Your Role in Keeping the Navy Cybersecure

- Don’t take the bait! Always verify sources of emails and the links in emails. If you’re directed to a site for an online deal that looks too good to be true, it probably is.
- Stay on known good websites. Avoid websites that are not business related or are not known good websites.
- Don’t connect unauthorized devices to the network. Unauthorized devices may contain software that can allow an attacker inside the Navy’s network.
- Remove your CAC or lock your computer. Don’t make it easy for an inside attacker by leaving your computer unlocked when you’re not using it.
- If you use passwords, make them strong. Don’t use easily guessed or weak passwords and safeguard them so they can’t be stolen.
- Safeguard your personally identifiable information. Attackers can use information they’ve obtained about you to appear legitimate so they can trick you into surrendering data they need to breach our networks and systems.
- Don’t use systems in unauthorized ways. The Navy has established policies to protect itself from compromise. Don’t put others at risk by using systems in ways that aren’t authorized.

What the Navy is Doing to Stay Cybersecure

- Making significant investments in solutions for reducing vulnerabilities, detecting attacks, and protecting systems and networks.
- Dividing our networks into segments to better detect intruders, prevent them from moving freely within the and isolate compromised segments during recovery procedures.
- Selecting and hardening critical subsets of systems.
- Modernizing systems and networks.
- Developing technical standards and instituting processes that ensure cybersecurity is addressed throughout the lifecycle of systems.
- Making investments in the training of the cybersecurity workforce.
- Making policy and process changes to improve the Navy’s cybersecurity posture.

Cybersecurity is commanders’ business and requires an “All Hands” approach

- All Users of Navy Networks and Systems: Follow these guidelines and adhere to cybersecurity policies, directives and best practices.
- Navy Leaders: Give cybersecurity the priority it deserves and set the example for others.

Report suspicious or unauthorized cyber activity to your Information System Security Manager (ISSM).

The Cyber Threat

The Anatomy of a Cyber Attack

Your Role in Keeping the Navy Cybersecure

What the Navy is Doing to Stay Cybersecure

One sailor leaving a watertight hatch unsecured can put the entire crew in danger. One sailor not following cybersecurity policy can put the Navy’s network, data, and systems at risk.
The Cyber Threat

Cybersecurity is Critical to the Navy’s Warfighting Capabilities

The Navy’s warfighting platforms, communications systems, and business systems rely on information technology. Cybersecurity protects them from being compromised.

The Cyber Threat is Real

Cyber adversaries want to steal or corrupt the Navy’s data, shut down our business systems and networks, and compromise the systems that run our facilities, ships, aircraft, and weapons.

Adversaries are Trying to Exploit Us Now

The software and equipment that protects the Navy’s networks detects and prevents many attempted exploits each day. The well-publicized compromises below are a reminder that skilled, determined adversaries have been able to breach cyber defenses before and they are looking for weaknesses now.

- 2018: US acknowledges Russian hacking, infiltration of its power companies.
- 2015: Joint Chiefs of Staff’s network hacked.
- 2013: Attackers compromise the Navy’s network.

A Risk to One is a Risk to All

Compromising the watertight integrity of the ship threatens everyone on the ship. Similarly, an exploit in one part of the Navy’s network can jeopardize other systems and data because attackers can move across the network to other targets once they’re inside it.

Cybersecurity is Important All of the Time

A ship’s readiness varies depending on where it is in the maintenance cycle but there is no comparable ebb and flow for the Navy’s systems and networks. The Navy has to protect itself all of the time from cyber exploits because attempts are relentless and they can have serious consequences to our warfighting capabilities.

The Anatomy of a Cyber Intrusion

Step 1: Recon – “Finding an Unlocked Door”

Gather information about targeted networks and systems. Attackers get the information needed to break in using several techniques, including trickery (“social engineering”). They trick users into surrendering data using techniques such as:

- **Phishing** (“fishing”) – by clicking on a link in what appears to be a legitimate email (“taking the bait”), users are directed to a fraudulent web site that installs bad software on their computer or captures data they enter on the website. Opening an infected email attachment can also install bad software on the recipient’s computer.
- **Water Holing** – users who happen to visit a fraudulent web site are exploited in the same way as those who take the bait in phishing attacks.
- **Pretending** to be someone legitimate because they’ve been able to obtain personally identifiable information about you.

Outside bad actors can break **weak passwords** while bad actors inside the Navy can steal passwords. Insiders can also hijack unattended computers, which allows them to quickly move to step 2.

**81% OF COMPROMISES USED STOLEN AND/OR WEAK PASSWORDS**

From Verizon’s 2017 Data Breach Investigations Report

During the first step, adversaries also use software to learn what software is being used on the targeted network.

Step 2: Intrusion – “We’re In”

Exploit known software problems that haven’t been corrected on the targeted network. Once inside the network, attackers can look for information that will give them greater access to systems and data or allow them to move to other targets in the network. If attackers want to shut down a network, they can attempt to overwhelm it with communication requests.

Step 3: Install Bad Software – “The Waiting Game”

Install software that will provide “back door” access to the network, allow remote control of software, or cause harm. Adversaries can bypass the first two steps by tricking someone to attach an unauthorized device (with bad software on it) to the network or doing it themselves if they’re an insider.

Step 4: Transfer Data – “Get What They Came For”

Transfer data to a location where it can be exploited. For adversaries interested in stealing data, they will move it to a location outside the compromised environment so they can attempt to crack the encryption.

Step 5: Clean Up – “Leave Without a Trace”

Erase any trace of the intrusion.