CYBER READINESS
INSTITUTE

Data Protection Basics for Remote Workers

In response to COVID-19, there was a rapid shift to remote work. Now, as the pandemic enters a new phase, we are seeing another shift to a hybrid work environment, in which some employees will be working from home, some from the office, and some from both home and office. This new reality will likely last through the year, at least, raising new challenges in protecting data.

Protecting your organization's data is important to the security and sustainability of your organization and you, as an employee, play a critical role in this protection. If each person is conscientious, the organization can build a culture of cyber readiness that spans from the home to the office.

For many remote workers, the data you will be accessing are documents (word processing, spreadsheets, or presentations), files (accounting), or databases (customer management or order tracking). Your company's most critical asset is data and strong cybersecurity protects your data. To adhere to basic rules for data protection, you will likely need to change certain aspects of your behavior.

To start, always be aware of what device (e.g. phone, laptop) you are using (company or personal), how you connect to the Internet (e.g. home WiFi, café, library) and your company's network (e.g. do you use a VPN or not), and how you access, work on, transfer, and store data (e.g. email, apps, etc.).

guide@cyberreadinessinstitute.com

Here are the key data protection tips for working remotely and/or in a hybrid remote/office environment. We've grouped the tips into a few basic categories:

Accessing Data

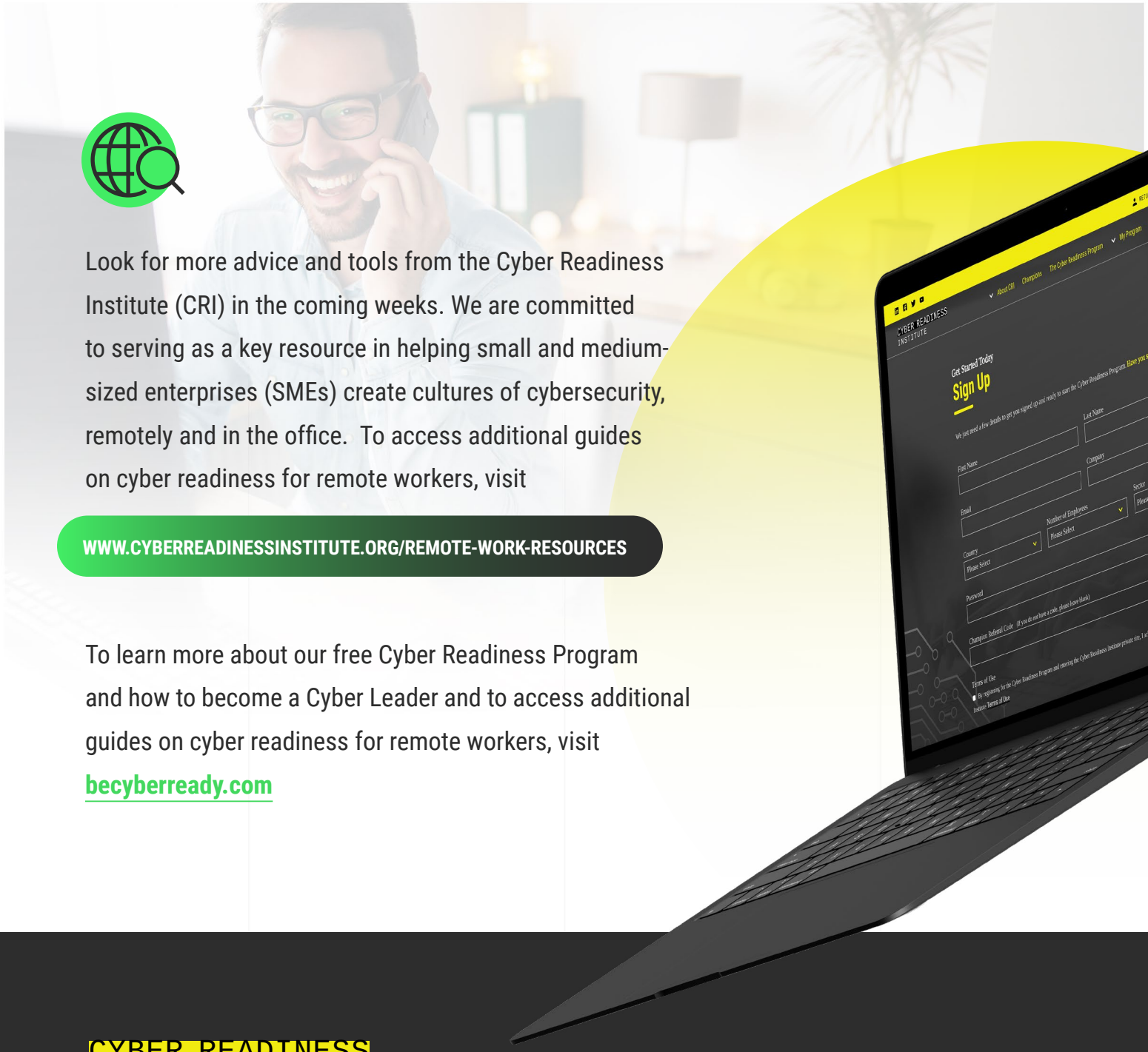
- Never share your passwords or log-in credentials
- Know what information is considered confidential and with whom it can be shared

Storing and Using Data

- Know where you are storing your documents – company server, cloud storage, personal cloud storage, personal computer, removable media (USBs)
- If you are using a shared computer, never store confidential information on it
- Mark sensitive information with appropriate naming (e.g., confidential, proprietary)
- Ensure that sensitive information is protected at home in the same ways you do at work.
- Use your company's document naming and version control procedures; if there are none, add a version number to your document names (e.g. New_Product_ Announcement_V1.docx becomes New_Product _Announcement_V2.docx)
- You should avoid saving documents to your personal computer to work on them

Sharing Data

- Never share sensitive (i.e., confidential, proprietary) documents without approval – even with others in your organization
- Use encryption whenever possible; if you absolutely need to send confidential information as an attachment, make sure the document is encrypted or password protected



Look for more advice and tools from the Cyber Readiness Institute (CRI) in the coming weeks. We are committed to serving as a key resource in helping small and medium-sized enterprises (SMEs) create cultures of cybersecurity, remotely and in the office. To access additional guides on cyber readiness for remote workers, visit

WWW.CYBERREADINESSINSTITUTE.ORG/REMOTE-WORK-RESOURCES

To learn more about our free Cyber Readiness Program and how to become a Cyber Leader and to access additional guides on cyber readiness for remote workers, visit **becyberready.com**

CYBER READINESS
INSTITUTE

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. To find out more, visit **www.becyberready.com**.