Cyber Threats and Cyber Hygiene During the COVID-19 Pandemic Crisis

A Pandemic Resource from NCSC

March 24, 2020 | Version 1

Bad actors take advantage of crisis situations when people are stressed, distracted, and emotionally vulnerable. Immediately after this pandemic started taking root, Homeland Security and the Cybersecurity and Infrastructure Agency (CISA) were advising about the expected increase in phishing, spear phishing, and scam activity. Government organizations have always been a target, and this pandemic offers exponentially more vulnerabilities to exploit. The following are a few cybersecurity tips and reminders that are particularly important during this pandemic crisis.

Use CISA.gov as a resource for cybersecurity information, security strategies, planning guides, and tips. CISA regularly issues alerts and updates bulletins to reflect current threats and patch releases.

Communication

Have a clear communication strategy. Ensure employees can differentiate between official communications and well-disguised phishing attempts. Socially engineered emails about health advice are on the rise and often contain links or other payloads to steal credentials and infect devices.

- Consider using a public-facing official information page and a separate, internal one for employees.
- Communicate official information through official mechanisms and accounts only.
- Avoid using links in email communications; advise employees to be suspicious of emails that contain links or attachments.
- Be alert for “smishing” attacks using SMS, text, and messages with links.

Social engineering

During a crisis, the public is more vulnerable to social engineering tricks. This includes government employees. “Smart computing” information, alerts, and reminders should be shared frequently with staff. All staff working remotely must understand their individual responsibility to be vigilant in protecting the court’s data and network by protecting their individual devices.

- COVID-19-themed phishing attacks and scams are on the rise. As this pandemic intensifies, phishing attempts and scams will increase.
- Teach “smart computing,” test periodically, and remind frequently.
- Prevention is worth the effort and can save time and resources.

Information/disinformation

Employees may see an increase in scams that include offers for hard to purchase items such as masks, hand sanitizer, and highly coveted toilet paper. Some may offer a miracle cure or protection system from COVID-19. Scams can be fueled by disinformation campaigns that increase panic and create unusual demand for certain goods. When products become scarce, people are more likely to fall for scams.

- Remind employees and the public that the Centers for Disease Control (CDC) is the official trusted source of information about COVID-19.

Multi-factor authentication

The best way to protect systems and data is through multi-factor authentication (MFA).

- Require strong passwords if MFA is not implemented.

VPN vulnerabilities

In a March 13, 2020 alert, CISA advised that Virtual Private Network (VPN) are being targeted.[1]

- Provision remote work capabilities to technology security personnel to ensure cybersecurity tasks can be performed regularly.
- Test remote access options for mass usage potential.
- Work with the executive team to prioritize users if resources become overwhelmed.

Principle of least privilege

Use the least privilege approach to limit access and reduce vulnerability.

Monitoring

Security tools are important for monitoring the network environment. Establish a baseline of what "normal" looks like, recognizing that "normal" will change rapidly during this crisis. Facility closures and social distancing mandates have forced a dramatic and unanticipated increase in remote work. To protect those teleworkers, technologists must increase their monitoring activities.

- Monitor logs for unusual logins.
- Ensure attack detection configurations and alerts are up to date

Patches and security updates

Whether the environment is in-house and provider-managed, court IT organizations must ensure software versions are current.

- Ensure patches and updates are rigorously maintained.
- Through configuration management, remote devices should automatically install patches. Instruct employees on how to properly patch and update their remote devices for areas that may not be fully automated.

[1] Alert (AA20-073A). *Enterprise VPN Security* | *CISA*, US Department of Homeland Security - Cyber and Infrastructure, 13 Mar. 2020, www.us-cert.gov/ncas/alerts/aa20-073a.