GENERAL DYNAMICS
Bath Iron Works

SECURITY AWARENESS REMINDER
04/09/2020

COVID-19 Related Cyber Threats

The US Department of Homeland Security (DHS) has issued a bulletin warning about an increase in cyber threats and phishing by malicious actors who are preying on concerns over the COVID-19 situation. These attacks are being waged by cyber criminals and nation states alike.

The bulletin summarizes the following threats:

- Email and SMS phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution, using coronavirus- or COVID-19- themed lures
- Registration of new web sites referencing coronavirus or COVID-19 in their names
- Attacks against remote access and teleworking infrastructure.

What you can do to help:

- Follow this guidance from DHS to help spot phishing:
    - **Authority** – Is the sender claiming to be from someone official (e.g., your bank or doctor, a lawyer, a government agency)? Criminals often pretend to be important people or organizations to trick you into doing what they want.
    - **Urgency** – Are you told you have a limited time to respond (e.g., in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
    - **Emotion** – Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or attempt to tease you into wanting to find out more.
    - **Scarcity** – Is the message offering something in short supply (e.g., concert tickets, money, or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.