Debrief

COVID-19 RAPID RESPONSE CALL
THURSDAY, APRIL 30, 2020

PANELISTS

- Michelle Kook, Intelligence Analyst, FBI Cyber Intelligence Integration Unit
- Elizabeth Burns, Intelligence Analyst, FBI Critical Infrastructure and Cyber Intelligence Unit
- Harold Davis, Supervisory Special Agent, FBI Cyber Division/Mission Critical Engagement Unit

Cyber Vulnerabilities

- During January, February and March the FBI received 1,200 complaints for COVID-19 scams.
- Institutions of higher education and law enforcement are targets for phishing and ransomware.
- The COVID-19 pandemic has led to a spike in businesses teleworking to communicate and share information over the internet. With this knowledge, malicious cyber actors are looking for ways to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities.
- Cyber actors may use any of the below means to exploit telework applications.
  - Software from Untrusted Sources
  - Communication Tools
  - Remote Desktop Access
  - Supply Chain Laptop Rentals

Teleworking Tips to Protect You and Your Organization

Do:

- Select trusted and reputable telework software vendors; conduct additional due diligence when selecting foreign-sourced vendors.
- Restrict access to remote meetings, conference calls, or virtual classrooms, including the use of passwords if possible.
- Beware of social engineering tactics aimed at revealing sensitive information. Make use of tools that block suspected phishing emails or allow users to report and quarantine them.

- Beware of advertisements or emails purporting to be from telework software vendors.
- Always verify the web address of legitimate websites or manually type it into the browser.
- Ensure that patches, software and virus protection is up-to-date.
- Educate employees about steps to protect against cybercrime.

Don't:

- Share links to remote meetings, conference calls, or virtual classrooms on open websites or open social media profiles.
- Open attachments or click links within emails from senders you do not recognize.
- Enable remote desktop access functions like Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) unless absolutely needed.

Collaborating with the FBI Field Offices

- The 56 FBI field offices provide trainings and briefings on cybercrime, and many of the offices have task forces involving local and state law enforcement agencies. Campus public safety agencies should get to know the agents in their respective field office.
- The field offices also work closely with campus chief information officers to prevent cyberattacks, and hold two academies a year for private sector and educational CIOs. Campus public safety agencies should have a relationship their respective CIO.

For further information on these topics, the FBI has produced these public service announcements:

https://www.ic3.gov/media/2020/200401.aspx

https://www.ic3.gov/media/2020/200406.aspx

https://www.ic3.gov/media/2020/200420.aspx