CYBER READINESS
INSTITUTE

Creating Good Cyber Ready Habits–One Person at a Time

The hybrid (remote-office) workplace is here to stay. Companies of all sizes are facing the realization that there is going to be a more permanent "new reality" to the workplace. Responses to the COVID-19 pandemic forced companies to rapidly deploy new technology to enable remote work. People scrambled to adapt their behavior to the crisis, but now it's time to establish sustainable cyber readiness habits that can secure the hybrid workplace.

CRI is focused on helping small and medium-sized enterprises (SMEs) develop a cyber ready culture. The purpose of this guide in our Hybrid Workplace series is to help you develop good cyber readiness habits. We will follow-up with other guides on implementing practical policies and demystifying technology for the hybrid workplace.

The goal is to build a culture of cyber readiness in your organization that includes all people and all locations. As employees go back and forth from home to office, cyber readiness habits need to span multiple locations across multiple devices.

Culture in your organization is built through the behavior of each individual. In organizations, people tend to emulate the behavior of their direct supervisors and people see and learn from the behaviors of others. When enough people develop good cyber readiness habits there is a tipping point and the overall culture evolves to embrace cyber readiness.

Your organization can reduce cybersecurity risk if your employees develop good cyber readiness habits. To do so, requires discipline, especially at the beginning of this cultural change.

Think about seatbelts in cars. Today, people reflexively reach for the seatbelt when they get in the car. It's a habit. But it wasn't always this way. It took behavioral change. Of course, there is the annoying beep if you forget to buckle-up. So, technology (the annoying beep) helped develop or sustain the habit. The same is true of cyber readiness. Technology can assist you to do the right thing, like turning on auto-updates for software. But ultimately it is up to you to develop good cyber habits – and to encourage others in your organization to do the same.

guide@cyberreadinessinstitute.com

Remember, a cyber ready culture is built one person at a time. Developing a habit takes a little time each day and discipline. Most experts say it takes about a month for something to become a habit and after three months you do it without even thinking about it.

Here are some tips on how to develop good cyber readiness habits for the hybrid workplace. You can use these for yourself and to lead others in your organization.

Log-off your computer every time you step away from it – whether you're at the office or home, log off if you step away. This means close your laptop or put your desktop computer to sleep.

Use multi-factor authentication every day – we know it's a pain in the beginning but take one action every day that requires you to receive and enter the multi-factor authentication code on your work or personal device. Once you get used to it, you'll see it's not a big deal.

Strengthen your passwords – think about your (probably long) list of passwords. Change one password each day to make it a 15+ character passphrase. Don't stop until your passwords are changed on all personal and work devices. Each passphrase should be unique and make sure to use a completely different theme for business and personal use.

Verify that you have backups – with people working from multiple locations, documents are often scattered on different devices. Different versions of the same documents exist in different places – and there may not be a backup. Backups also make you resilient against ransomware.

Ask one person each day how they are doing with their cyber ready habits – whether in-person or on video conferencing, get in the habit of asking others about their cyber habits. Start by asking someone, "Have you used multi-factor authentication today?"

Stay tuned as we continue our hybrid workplace series to demystify cybersecurity by providing tips for managers and employees.

About CRI

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). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.