# 20 WAYS TO BUILD YOUR
# *SECURITY FORTRESS FROM ANYWHERE*

## AT HOME
- ❑ Have separate devices for work and personal use
- ❑ Connect to Ethernet (wired) or at least WPA2 (Wi-Fi Protected Access 2) for a secure wireless connection
- ❑ Use a VPN (Virtual Private Network) whenever possible to access employer systems/data
- ❑ Keep router and modem firmware up-to-date
- ❑ Secure IoT devices (smart speakers, appliances, etc.) - use strong, unique passwords whenever possible

## CLOUD SECURITY REMINDERS
- ❑ Enable multi-factor authentication (MFA) that requires a separate device when possible
- ❑ Practice good password hygiene
- ❑ Never save passwords in your browser
- ❑ Keep work-related communication to systems approved by your organization
- ❑ Check privacy/location/security settings on apps and restrict any unnecessary access

## TRAVELING
- ❑ Don't use public Wi-Fi when accessing confidential info, use a personal hotspot instead
- ❑ Keep devices secure and accounted for at all times
- ❑ Disable automatic bluetooth pairing
- ❑ Don't allow your devices to auto-join unfamiliar Wi-Fi networks
- ❑ Don't use borrowed chargers or public charging stations

## PHYSICAL SECURITY REMINDERS
- ❑ Never use unknown USB devices
- ❑ Always lock your workstation
- ❑ Keep confidential information secure - use privacy screens and headphones if necessary
- ❑ Implement a clean desk policy by removing business documents, notes, etc.
- ❑ Don't allow unauthorized individuals to tailgate

access one

www.accessoneinc.com | info@accessoneinc.com | (800) 804-8333

*Source: KnowBe4, Inc.*