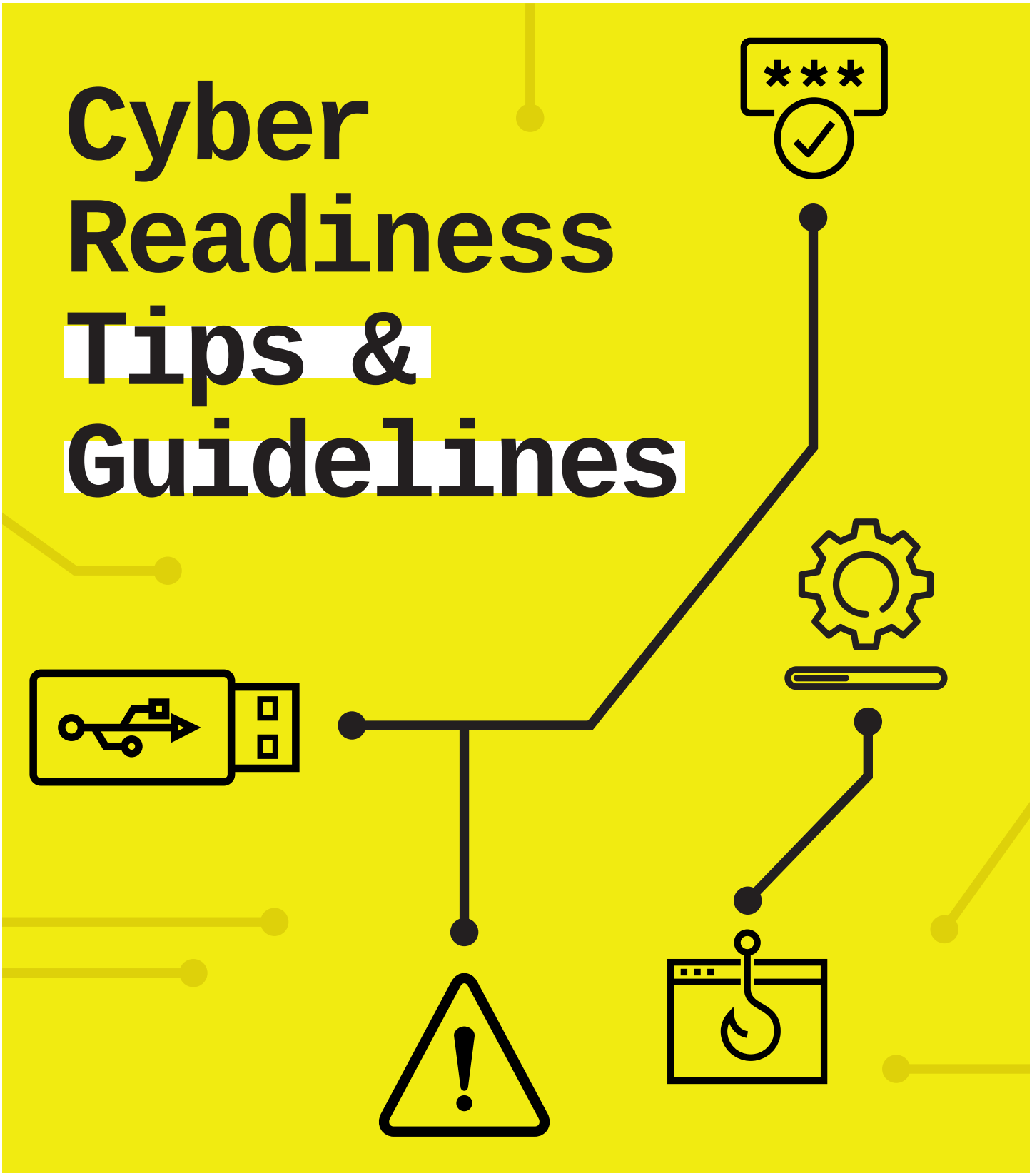
CYBER READINESS
INSTITUTE

Cyber Readiness Tips & Guidelines



Most companies have guidelines that all employees are required to follow about basic responsibilities like showing up to work on time, or what to wear to the office, or how to request vacation time. Guidelines on basic cyber readiness should be included as well. After all, the security of your data and systems has a huge impact on your business and your customers. We recommend you use the following tips and guidelines to help inform your employees and hold all team members accountable to create a culture of cyber readiness.

Passwords

Strong passwords are essential to securing your systems and accounts. Whether you're accessing work emails, retrieving files from a shared hard drive or logging into any online services, the password, or pass*phrase* you use is important. You can even add another layer of security with two-factor authentication. Two-factor requires you to input a unique code that is sent to your mobile device for each new login. Two-factor authentication creates an important security link between the password and the person.

We encourage you to use these guidelines for your employees:

1. Use a long passphrase that includes special characters.
   For example, pick a line from your favorite TV show, movie or song.

2. Never use the same passphrase for personal and work accounts,
   and do not share your usernames and passwords with anyone,
   including team members.

3. Use two-factor authentication any time it is available.

Software Updates

It’s critical to keep all software and operating systems up to date.
Each update released from the software provider can include important fixes and patches that protect your software and systems from attacks. Many companies assign one person to manage updates for all company computers, which is preferable. Alternately, you can require each employee to manage their own updates. Either way, regular updates are critically important.

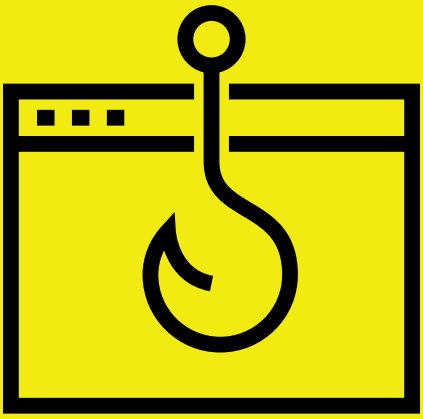
We recommend the following guidelines for updates:

1. Turn-on the auto update feature on all devices and software whenever it is offered.

2. Regularly update all of the operating systems, software and apps for computers, phones and tablets as soon as you receive a notification that indicates an update is ready.

3. Update all software and apps – both those issued by the company and those downloaded by the employee.

Phishing



Phishing is one of the most common, and most dangerous cyber issues today. Often a phishing email may look like a real, safe message. But opening it may result in downloading software viruses or giving attackers access to your data. Everyone receives phishing emails. That's why it's important to know what to look out for. Awareness is the best defense against phishing.

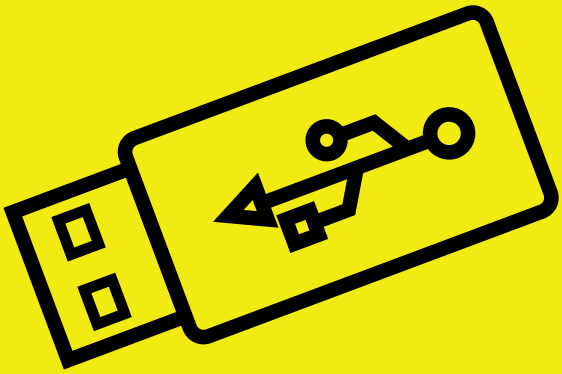
Here are a few tips that will help:

1. Check the sender's email address and any other identifying information, such as the company logo, street address, and contact details for any inconsistencies, or signs it may be fake.

2. If you are not familiar with the email sender, do not click any links or download any attachments in the email.

3. Delete any suspicious emails and immediately empty your trash.

USBs and Removable Media



USB drives are handy for sharing files between computers, but they can also be used to deliver viruses and malware. There's no way to tell where the drive has been, or who may have compromised it. The best way to avoid risk with USB drives and other removable media is to avoid using them completely. However, instituting an outright ban on USB drives may be a challenge.

Therefore, we recommend all employees follow the guidelines below:

1. Introduce easy-to-use alternatives to USB drives, such as cloud-based file-sharing services so that USB drives are less necessary.

2. Set up a computer that is not connected to the company network that can be used as a malware scanner for USB drives, and to remove the needed information from the USBs.

3. Most importantly, use good judgment. If you do not know where the drive came from, do not plug it in.

Incident Response

Cyber readiness is all about taking the right steps to reduce risk, but also being prepared when an incident does occur. Having an incident response plan is a critical step to becoming cyber ready. Think of it like a fire drill – if an emergency does happen, it's important to have a plan in which everyone knows their role.

You'll find further information on incident response in the Cyber Readiness Program, but at a minimum, focus on these three areas:

1. **Prepare:** Make sure all employees conduct regular backups of their work and data.

2. **Respond:** If an attack or issue occurs, immediately disconnect the affected device from the company network. All employees should be required to take this step.

3. **Recover:** Restore the lost data from a backup, and use the incident as a learning experience to reinforce the importance of cyber readiness principles like password security, software updates, phishing awareness and USB safety.

READY TO TAKE YOUR SKILLS
TO THE NEXT LEVEL?

EXPLORE THE CYBER READINESS PROGRAM

The Cyber Readiness Program is a free, online resource that lays out practical steps you can take to assess and improve your cyber readiness. It's easy to use and easy to track your progress. You can work at your own pace. Once complete, you'll receive a Cyber Readiness Certificate to show customers and suppliers that you've taken steps to create a culture of cyber readiness throughout your organization.

Learn more:
https://www.cyberreadinessinstitute.org/the-cyber-readiness-program