Huntington
Ingalls
Industries

memo

To: All HII Employees

From: Bharat Amin, Executive Vice President and Chief Information Officer

Date: July 16, 2020

Subject: COVID-19 Cybersecurity Working from Home: Routers Tips

Dear HII Employees:

As part of a comprehensive cybersecurity program, including user awareness training and education, we want to share information that helps keep you and our company safe. A recent article in SC Magazine provided valuable information about how employees working from home could be exposed to hacking attempts.

Home routers are a common piece of network hardware that allow communication between your home network — such as your personal computers and other connected devices — and the internet. And just like any piece of information technology infrastructure, routers can have vulnerabilities leaving them susceptible to cybersecurity attacks. While we would never say we are immune to this threat from an HII perspective, our primary safety net on this and other devices on a home network is the requirement to utilize our virtual private network, or VPN, with company devices.

In a July 7 article, SC Magazine reported that the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE in Germany inspected 127 routers from several vendors and discovered vulnerabilities in all of them. According to the study, 46 routers did not get any security update within the last year. “Many routers are affected by hundreds of known vulnerabilities. Even if the routers got recent updates, many of these known vulnerabilities were not fixed.”

Here are five work-from-home cybersecurity tips related to routers for you to keep as a reference guide to educate yourself and others, as this applies to your home security and safety as well.

1. **Use the strongest encryption protocol available. It is recommended to use the combination below:**
    - Wi-Fi Protected Access 2/3 (WPA 2/3)
    - Personal Advanced Encryption Standard (AES)
    - Temporary Key Integrity Protocol (TKIP)
2. **Change the router’s default administrator password.**
    - Change your router’s administrator password to help protect it from an attack using default credentials.
3. **Change the default service set identifier (SSID).**
    - Sometimes referred to as the “network name,” an SSID is a unique name that identifies a particular wireless local area network (WLAN). Instead of Linksys4482 or ATT7389962, choose a name without any personal information such as: FootballFan4, The LAN before time, SkyNet2020, or Happy Wifi Happy Lifi.
4. **Upgrade firmware.**
    - Check your router manufacturer’s website to ensure you are running the latest firmware version. Firmware updates enhance product performance, fix flaws and address security vulnerabilities.
5. **Monitor for unknown device connections.**
    - Use your router manufacturer’s website to monitor for unauthorized devices joining or attempting to join your network.

Remember, we all are the first line of defense when it comes to protecting HII’s network. Let’s continue working together toward keeping HII’s digital infrastructure and sensitive data safe.