Department of Homeland Security Warning About Increased Cyber Attacks

January 9, 2020

The Department of Homeland Security (DHS) is warning businesses that there will likely be an increase in cyber threats due to heightened tension with Iran. They advise that you should expect and be prepared for an increase in phishing attacks. Phishing is when someone sends you a deceptive email in an attempt to steal information or infect your computer with malware.

As part of their warning, DHS also recommends that you make sure that your systems and data are backed up and tested, and that you implement multi-factor authentication where possible.

Below is a short list of best practices for evaluating email and website links:

- **Know the red flags** (Grammatical errors or typos, incorrect or unfamiliar email address, scare tactics and a sense of urgency)
- **Think twice before clicking** a link or downloading a file from an unknown external source.
- **Verify all websites.** Many nefarious players will create domains that are similar to a real one. An example of this would be ANCHLN.com vs Anchin.com. At first glance it is easy to miss the mistake. Trust, but **verify!**
- Use **different passwords** for all sites. Strong passwords are key. That being said, you should always use different passwords for each and every site. You can utilize password management tools like Lastpass or Dashlane to help you store and remember these secure passwords.
- **Never** share your password with anyone.
- All emails that contain personal identifiable information (**PII**) should only be sent through a **secure** email platform.

To discuss these and other matters of importance related to cybersecurity, contact your Anchin Relationship Partner or Russell Safirstein from Redpoint Cybersecurity at 212.840.3456 or russell@redpointcyber.com.