COVID-19 Telework Security and Privacy Concerns and Considerations

April 16, 2020

As companies and schools have shifted to remote work and tele-education during the global COVID-19 pandemic, threat actors, unfortunately, are capitalizing on opportunities to exploit human vulnerabilities and the increased use of technology, including virtual environments.

Since the outbreak, security intelligence communities have observed the steady rise in COVID-19 themed scams – phishing emails designed to look like they're from the CDC and WHO, advertisements aimed at selling bogus protective gear or medications to treat coronavirus symptoms, tax collection threats, and fake websites that attempt to install malware onto a victim's device. Also, with the increased use of video teleconferencing ("VTC") tools to conduct business or education remotely, cybercriminals are taking advantage of potential security gaps in these products to hijack calls, access or steal sensitive data, and conduct other malicious activities.

Here are several tips for protecting critical information and users from ongoing security threats amid the crisis:

- Avoid clicking on links and opening attachments in unsolicited or unusual emails and text messages.
- Only utilize trusted sources, such as official government websites, for accurate and fact-based information.
- NEVER provide sensitive or personally identifiable information, such as your SSN, bank account/credit card information, date of birth, or login credentials (username and password), over the phone or by email.

- Apply two-factor authentication to verify user identity whenever possible.
- Conduct due diligence of third-party products and solutions (e.g., VTC, VPN, VOIP, instant messaging) to understand their security controls and features, default settings, and limitations.
- Ensure virtual meetings are private by requiring a password for entry or controlling access.
- Make sure software is up-to-date and critical vulnerabilities are patched.
- Immediately report suspicious emails and activities to your information security team.

For additional information issued by the CDC, CISA (Cybersecurity and Infrastructure Security Agency), FBI, and NIST (National Institute of Standards and Technology), see the following resources:

- CDC | COVID-19-related Phone Scams and Phishing Attacks
- CISA | Defending Against COVID-19 Cyber Scams
- CISA | Security Tip: Using Caution with Email Attachments
- FBI | PSA: Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments
- FBI | Exec Discusses COVID-19-related Schemes
- FBI | Guidance on Defending Against VTC Hijacking
- NIST | Cybersecurity Blog on Preventing Eavesdropping and Protecting Privacy on Virtual Meetings

Stay safe and continue to be security aware and vigilant!