1901 Group

INFOGRAPHIC SERIES

# WORKING FROM HOME SECURELY

**Working from home** as part of a fully remote workforce in the age of serious cyber attacks brings unique challenges to maintaining strong security. It's a time of mixing business with personal that's unavoidable for nearly everyone.

## THREATS — WHAT TO **LOOK OUT FOR**

### PHISHING

Social engineering that uses email to trick you into providing confidential information. Keep an eye out for the signs.

### VISHING

Social engineering that uses the phone to trick you into providing confidential information. Verify who you're talking to.

### ILLICIT ACCESS

Allowing your spouse, children, or roommates to use your work laptop can inadvertently lead to giving malicious actors access to our network. Use it for work only.

## ACTIONS — WHAT YOU CAN **DO TO BE SAFE**

### STAY UPDATED

Follow your employer's protocol to keep your operating system up to date. Don't share your password with anyone.

### VPN

Use your company's VPN connection when necessary and disconnect when you're not using it.

### BACKUP

Backup everything using secure cloud storage. Don't get stuck losing your work; recovery will only be more difficult while we're all working away from the office.

Reach out to your company's IT support staff with any information security related questions or to report an information security breach of any kind.

## TELEWORK SECURITY CHECKLIST

Telework offers the flexibility to work from anywhere, anytime. Working remotely lets us get the job done in unforeseen circumstances and unconventional places. Ensuring that your home network is protected from threats is critical. Use this checklist from GSA **to keep your personal network, data, and devices safe.**

### PROTECT YOUR HOME NETWORK

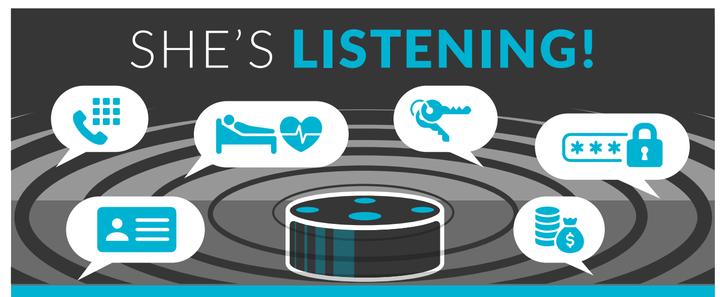
- ☑ Use a router or switch with a built-in firewall
- ☑ Change the network name (SSID) default
- ☑ Turn off the broadcast of your SSID so it can't be found by others
- ☑ Change router admin username/password
- ☑ Don't install personal firewall software on your work computer without approval

### PREVENT MALWARE

- ☑ Use updated anti-virus software
- ☑ Apply software updates and enable automatic updates
- ☑ Do not open email attachments from strangers
- ☑ Do not use free, unsecured WiFi; Use your mobile hotspot instead
- ☑ Turn off Bluetooth when not in use

### PROTECT YOUR PERSONAL DEVICES

- ☑ Enable WiFi Protected Access 2 (WPA2) on the wireless connection devices
- ☑ Change passwords regularly, use a strong password that is at least 8 characters long with a mixture of upper and lower case letters/symbols
- ☑ Maintain different passwords for all accounts, do not store written/typed passwords - use a password manager
- ☑ Keep mobile devices locked using a strong password, fingerprint, or other methods
- ☑ Review your apps routinely and remove unused apps and/or any apps you did not install yourself
- ☑ Install Find My Phone (iOS)/Find My Device (Android) to quickly locate and remotely wipe your phone if lost




Don't have **confidential conversations** near a **smart speaker**

Devices such as Amazon's Alexa, Google Home/Nest, and others are susceptible to a variety of exploits and threats. Make sure you do not discuss privileged information in the same room as your smart speaker.

CONTENT SOURCE: GSA Telework Security Best Practices | gsa.gov
DESIGN: John Bennett | Creative Director | 1901 Group