REDUCING PERSONAL CYBERSECURITY RISK

Much of our focus for Cybersecurity Awareness Month is on how the Navy's cybersecurity is threatened by nation states, ideologically motivated hackers, cyber criminals, and malicious insiders. Our cybersecurity workforce and Cyber Mission Forces battle these cyberspace adversaries every day.

But just as importance is for each and every one to pay close attention to your own cyber vulnerabilities, at work and at home. Those same adversaries mentioned above can target you whether you are at work or on a personal device outside of work.

Cyber criminals use some of the same tools and techniques as these bad actors to target anyone who has a personal computer, smart phone or smart device. They are primarily interested in financial gain but may hack for other illegal purposes. Regardless, you are the front line that is defending your personal data and devices from their attacks.

The Department of Homeland Security (DHS) has produced a series of short, information-packed, easy-to-read "tip sheets" for protecting yourself online. These guides are available at https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019 but we have reposted tip sheets for protecting yourself on the home front at https://www.navy.mil/local/cyberawareness/.

SHAKE UP YOUR PASSWORD PROTOCOL

According to National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.

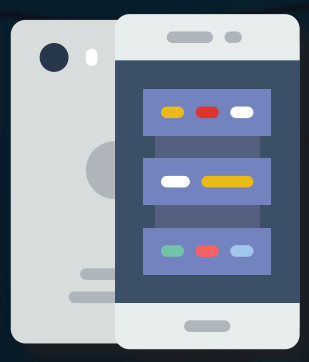
DOUBLE YOUR LOGIN PROTECTION

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

PLAY HARD TO GET WITH STRANGERS

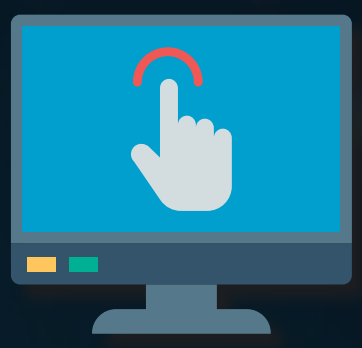
Cybercriminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate— or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender.

KEEP TABS ON YOUR APPS



Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.

NEVER CLICK AND TELL



Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and your physical belongings—online and in the physical world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are – and where you aren't – at any given time.

IF YOU CONNECT, YOU MUST PROTECT

Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with antivirus software.

STAY PROTECTED WHILE CONNECTED

Before you connect to any public wireless hotspot – like at an airport, hotel, or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with "https://" when online shopping or banking.