CIS Center for Internet Security®

Resource Guide for Cybersecurity During the COVID-19 Pandemic

COVID-19 Related Cyber-Attacks

The The Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operations Center (SOC) is also seeing an increase in specific types of attacks. Most of these can be thwarted by sound cyber hygiene, including increased vigilance from employees. Here are the prominent scams our operations center is seeing, and quick tips to help your organization from becoming a victim.

Phishing and Malspam

Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.

- Learn more: **A Short Guide for Spotting Phishing Attempts**

Credential Stuffing

It may have been necessary to make services available to employees remotely, without the time to secure accounts through multi-factor authentication (MFA). Along with securing accounts with MFA, employees should make sure all passwords are secure, and should never reuse passwords on different accounts.

- Learn more: **NIST Multifactor Authentication Practice Guide**
- Learn more: **Security Primer – Organizational Password Best Practices**

Ransomware

In some cases it is possible malspam emails that start a ransomware infection will use a COVID-19 lure. While preventing ransomware attacks from being successful is the best outcome, being prepared with backups is next best.

- Learn more: **7 Steps to Help Prevent and Limit the Impact of Ransomware**

Remote Desktop Protocal (RDP) Targeting

An increase in the number of employees connecting remotely means an increase in the number of systems with RDP (port 3389) open and potentially being scanned. While your workforce needs to access systems remotely, limited and secure access by VPN can reduce the attack surface.

- Learn more: **Security Primer – Remote Desktop Protocol**
- Learn more: **Intel Insights – How to Disable Remote Desktop Protocol**

Distributed Denial of Service (DDoS) Attacks

Downtime from an attack is even more detrimental with a remote workforce. A larger remote workforce can even act as an unintentional DDoS attack, simply because more users are trying to access services at the same time. To handle these possibilities, and ensure you are protected against DDoS attacks, have increased bandwidth allocations ready, temporarily disable unused services to allow for more bandwidth, and discourage your employees from streaming videos, music, or other streaming services through the VPN.

- Learn more: **EI-ISAC Cybersecurity Spotlight – Denial of Service (DoS) Attacks**
- Learn more: **Technical White Paper – Guide to DDoS Attacks**

Also, remind your employees to look out for malicious websites, apps, and non-cyber frauds.

- Learn more: **What You Need to Know About COVID-19 Scams**

Securing Business Networks for the New Normal

Organizations should implement CIS Controls Implementation Group 1 (IG1) in order to enhance cyber hygiene. These 43 actions are prescriptive and prioritized to help prevent many of the previously-mentioned attacks. You can use the free CIS Controls Self-Assessment Tool, CIS CSAT, to measure progress toward implementing the CIS Controls.

These CIS Sub-Controls are particularly important:

- **CIS Sub-Control 8.2:** Ensure Anti-Malware Software and Signatures are Updated
- **CIS Sub-Control 10.1:** Ensure Regular Automated Backups
- **CIS Sub-Control 10.2:** Perform Complete System Backups
- **CIS Sub-Control 10.4:** Ensure Protection of Backups
- **CIS Sub-Control 10.5:** Ensure Backups Have at Least One Non-continuously Addressable Destination
- **CIS Sub-Control 12.4:** Deny Communications Over Unauthorized Ports
- **CIS Sub-Control 17.6:** Train Workforce on Identifying Social Engineering Attacks

Learn more: **CIS Controls Implementation Group 1**

Securing Employee Home Networks

While conducting business through a VPN can add a layer of security, there are simple steps employees can take to secure their home networks. Employees need to know what devices they are using while working from home. Once they've identified the devices they're using, have them download the instruction manuals from the respective manufacturer websites. These instruction manuals will give them step-by-step instructions on how to enable security settings like these:

1. Practice smart password management and enable two-factor authentication (2FA) wherever possible.
2. Enable automatic updates for all routers and modems. If equipment is outdated and can no longer be updated, it should be replaced.
3. Turn off WPS and UPnP.
4. Turn on WPA2 or WP3.
5. Configure the router or modem's firewall with a unique password and enable the firewall.

Learn more: **CIS Controls Telework and Small Office Network Security Guide**

Employee Personal Device Security

Some employees may be using personal equipment instead of, or alongside, company-issued hardware. Here are some of the steps employees should take to secure their personal devices, especially when they're using them for work purposes:

- Learn more: **CISA Home Network Security Tips**

Patching

Patching systems to remedy known vulnerabilities continues to be essential. Your organization's plan for doing so may need some adjustment with a largely remote workforce.

- Learn more: **Cybersecurity Challenges of a Sudden Remote Workforce**

Home Computers

Recommend employees implement security on these devices including installing anti-virus, firewall, and anti-spyware, and apply security settings in web browsers.

Printers

Employees should look up printer security for their printer make and model to ensure security of the device and network connection. If printing, use an appropriate shredder based on company best practices.

USB Devices

Staff should use only company-approved USB devices.

Storage

Designate how and where an employee can store sensitive information. Use hard drive encryption on work laptops or external hard drives.

Access by Others

People who work from home during the occasional weekday usually don't have a full house, but they might now. Ask employees to keep work devices for professional use only and lock their devices when they step away from them. Innocent activity on a work computer could lead to a breach. This is also a good opportunity to educate family on cybersecurity.

Secure Video-conferencing

Video-conference capability has become a staple to help employees continue to meet face-to-face while working apart. Keeping meetings private and password-protected, with a unique password for each meeting, are essential for ensuring security.

- Learn more: **CISA – FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing**

Additional Resources

- MS-ISAC Webinar: **The First Severe Pandemic of the Information Age**
- SANS Institute: **Tips to Secure Your Organization in a Work-From-Home Environment**
- SANS Institute: **SANS Security Awareness Work-from-Home Deployment Kit**
- Global Cyber Alliance: **Work From Home. Secure Your Business.**

COVID-19 Indicators of Compromise

- Anomali: **Defend Your Organization Against [COVID-19] CoronaVirus-Themed Cyber Attacks**
- DomainTools: **Free COVID-19 Threat List - Domain Risk Assessments for Coronavirus Threats**
- MalwareBazaar: **MalwareBazaar Database**
- PhishLabs: **COVID-19 Threat Intelligence**

Free Tools

- **Quad9:** You can point your DNS server to this system, which will block suspicious requests from your system to malicious domains or IP addresses.
- **KnowBe4's Ransomware Simulator:** Scans for ways into your network by malicious actors.
- **Shodan:** Find vulnerable devices on your network.
- **Censys:** Find vulnerable devices on your network.