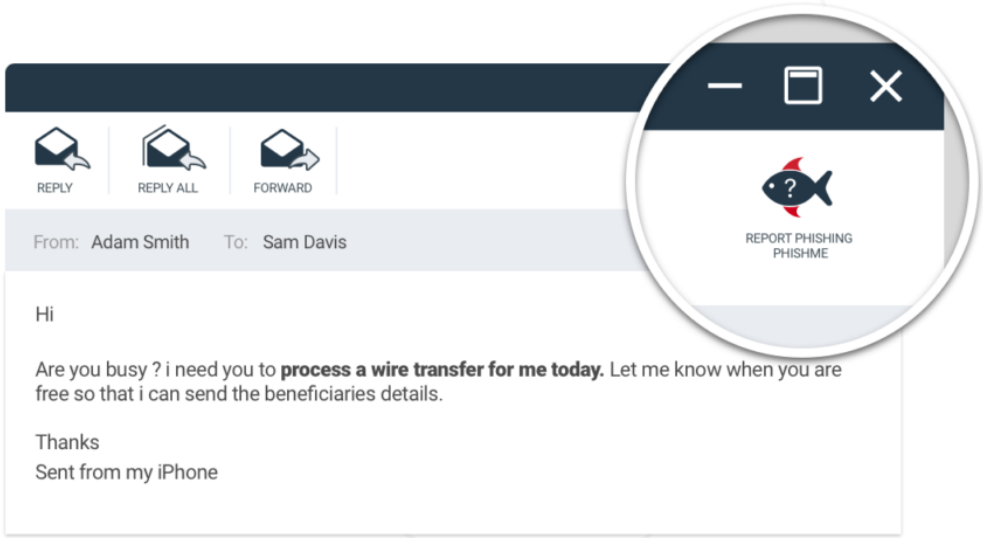
MARCH 2019

# OUCH!

## NHRMC Phishing Awareness Program

When suspicious emails make it through our defenses, we rely on you as our last line of defense. Therefore, it's vitally important that you learn to properly identify and report suspicious emails as potential threats.

In the coming months, we'll be running a comprehensive phishing awareness program. By taking a proactive stance and learning how to spot and report potentially dangerous emails, we can keep our organization safer.




## What Does the Program Entail?

In this program, you will periodically receive simulated phishing emails that imitate real attacks. These emails are designed to give you a realistic experience in a safe and controlled environment. This method allows you to become familiar and more resilient to real world tactics.

If you see any suspicious emails report it with the Report Phishing Button. If you do fall for one of the simulations, we ask that you take 30 - 60 seconds to read and understand the brief education material that is presented afterward.

As the program continues to progress, you will be able to better spot phishing attacks, both at work and at home.

New Hanover Regional Medical Center

MARCH 2019

# OUCH!

## NHRMC Phishing Awareness Program

### What To Do If You Receive a Suspicious Email


If you suspect you have received or reacted to a phishing email, report it immediately by clicking the Report Phishing button in Outlook, Outlook Web or Outlook Mobile. Don't be afraid to report anything suspicious. Many times attackers try to use fear or embarrassment to get you to respond. For example: there was a recent phishing email that told the user that the attacker had accessed video from the user's webcam showing them on an adult website.

Reporting a suspicious email will notify the right people in our organization about the possible attack. If the email is a simulated email that is part of our awareness program, you will receive instant feedback thanking you for reporting. If the email is malicious, quick reporting will help us prevent a widespread breach. Your active participation is crucial to help protect our organization.

### The Dangers of Spear Phishing

Chances are you've received a few general phishing emails in your personal or work-related inbox before. These emails are sent to the masses, with the hope that just a few of the thousands or millions of recipients fall victim.

Spear-phishing emails, by contrast, are targeted attacks that take advantage of personal and professional relationships, organization hierarchies, and human curiosities. These highly personalized emails pose a unique threat because they can bypass technical controls like antivirus and spam filters.

In today's world, it's necessary to work online, and spear phishers will use the information we post to trick us into clicking a link, opening an attachment, or entering sensitive information into legitimate-looking websites. Slow down and examine emails closely before taking action.

### Important Reminder

Please do not use your NHRMC email account and password for non work related websites or applications as attackers that hack those systems can turn around and attempt to use your information to access NHRMC systems.

New Hanover Regional Medical Center