Uncle Sam WANTS YOU TO LEARN OPSEC

OPSEC

FOUR THINGS EVERY SAILOR SHOULD KNOW:

1. *What is OPSEC?*

OPERATIONS SECURITY

It is a systematic, proven process that identifies, controls and protects sensitive information about a mission, operation or activity.

2. *What does it do?*

IT KEEPS OPERATIONS SAFE

When OPSEC is effectively employed it denies or mitigates an adversary's ability to compromise or interrupt a mission, operation or activity.

3. *How does it work?*

Through proper consideration of each of the five steps within the OPSEC process and the process injected in all plans.

4.

OPSEC IS EVERYONE'S RESPONSIBILITY.

USE IT TO PROTECT YOUR COMMAND, SHIPMATES AND FAMILY.

SOCIAL MEDIA RESPONSIBILITY

The More You Know!

KEEP SENSITIVE INFORMATION SAFE

DANGEROUS ☒	SAFE ☑
I work as an intel officer at 6th Fleet in Naples.	I am in the U.S. Navy, stationed in Naples.
On USS George H.W. Bush, we're heading back to Norfolk in 12 days!	On USS George H.W. Bush... Can't wait to get home soon!
On USS Mahan, pulling into Dubai tomorrow.	Excited for our upcoming port call!

We Want YOU! To Be Aware of Your Social Media Presence

✓ DO

* Check your privacy settings often.

* Be aware of your family's social presence. Talk to them about OPSEC and what details they can share socially.

* Follow and share:
official U.S. Navy sites
OMBUDSMAN page
Command social media

✗ DON'T

* Accept friend requests from strangers.

* Share personally identifiable information

* Post information you wouldn't share in other social settings. If you wouldn't say it, don't post it.

* Share U.S. Navy information that has not been officially released.

* Post details about ship movements or taskings

Email Phishing

☒ NEVER SHARE ANYTHING ONLINE YOU WOULD NOT TELL DIRECTLY TO THE ENEMY

☒ NEVER POST PRIVATE OR PERSONAL INFORMATION

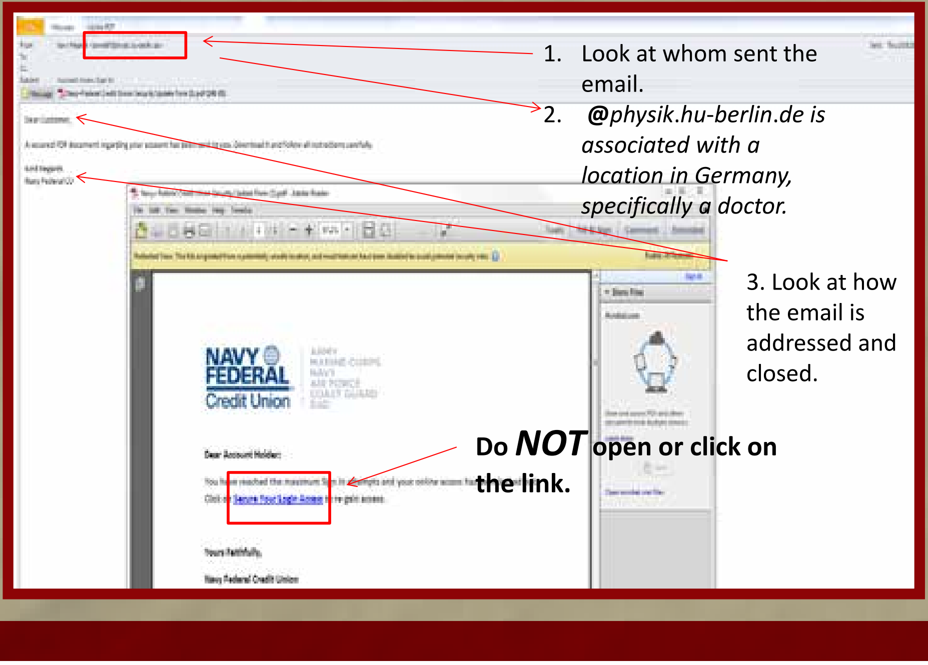
☑ ASSUME ANY INFORMATION YOU SHARE ELECTRONICALLY WILL BE MADE PUBLIC

PHISHING SCAMS TEND TO HAVE COMMON CHARACTERISTICS THAT MAKE THEM EASY TO IDENTIFY:

* Spelling and punctuation errors
* Scare tactics to entice a target to provide personal information
* Sensational subject lines to entice targets to click on attached links or provide personal information
* Include redirect to malicious websites which require you to input usernames and passwords to access
* Try to appear genuine by using legitimate operational terms, key words and accurate personal information
* Fake or unknown sender

When in doubt about a suspicious email from a supposed bank, call your financial institutions or check with your command Information Assurance (IA) lead. Your command IA can also assist with other types of suspicious email

Commercial e-mail is vulnerable to attack. DoD policy currently allows users to receive and access commercial email via DoD systems. However, with ever-increasing threats and damage to systems, the DoD will take action to reduce vulnerabilities to our systems. This includes blocking access to commercial email, scanning incoming email, filtering “junk” email, etc.



Dear Customer,

Kind Regards,
Navy Federal CU

Dear Account Holder:

Yours Faithfully,

Navy Federal Credit Union

1. Look at whom sent the email.
2. *@physik.hu-berlin.de is associated with a location in Germany, specifically a doctor.*
3. Look at how the email is addressed and closed.

Do *NOT* open or click on the link.