CYBER DEFENCE INTELLIGENCE CENTER

November 3, 2020

Holiday Cyber Protection

SCOPE: This intelligence briefing affects all Industry Segments and Organizations.

As the holiday season approaches, and with added complication of the pandemic, email scammers are in full force. This time of year you can expect a lot of phishing attempts. The FBI has seen a significant increase in the frequency and sophistication of email-based attacks.

Bad actors are attacking the healthcare industry specifically right now.

Trying to take advantage of the fact that everyone is busy and distracted this time of year, bad actors will use a variety of scams to trick targets. Here are some common phishing strategies:

- A link in an email that asks you to click and perform a task
- An executive asking you to perform a task that involves making a purchase
- A business partner asking to change Banking information
- Another employee sending a file for review, that is not expected.

There are some indicators in place to help you identify these attacks:

- {EXT} before the Subject line of the email indicates that the email is not from someone within your company
- There are usually errors that do not make sense or seem odd in the request
- The sender's email address does not match their email Display name. (i.e. Betsy Jones, <badactor123@gmail.com>)
- Any email containing a link

These attacks can be devastating if they contain Ransomware or Malware. Everyone should exercise "Healthy Paranoia" and be skeptical of all emails.

It is very important that you take time to read your emails carefully, especially when you are being asked to perform a task. Best practice is to pick up the phone and verify that the person who is requesting you to perform the task is actually the real person, and under no circumstance should you provide any personal information or click on any links.

If you have any questions or need assistance determining if an email is legitimate, contact your information security team.

If you see something, say something!

Prepared by the Cyber Defense Intelligence Center Analysis Team.