Thank you for participating in our Phishing E-mail User Training Program.
This was brought to you by the SUNY Security Operations Center and
Onondaga Community College IT Security.

What Just Happened?

The e-mail you just clicked on was a simulated phishing e-mail, the same kind of e-mail that hackers use to steal data. **If this had been a real attack, your computer could have been hacked, simply by visiting a webpage.** Rest assured that this time, no harm was done and no information was collected if you had filled out the form. To keep you and your data safe, your organization is periodically sending out these phishing emails to educate users.

What is Phishing?

Phishing refers to sending an e-mail which tricks someone into clicking on a link or opening an attachment. The end goal of phishing is to steal valuable information, such as usernames and passwords.

Why Should You Care?

Clicking on links in phishing e-mails, or filling in confidential information on malicious websites, can put your data at risk - not only the company's but also your personal data. Through phishing emails, attackers can gain access to confidential company data, steal money from your bank accounts, and steal your identity.

What's Safe To Do, And What Isn't?

There is very little risk in simply opening e-mails. In almost all cases, opening an e-mail will not result in compromise.

The risk is in clicking on links or opening attachments. Attackers can e-mail you infected attachments which install malicious software, or "malware" for short. Clicking on a link can take you to a website which steals login or other valuable information. The website could also install malware on your machine without your knowledge.

Why Are We Sending Simulated Phishing Emails?

These tests are designed to help you. The lessons learned apply not only to work but to your personal life. Be sure to share with your family and friends. If you have

How Can You Spot a Phishing E-Mail?

Phishing emails can be hard to recognize, and every phishing e-mail is different. Here are some telltale signs:

- **Bad spelling and grammar:** Simple phishing emails are often poorly written. If the content of the e-mail doesn't line up with what you'd expect from the sender, beware!
- **Did you do something to initiate the e-mail?:** Ask yourself if you made a purchase or processed a transaction that would lead you to expect the email from that company. If you didn't, chances are good that it's a phish.
- **Deceptive links:** Move your mouse over any of the links in the e-mail, without clicking. You should see the address where the link will take you.

If it's an e-mail from your bank, but the link doesn't display your bank's website, don't click.

- **Sense of urgency:** Is the e-mail claiming that you were charged an extraordinary amount on your cell phone bill, or telling you your e-mail account has been suspended? Be careful - somebody may want to push your buttons so you click on a malicious link. When in doubt, pick up the phone.
- **No name in e-mail:** Is an e-mail starting with *Dear Customer* but not incuding your real name? Chances are the fraudster doesn't even know who this e-mail account belongs to. Don't click.
- **Still unsure?:** If you are unsure whether the e-mail is legimate, call the company OR open a web browser and type in the company's website address. Don't copy and paste from the links in the e-mail.

If you receive any "phishy" emails, please forward them to your IT department, asking them to analyze the e-mail.

any more questions on what phishing attacks are, or on security in general, feel free to contact your IT security team for more information.