TELEWORK ESSENTIALS TOOLKIT

# TELEWORKERS – YOUR HOME NETWORK

## DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

## ACTIONS

### 1 CONFIGURED AND HARDENED

Ensure your home network is properly configured and hardened. Change all default passwords and use strong, complex passwords. Ensure your home wireless router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum and disable legacy protocols such as WEP and WPA. Ensure the wireless network name (service set identifier [SSID]) does not identify your physical location or router manufacturer/model. Use a protective Domain Name System (DNS) service. (TECHNICAL)

- CISA Tip on Securing Wireless Networks
- Center for Internet Security (CIS) Telework and Small Office Network Security Guide
- GCA Cybersecurity Toolkit for Small Business
- Work From Home Coalition Guidance

### 2 SECURE PRACTICES AND ORGANIZATIONAL POLICIES

Follow secure practices and organizational policies for handling sensitive data including: personally identifiable information (PII), protected health information (PHI), classified materials, intellectual property, and sensitive customer/client information. Avoid storing or transmitting sensitive organizational information on personal devices. If personal devices are approved for telework use, regularly apply the latest patch and security update on your devices. Follow your organization's guidance on securing your devices, including implementing basic security controls like password authentication and anti-virus software. (TACTICAL/TECHNICAL)

- Cyber Readiness Institute Data Protection Basics for Remote Workers
- Cyber Readiness Institute Authentication/Passwords Guidance
- GCA Cybersecurity Toolkit for Small Business

### 3 OPENING EMAIL ATTACHMENTS AN CLICKING LINKS

Use caution when opening email attachments and clicking links in emails. Increase your awareness of phishing tactics, current phishing campaigns, and social engineering to effectively report suspicious emails and communications. (TACTICAL)

- CISA Tip on Using Caution with Email Attachments
- Cyber Readiness Institute Phishing Guidance

### 4 COMMUNICATING SUSPICIOUS ACTIVITIES

Make sure you know the procedures for communicating suspicious activities to your organization's IT security team and promptly report all suspicious activity. (TACTICAL)

- Telework Security Basics

OTECH

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance