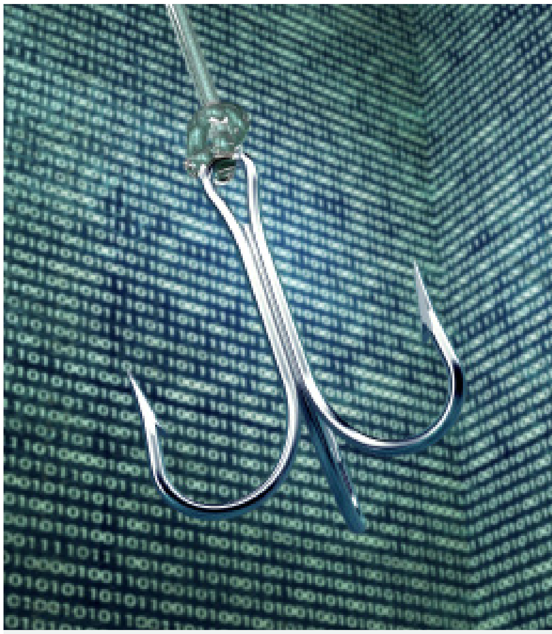
Today's Phishing Can Have You on the Hook for Millions—
Here's What You Need to Know…

Understanding the practices of a hacker can help to better prepare defenses. Phishing, a form of social engineering, is an attempt to acquire sensitive information such as usernames, passwords, bank account information, credit card details, and social security numbers by masquerading as a trustworthy entity. As our society shifts to relying more on electronic communication, **phishing attacks are becoming increasingly effective and widespread**.

As companies shore up their security footprints, hackers are forced to be more creative to get in. They will often try to prey on unsuspecting or unknowing users who they hope are too busy to pay attention to the details. A prize needs to be claimed immediately or there is a problem with a user's account that must be dealt with. **Phishing attacks are effective largely because they convince the recipient to bypass critical thinking**. They push users into thinking emotionally and acting without thinking.



Hackers often try to prey on unsuspecting or unknowing users who they hope are too busy to pay attention to the details.

How Phishing Works

A phishing scam is typically carried out with the help of an unsolicited email or a fake website that poses as a legitimate site to lure in potential victims and prompt them to provide:

- valuable personal or financial information;
- system user IDs; and/or
- passwords.

Newer phishing attempts involve incoming phone calls where the hacker poses as a representative of a known vendor. They claim they haven't been paid for a past due invoice, and trying to get the unsuspecting victim to wire them payment or provide financial information, check routing numbers, etc. Armed with this information, a criminal can commit identity or financial theft.

Phishing emails often target unaware end users, tempting the user to click on a link or attachment that will ultimately download spyware. Scammers craft their emails and web pages carefully, often copying web page layouts and logos of the entity they are trying to impersonate.

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com

Today's Phishing Can Have You on the Hook for Millions— Here's What You Need to Know…

The 8 "Dos & Don'ts" of Phishing Prevention

#1 DO be very wary of any unexpected email asking to click links, open attachments, or download files—especially if financial or other private information is requested.

#2 DON'T provide personal information or information about the organization, including its structure, networks, or log-in credentials unless certain of a person's identity.

#3 DO be extremely cautious of the validity of the email if spelling or grammatical errors are noticed.

#4 DO look for 'https://' and a lock icon in the address bar before entering any private information.

#5 DON'T click a link from an email message, and don't copy a link from an email message to paste into a web browser. Phishers can make links appear to go to one place, but then actually direct victims to a different site. For example, when receiving an email from LinkedIn, type www.linkedin.com into a browser or use a known bookmark.

#6 DON'T send personal or financial information by unencrypted email.

#7 DO have a firewall and an updated anti-virus program that can scan emails.

#8 DO STOP and THINK before you CLICK.

Educate your employees on the mechanics of phishing.

BLUE ORANGE® COMPLIANCE

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com

Today's Phishing Can Have You on the Hook for Millions—
Here's What You Need to Know…

Spear Phishing

Spear phishing is a targeted phishing campaign typically sent randomly to a set of users, generally with no ties to one another. A spear phishing campaign is a directed attack with a specific target and goal in mind—and often a higher payoff for the hacker.

How Spear Phishing Works

In spear phishing, a target is selected such as a specific company, a department within the company, or an individual employee of the company. Unlike a typical phishing campaign, the target is not random. Careful thought and planning go into selecting the target.

The hacker will then collect information about the target. Social engineering, social media accounts, corporate websites, press releases, and information from the dark web are all resources at the hacker's disposal.

With the appropriate amount of information, the hacker will release the targeted attack, generally in the form of an email sent directly to the individual target. The email will appear to be sent from a trusted source such as a spouse, relative, or company executive and will be crafted in a way to elicit an emotional response with the goal of getting the recipient to either open an attachment in the email or click through to a web site and enter sensitive credentials.

Once the payload has been delivered (the attachment was opened or the link was clicked), the hacker is free to continue the exploit and collect the sensitive information they were after.

Spear Phishing Prevention

Because spear phishing is a targeted attack, the hacker will go to greater lengths to cover their tracks and prevent detection than they would with a typical phishing attack. The techniques used to prevent phishing attacks also apply to prevention of spear phishing. Additionally, employees should be aware that if an email from a trusted source seems unusual or out of the ordinary, a quick phone call to the sender to verify the contents can be the difference that stops a spear phishing attack.

Today's Phishing Can Have You on the Hook for Millions—Here's What You Need to Know…

Whaling

Like phishing, whaling is an attempt to acquire sensitive information by masquerading as a trustworthy entity. But in this crime, the targets are typically executive or C-level employees who have access to high-level protected health information or financial data.

How Whaling Works

Hackers use various forms of social engineering to gain information about high-level employees. Armed with this information, hackers will disguise themselves as a trusted entity in an attempt to acquire financial information or sensitive data. Hackers may even use social media to determine when a high-level employee is on vacation and then contact his or her assistant.

Whaling typically targets executive or C-level employees who have access to high-level protected health information or financial data.

Whaling Prevention

Whaling prevention techniques are similar to phishing prevention techniques (see previous). In this case however, it is imperative that executive-level employees are educated on the possibility of these scams.

Cyberattacks are an ongoing and ever-evolving threat to healthcare providers. **The key is to be prepared**. Develop a system of protecting against cyberthreats, detecting them, responding to them, and recovering from them. With a solid system in place, a provider can prevent attacks and mitigate the effects of breaches should they occur.

BLUE ORANGE® COMPLIANCE

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com