YOUR RESPONSIBILITY/

- **Be suspicious of emails** containing “urgent” requests for personal information, multiple spelling mistakes, and poor grammar.
- **Do not open links** sent through suspicious emails, instant messages, or text messages.
- **Avoid filling out any forms** in email messages that ask for personal information.
- Always use a **secure website** when submitting credit card or other sensitive information via the Internet. Cybercriminals are now able to spoof “https://”, so enter website addresses manually to avoid malicious links.

CONTACT/

[1] http://www.net-security.org/secworld.php?id=16626
[2] http://www.phishingbox.com/social_engineering_testing_facts.html
[3] http://www.symantec.com/security_response/publications/threatreport.jsp

S443-023

SECURITY AWARENESS
YOUR BEST DEFENSE

PHISHING

PHISHING
KEEPING YOUR IDENTITY & PERSONAL INFORMATION SAFE.

The Counterintelligence Awareness Library

PHISHING/

Cybercriminals will use every method available to gain valuable information from you. That's why you need to know about phishing. Phishing employs social engineering tactics meant to defraud you with the ultimate goal of using your stolen information to gain access to your identity and even your money.

PHISHING: The use of email messages, websites, and text messages laced with malicious software that, once downloaded to your personal computer, steals your personal identification information.

Keeping It Real

While running errands, you receive an "urgent" text message from your bank; your account has been compromised which may result in a loss of funds if not immediately addressed. The message asks you to click on a link in order to change your password and PIN. You notice the name of your bank is misspelled as are other words in the message.

SPEAR PHISHING: The use of targeted phishing tactics which seek to defraud specific organizations or users of confidential or sensitive data through email spoofs and fraudulent hyperlinks.

Keeping It Real

You receive hundreds of messages each day. One in particular catches your eye as the sender isn't someone you've ever had contact with before and the subject line is written in broken English. When you open the email, there's a brief note concerning your organization and a request for immediate action through a link. When you hover over the link, the caption actually contains a strange URL.

WHALING: The use of phishing and spear phishing tactics to defraud prominent high-ranking individuals such as senior executives and members of leadership teams; also known as "The Big Catch."

Keeping It Real

As Associate Director of your section, it isn't uncommon for you to receive messages directly from your senior leader; however, this message in particular strikes you as odd. She's asked you to open and fill out the forms compressed in a .zip file attached to the message and submit them through a specified online site. The directions are vague and there are glaring grammatical errors within the message including a typo in her own name.

A phishing attack has three characteristics: a **LURE**, a **HOOK**, and a **CATCH**.

LURE/

An enticement delivered through email encouraging you to follow a spoofed hyperlink to a malicious website — also known as a **hook**. It could also be in the form of an executable file hidden in an attachment that you are tempted to open, thereby launching a malicious process on your computer.

HOOK/

A malicious website, provided within the emailed lure, designed to look and feel like a legitimate site. The **hook** asks you to disclose personal information once you reach it.

CATCH/

The originator of the phishing message uses the information collected from the **lure** and **hook** to steal your funds and identity.

60%

of targeted phishing attacks used the **name of a financial institution** to gain access.[1]

91%

of targeted attack campaigns use **spear phishing tactics.**[2]

Phishing and social engineering attacks resulted in the **compromise of over 552 million identities.**[3]