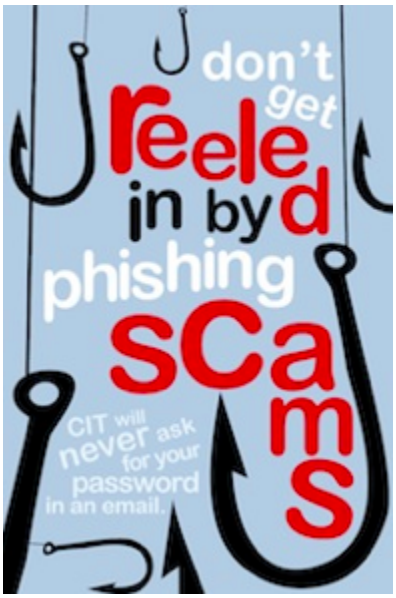
If you believe you have responded to a phishing attack which might compromise your accounts, you should immediately change your password(s) and notify the CIT HelpDesk at 585-245-5588.

What is Phishing?One of the most common security threats faced by Internet users is something known as *phishing*. Phishing is an attempt at identity theft where the criminal impersonates some official entity and tries to get the victim to provide them with personal information such as Social Security numbers, Credit Card numbers, and passwords. The information can then be used by the thief to impersonate the victim in order to commit fraud and to steal or damage the victim's personal resources.

Email is one of the more common avenues for phishing attacks. Email phishing attacks occur against Geneseo users almost daily. The criminal will send an email with a subject line and body that appear to come from an official source:

> *From: Geneseo Helpdesk <baduser@yahoo.com>*
> *Subject: SUNY Geneseo Helpdesk*
>
> *Your account has been targeted for deletion. In order not to lose your account you need to send us your username and password immediately in order to confirm your identity.*
>
> *Alternatively you can click on the following link to login and verify your identity:*
> *http://www.geneseo.edu/login/*
>
> *Sincerely,*
> *Geneseo Help Desk*

You should always distrust such communications.



How should I guard against Phishing attacks?

- **Never** send your account password or any personal information to anyone via email. No reputable organization will ever ask you to send them such information via email.
- **Never** give someone who calls you on the phone your personal information. If necessary, tell them you will call them back. Look up the publicly listed phone number for the organization and contact them.
- **Never** click on a link embedded in an email unless you have verified the sender's email address to be legitimate and you trust them. Even then, it is always better to retype the URL vs. clicking a link. A link can be made to look like a legitimate URL when it in fact goes to some place entirely different. Try clicking on the link shown above in the fraudulent email to see an example.
- You should **carefully check** the email address of the sender of any communication. Look at the email address very carefully and do not trust the text preceding the address.
- If you click on an embedded link (which we don't recommend), **look carefully at the URL** in the browser to make sure it is the real web site for the organization. Criminals can be very clever in crafting domain names and web pages that look very close to official sites.

How can I help to protect SUNY Geneseo from Phishing?

1. When CIT receives reports of widely delivered malicious email, we will Tweet or post a status message. You can also help us protect our inboxes by marking the malicious email as spam or reporting it as phishing.
2. To report the message as spam in Gmail, click on the Spam button.

3. To report phishing in Gmail, click the drop-down arrow next to “Reply” and select “Report phishing.” Reporting a message as phishing will prevent that user from sending you more emails.

4. Most importantly, **never reply** to suspicious emails, tweets, or posts with your personal or financial information. Also, **don’t fill out forms or sign-in screens** that link from these messages.

Related Articles

- http://en.wikipedia.org/wiki/Phishing
- http://www.antiphishing.org
- http://www.mozilla.com/en-US/firefox/phishing-protection
- https://support.google.com/accounts/answer/75061?hl=en
- Google's *How to Detect Phishing* Video

More Help

For questions, contact the CIT HelpDesk by calling (585) 245-5588, or visiting our online service desk.