Objective

• Inform and increase the awareness of all Department of Defense personnel of the dangers and threats imposed on DoD information systems as a result of “spear-phishing” emails.

• Instruct personnel on how to recognize these email threats while offering methods to help counter the threat.

Instructions
- To advance to the next slide, click the button.
- Click to return to the previous slide.
- Click on the hyperlinked (blue, underlined) text to get more information on an item.
- Click to return from the hyperlinked location.
Phishing is a criminal activity using social engineering techniques.

“Phishers” attempt to fraudulently acquire sensitive information, such as passwords, personal information, military operations, and credit card/financial details, by masquerading as a trustworthy person or business in an electronic communication.

BUT, DID YOU KNOW…….
Hidden Threats of “Phishing”

Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software.

What this means…
These emails may contain mini-programs that will be installed on your computer. They may capture your keystrokes or capture your personal files and send them to people they shouldn’t be going to … without you knowing it!!!
Hidden Threats of “Phishing”

Most phishing attempts are for identity theft, but there is a rise in attempts at gaining access to online banking, federal, and defense information.

These hidden/unknown threats can capture your passwords/login credentials and also compromise unclassified, but yet sensitive, information that can put Department of Defense operations at risk.
What is “Spear Phishing”?  

**Spear Phishing** is a **GREATER** threat!!!

Spear Phishing is a **highly targeted** phishing attempt.

The attacker **selectively chooses** the recipient (target) and usually has a **thorough understanding** of the target’s command or organization.
What is “Spear Phishing”?  

The attacker may:

- Address the recipient by name
- Use lingo/jargon of the organization
- Reference actual procedures, SOPs/TTPs, or DOD Instructions

The email may appear very genuine. Sometime these emails have legitimate operational and exercise nicknames, terms, and key words in the subject and body of the message.
Phishing is not anything new and many of you may have seen examples in emails from your personal / at-home email accounts.

Common Examples of Phishing

- You may have seen emails that appear to come from your bank or other online financial institutions.

Commonly Seen Commercial Examples: eBay, PayPal, all banking and financial institutions
Phishing Email sent portraying Bank of America, Military Bank

Entices the user to complete a survey and receive a $20 or $25 credit

Bank of America

Military Bank

Dear Customer,
Bank of America Military Bank is doing a 20$ Reward Survey. Bank of America Military Bank will add $20 credit to your account just for taking part in our quick 5 easy question survey. To get advantage of this offer click on the link below.

< URL REMOVED >

This message has been sent only to our special customers.

Thank you,

Bank of America Military Bank Customer Service
Convincing website linked from BOA Military Bank email
Bank of America Military Bank

Convincing website linked from BOA Military Bank email
Should I be worried?

YES, this is occurring within DOD

The attacker’s primary focus is to get you to open an attachment or follow a web link. These actions may install the malicious software.

Most spear phishing attacks within DOD are not for identity theft.
Everyone within DOD is a target. Attempts have been seen at all levels and areas. Military, Civilians, Contractors All Ranks All Services All Geographic Locations

Discovered “spear phishing” messages within the DOD can be very convincing
• “From” field of an email can be easily faked (spoofed). It might appear completely correct, or have a similar variation.

account_security@mypay.com

• On the other hand, the message may come from a legitimate email account, because that account has been compromised.

john.smith.yourboss@yourbase.mil

This can occur when the attackers obtain someone’s login credentials and email contacts in their address book in order to obtain more accounts.

How can I be sure?

Is the message digitally signed?
Other recognition factors of phishing attempts:

1) Generic Greeting
2) Fake Sender’s Address
3) False Sense of Urgency
4) Fake Web Links. Deceptive Web Links. Email is requiring that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment.
5) Emails that appear like a website
6) Misspellings and Bad Grammar
Recognition (Example 1)

Sanitized example of a message with a link to a website that installs malicious software. **DO NOT FOLLOW THESE LINKS**

From: FamilyCare@dhhs.gov
To: [Redacted]@navy.mil
Cc: 
Subject: Care Your Family

Child and Youth Services is an integral part of the Army mission. Our new program support the Soldier which in turn enhances Army readiness. In other words, a soldier can concentrate on his/her mission knowing that their children and youth are safe and supervised by trained and professional staff while participating in quality developmental programs. If you are that soldier, visit our website:

http://familysupport.[-].com/newprogram.html
Recognition (Example 2)

Sanitized example of a message with an attachment that contained malware.
DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL

NOTE: VALIANT SHIELD was an actual exercise event. Message was sent from a supposed exercise account.
Sanitized example of a message with an attachment that contained malware. DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL.
Sanitized example of a message with an attachment that contained malware.

DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL.
Prevention (as a receiver)

Be cognizant and vigilant of this threat.

Before clicking on any weblink within a message or opening up an attachment, be sure the source of the email is legitimate. Is it digitally signed?

The links and attachments can contain malware, spyware, viruses, and trojan horses.

If you click on these illegitimate links/attachments, your computer or account will likely be compromised.
At a minimum, Digitally Sign All E-mails?

If your position involves official direct email contact with outside DoD entities, digital signatures might not be an option.

If this is the case, be suspect of the format and enclosed attachments with these individuals.
Note on Operations Security (OPSEC)

Users should **digitally sign and encrypt** all messages that contain: (at a minimum)

- For Official Use Only (FOUO)
- Privacy Act / personal information
- technical and contract data
- proprietary information
- foreign government information
- financial information
- source selection information
Do not send emails using “HTML” formatting.

Use “Plain Text” or “Rich Text” formatted emails.

“Plain Text” (or ASCII) is preferred because Rich Text looks the same as HTML formatting.

How do I set this up?
The importance of digitally signing your messages can’t be stressed enough. To date, there are no known “spoofs” to digital signatures, other than compromised PKI credentials due to negligence.
Be aware of current information systems threats and targets within DOD

Command and organization Information Security professionals should be following these current threats and continually educating you on them. Specific reports and alerts are published by JTF-GNO.
• JTF-GNO Portal:
  NIPRNET:  https://www.jtfgno.mil (CAC required)
  JTF-GNO J2/J3 Alert 066-06 (PDF, CAC required)
  SIPRNET:  http://www.jtfgno.smil.mil

• DOD Information Awareness Training
The JTF-GNO directs the operation and defense of the Global Information Grid across strategic, operational, and tactical boundaries in support of DoD’s full spectrum of war fighting, intelligence, and business operations.
Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

All Social Engineering techniques are based on flaws in human logic known as cognitive biases.

[Cognitive biases won’t be expanded here, but it involves the different ways we all perceive reality and how “bad people” use these facts to get what they need.]
1) In Outlook, in the menu bar, select “Tools” -> “Options”
2) Select the “Mail Format” tab and select “Plain Text”
3) Click on “Internet Format” (then… next slide)
4) Under “Outlook Rich Text” options, select either “Convert to Plain Text format” or “Send using Outlook Rich Text format”
Sign a Message

When composing a message in Outlook, ensure you sign the message by selecting the button below.

To encrypt, select the envelope with the blue lock icon.