CRI REMOTE WORK RESOURCES

CYBER READINESS INSTITUTE + CYBER HAWAII

Top Three Dos & Don'ts for Remote Workers

Cyber criminals are using the COVID-19 pandemic to take advantage of remote workers by stealing their personal and professional information. To protect yourself in this growing threat environment and new security reality, outlined below are simple dos and don'ts to be more cyber ready.

Since the start of the pandemic, everybody has learned to take three simple actions to stay healthy. Wash your hands for 20 seconds. Don't touch your face. Stay six feet apart. Sure, it took some behavioral change, but you're probably used to it after a few weeks. You need to take the same "can-do" attitude in changing simple behaviors regarding how you use your computer, tablet and smartphone.

Cybersecurity takes a collaborative community effort, similar to what is required to fight the coronavirus. So, please share this guide with your co-workers, family and friends.

Do

- Use separate passwords/passphrases for work and personal use – ideally at least 16 characters
- Update all software on all devices regularly – ideally on a weekly basis
- Use multi-factor authentication (whenever possible)

Don't

- Click on links or attachments in emails from senders you can't verify
- Send financial or personal info by email until you've called to verify the transaction
- Use USBs, public computers or Wi-Fi (if at all possible)

Look for more advice and tools from the Cyber Readiness Institute (CRI) in the coming weeks. We are committed to being a key resource in helping small and medium-sized enterprises (SMEs) balance remote work and cybersecurity. To access additional guides on cyber readiness for remote workers, visit **https://www.cyberreadinessinstitute.org/remote-work-resources**

To learn more about our free **Cyber Readiness Program** and how to become a Cyber Leader, visit **www.cyberreadinessinstitute.org**.

About the Cyber Readiness Institute

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). The self-guided, online Cyber Readiness Program is available in Chinese, English, French, Spanish, Portuguese, Arabic, and Japanese. Please contact us with questions, comments or success stories (**guides@cyberreadinessinstitute.org**).