CYBER READINESS
INSTITUTE

Securing a Remote Workforce

The next several months will offer challenges for nearly every person around the world as normal routines are uprooted by the coronavirus. Children and teachers will be collaborating remotely, workers will do their jobs from home and business owners will run their companies from their living room, instead of the boardroom.

We are fortunate that today's advanced technologies will enable many of us to continue our work with little disruption. The availability of inexpensive computing power, access to cloud services, and high-speed Internet connections makes remote work a viable alternative that could help slow this global health crisis.

But as more people join the cyber workforce, we need to be aware that we are exposed to other risks. As every workplace, small and large, goes remote, we all need to be hyper-vigilant about good cyber hygiene practices.

Here are some critical steps that all of us can take to protect our online safety and security.

As every workplace, small and large, goes remote, **we all need to be hyper-vigilant about good cyber hygiene practices.**

guide@cyberreadinessinstitute.org

Passwords

Passwords remain the frontline defense for accessing critical data and applications. Remote working adds to the complexity of relying on the security of every employee's home network.

- Ensure that the home router password is not easily guessed and does not include your address or personal names.
- Enable multi-factor authentication (password + one other requirement such as a text message) whenever possible, including access to critical data in cloud applications used for data and document sharing.

Patches

Operating system security patches must be accepted and stay up-to-date.

- Require employees to have their operating systems set to automatically update.
- Remind employees — weekly — to accept all relevant security patches.

Phishing

The more of us who are online over the upcoming weeks, the more we can expect an increase in online scams, social engineering, and phishing attempts. Hackers and criminals are sure to use concerns about virus spread and the insatiable desire for news to trick people.

- Always "mouse" over the email sender's name to determine the sender's true origin to ensure the sender's name is not fraudulent.
- Most individual ransomware emails are fake. If you can, ensure that you have the emails verified by a security professional before responding.
- Every company should identify a point of contact within the company whom every employee should contact when he/she receives a phishing email or individual ransomware. This awareness and communication will inform employees of current tactics of malicious actors.

Social Distancing

Social distancing works online too.

- Limit the amount of personal data that you are sharing on social media to reduce your threat landscape.
- Share all data via online secure cloud applications. USB memory sticks should not be used to share data as they can spread malware.