CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

The Cyber Readiness Training Toolkit

Everything you need to provide Cyber Readiness Training to your workforce

This Training Toolkit is a part of the Cyber Readiness Institute's Cyber Readiness Program and based on best practices from leading cybersecurity experts.

Foreword by Kiersten Todt, Managing Director, The Cyber Readiness Institute

A Note to the Cyber Leader:

Kiersten Todt

Managing Director, The Cyber Readiness Institute

Your journey through the Cyber Readiness Program has come to its most important point: implementation. Now, it's time for you to take the knowledge you've gained throughout the program, and share that with your colleagues. As your organization's Cyber Leader, you have the ability to affect lasting change in your organization, and in the global value chain at large.

In the following Cyber Readiness Training Toolkit document, we have included key resources to help you communicate cyber readiness best practices across your organization, and do it in a way that drives meaningful change. You'll find email templates that you can copy and customize to message your colleagues. There are checklists to share so that all members of your organization can be held accountable to the same standards in addressing the four core cyber issues. Lastly, there are links to additional resources, both from CRI and from across the cybersecurity community that can provide additional guidance for your team.

Implementation is the most important step in the Cyber Readiness program, because it is the moment that knowledge becomes action. We invite you to use the resources in this Toolkit to create a culture of Cyber Readiness in your organization.

Again, congratulations on your accomplishment, and on behalf of CRI, I wish you and your organization continued success.

About the Program

The Cyber Readiness Program is a simple, practical way for organizations to provide security awareness training to employees and establish sustainable, effective cyber readiness practices. Specifically designed for small and medium-sized enterprises, this Program focuses on human behavior and will help you create a workforce that is empowered, educated, and engaged in effective cyber hygiene practices that directly impact the security and viability of your business.
Learn more at: cyberreadiness.org

Table of Contents

Introduction

How to use the Cyber Readiness Workforce Training Toolkit

This toolkit is intended for the Cyber Leader, and provides everything you need to get your workforce Cyber Ready. With these simple, ready-to-use training materials, you can effectively educate your workforce about the four core cyber issues, as well as clearly communicate your new company policies surrounding them and your incident response plan protocol.

Some of the resources provided in this toolkit include:

- Program Implementation Guidelines
- Workforce Training Outline / Agenda
- Tips for Successful Cyber Readiness Training
- Guidance for incorporating security into your workplace culture
- Ready-to-use email templates to train employees
- Downloadable training videos to save and share
- Reference PDFs to distribute and post in common work area

Requirements Before Training Implementation

Before you implement the Workforce Training outline in this toolkit, make sure that the Cyber Leader has done the following:

Taken the Cyber Readiness Baseline Assessment Survey

The Cyber Readiness Baseline Assessment that's in the "Assess Your Current Cyber Readiness" stage of the online leadership training course should be completed before training implementation.

Understanding and documenting how your organization currently handles passwords, software updates, phishing prevention, and USBs and removable media is an important first step in the path to cyber readiness.

Establishing this baseline provides a practical way to measure success for your organization. After all, you can't improve what you don't measure.

Customized the Cyber Readiness Playbook

The Cyber Readiness Playbook addresses the root causes of most cyber issues and provides step-by-step guidelines for effectively handling these issues at an organizational and individual employee level.

This Playbook codifies the policies and protocols and is the reference source behind the concepts communicated in this training program.

If the Baseline Assessment and Playbook have been completed by the Cyber Leader, then you are ready to move forward with this toolkit and start getting your workforce Cyber Ready!

Preparing to Train Your Workforce

Program Implementation Guidelines

The Cyber Readiness Training is designed to be as concise and actionable as possible for employees. While each training session only involves about 10 minutes of time, each lesson does involve some action on the employee's part, either to set up the protocols in place or to verify the settings on their systems. So that compliance with these policies doesn't unnecessarily impact business operations, we suggest sending one email a week to employees, for a 6-week program length and a final recap email.

Tips for Getting Started

You understand the mission. You have a playbook. You've got an action plan. Now it's time to make an impact! Being intentional in executing this training will help make this Program as successful as possible for your organization. Some things to consider as you make a plan to educate and engage your workforce on these issues:

Be Positive

A positive approach and mindset go a long way in gaining the trust and buy-in that precedes compliance with these policies and practices. Be understanding that change takes time and that people don't mean any harm when they forget or make mistakes.

While you've put in a lot of time and thought into these issues, it's important to remember that most employees likely have not. The exciting part of your role is showing people how simple it is for them to make a huge impact within your organization.

Make a Plan

Treat it like a campaign, with a start and end date for this process and defined goals. Set expectations on what the training will involve and what needs to be changed in how certain processes are done.

Make it Simple

Try to make it as easy as possible for people to get informed and educated on these issues. This could involve some sessions being virtual "lunch and learns" for initial training and Q&A time, follow-up emails to recap content, and positive reminders in various all-hands or team meetings about cyber readiness practices.

Make it Realistic

You're likely eager for success and dramatic improvements but setting realistic goals for implementation is important to avoid frustration. Understand people won't be perfect at first - encourage any and all progress and positive change and provide gentle reminders as needed.

Understand people have a lot going on and often resist change to avoid feeling overwhelmed. Share your passion and enthusiasm for these changes so that people share your excitement and understand this program is worth their time to learn.

Make it Meaningful

Show people how important they are to the success of the company. Connect the dots as to how each person's behavior and habits directly impact their own security as well as their colleagues and beyond.

Make it Stick

Don't assume people will remember everything the first time they're exposed to it. Make sure to use the resources in the communications kit so that there are reminders around the workplace and memos to jog their memory on these issues.

Publicly recognize the effort people put into these practices. Make people feel good for engaging in these behaviors vs controlled, annoyed or hassled by the changes.

Training Program Overview

Here's a quick rundown of what your workforce will learn and accomplish in just a short time with this training:

Know the Four Core Cyber Issues for Business Security

- Learn the 4 biggest sources of cyber breaches and how simple behavior changes can make all the difference

Understand the Core Cyber Policies in your Cyber Readiness Playbook

- Get informed on the new company policies surrounding these areas and understand how these cyber issues should be handled by each employee

Know the 3 Steps in Incident Response & Who To Contact

- Every employee should be aware of the Incident Response Plan and should know what to do in response to a cyber event, who to contact for support and when to reach out to a third party for help.

Understand Their Role in Practicing Cyber Hygiene

- Understand the responsibility that each employee's personal work habits and behaviors play in preventing company data from being compromised, exposing sensitive customer data along with their own personal security.

Learn to Maintain Cyber Readiness & Empowered to Improve

- Resources should be easily accessible, regularly reviewed and incorporated into employee onboarding training to ensure consistency and dedication for maintaining and improving your organization's cyber readiness.

The effort spent on this training is well worth the time. Regardless of current cyber readiness, this Program will improve overall cybersecurity awareness and help to prevent against attacks and reduce the risk associated with the most common cyber issues.

Cyber Readiness Training Implementation

CYBERREADINESSINSTITUTE.ORG

Training Outline

Below is the Cyber Readiness Training Curriculum for this training program, which can be sent via email to your teams or used to guide virtual or onsite training sessions. We recommend implementing the training in the written email format provided to reduce friction and maximize flexibility for employees reviewing this content.

Workforce Training Curriculum

	Content/Topic	Included Resources:
Training Email 1	Our Cyber Readiness Training Begins!	✓ Email Message ✓ Cyber Readiness Overview PDF ✓ Training Agenda
Training Email 2	Strong Password	✓ Email Message ✓ Strong Password Video ✓ Password Guide PDF
Training Email 3	Software Updates	✓ Email Message ✓ Software Update Guide PDF
Training Email 4	Phishing Awareness	✓ Email Message ✓ Catch a Phish Video ✓ Phishing Red Flags Guide PDF
Training Email 5	Using UBSs	✓ Email Message ✓ USB Use Guide PDF
Training Email 6	Incident Response Plan	✓ Email Message ✓ Incident Response Plan PDF
Training Email 7	Core Issues Recap	✓ Email Message ✓ 4 Core Issues Overview
(Optional) Training Email 8	Cyber Readiness Certification & Employee Survey	✓ What it Means to Be Cyber Ready Video ✓ Employee Survey/Assessment

Email Training Templates

Training Email 1

Subject: New Security Awareness Policies & Training

Hi Team!

[ORG NAME] is getting Cyber Ready! What this means for us:

1. **New Employee Policies** - We've added some new policies and protocols to our handbook that provide procedures and guidelines for better security here at [PUNCH]. You can review these policies here. [LINK]
2. **Employee Training** - We're also going to take a few minutes each week to learn about these policies and provide you with the resources you need to implement these changes.

You might be wondering what "Cyber Ready" means. Being "Cyber Ready" means being smart about technology habits and knowing what to look out for to stay safe.

Cybercriminals know how most of us work and they exploit these common habits to get past sophisticated cybersecurity technology. In fact, a handful of behaviors are the source of most cyber breaches and how criminals were able to get in. Fortunately, when we know what to do and what not to do around these four core cyber issues, the chance of these attack methods working goes down dramatically.

1. Passwords - 63% of data breaches result from weak or stolen passwords.
2. Software Updates - 77% of attacks exploited gaps in software already on computers
3. Phishing - 91% of all cyber attacks start with a phishing email
4. USBs and Removable Media - 27% of malware infections originate from infected USBs

Locking down these four areas means that the sensitive data related to [ORG NAME], customers, vendors, and fellow employees is more secure.This is why we're going to be sending out a few brief emails that will provide some basic training about the four core cyber issues and the simple things we can all do to avoid and prevent them.

These emails are a part of the Cyber Readiness Program's cybersecurity awareness training, and cover how to handle passwords, software updates, and USBs, along with phishing awareness training. Addressing these four key issues will dramatically improve your organization's resilience and readiness for a cyber event.

Please note that policy adherence and this training is required. These emails and requests should only take 10-15 minutes to complete, and we request that you reply to your direct supervisor after completing each training session.

The first training email will be sent [MM/DD]. In the interim, please read the Training Agenda PDF and the Program Overview to learn more about this effort.

If you have any questions on this, just let me know!

[EMAIL SIGNATURE]

Training Email 2

Subject: Core Cyber Issue #1: Passwords At Work

Hi Team!

It's our first session in our Cyber Readiness Program training series!

Core Cyber Issue #1 - Passwords

A password is a door into a network, individual or an organization. We use hundreds of passwords and connected devices in our professional and personal lives -- each of these are doors into our company. A weak password is like leaving the door unlocked.

Each of our passwords are gatekeepers to the important information and systems we are trusted with and accountable for. We can't let them be easy targets.

A hard-to-crack password is the first line defense against opportunistic hackers. Making a strong password takes just a few seconds, and is something every [ORG NAME] employee is required to do to help keep our data as secure as possible.

Here's a quick video about how to make strong passwords you can easily remember and use:

[LINK]

We've also updated our company policies around passwords, which applies to all employees and contractors of [[ORG]]. Some highlights of this policy are:

- Use passwords or PINs on all devices, including personal phones and tablets
- Create your passwords using a 15 character passphrase
- Never use the same password for business or personal purposes
- Never use or reuse the same passphrase on two (or more) systems at the same time
- Never share accounts among multiple people
- Enable multi-factor authentication if it is available for any apps used on company devices and personal devices used for business

The attached is a Password Checklist PDF that provides you with step-by-step guidance on implementing this new policy, which you can read in full here [LINK].

Please note that policy adherence and completing the Password Checklist PDF is required for all [ORG] employees. This checklist should only take 10-15 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you've completed this checklist.

If you have any questions about this training or how to use and manage your passwords, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

Training Email 3

Subject: Core Cyber Issue #2: Software Updates

Hi Team!

We're on our second session of our Cyber Readiness Program training series!

Core Cyber Issue #2 - Software Updates

You're probably familiar with those pop-up notifications telling you a software update is available for your computer, laptop, tablet, or mobile device. While it can be tempting to click "Remind me later," that's a bad idea. Software updates repair important security gaps and fix critical bugs that have been identified and should be installed right away.

Not installing these updates leaves the door wide open to known security vulnerabilities that cybercriminals can and do use to get in and make an attack. The infamous WannaCry Ransomware Attack took advantage of an identified security flaw in Windows OS that had already been fixed in an update two months prior. Even though the attack only affected those who had not installed the update, in just 24 hours more than 230,0000 systems were compromised and caused $4B in global damages.

Installing updates can eliminate these easy access points and protect against malware and ransomware attacks. Fortunately, software updates are easy to do.

Most operating systems and software can be set to "auto update," which can automate the installation of updates and minimize the interruption to your work. It only takes a few minutes to make sure or turn on "auto update" for apps, systems and devices, so please do so as soon as possible.

Like we did for passwords, we've also revised our company policies surrounding software updates. These standards apply to all employees and contractors of [[ORG]].

Some highlights from our new policy are:

- **Enable auto-update on all your devices,** including personal devices, such as cell phones and tablets that connect to [[ORGs]] network, including systems (e.g.: Windows, OS X, iOS, Android, etc.).
- **Don't ignore the auto-update notifications.** Once prompted, updates must be installed within 24 hours.

The attached is a Software Update Checklist PDF provides you with step-by-step instructions and links for easily getting this done, which you can read here [LINK].

Please note that policy adherence and completing the Software Update Checklist PDF is required for all [ORG] employees. This checklist should only take 10-15 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you've completed this checklist.

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

Training Email 4

Subject: Core Cyber Issue #3: Phishing

Hi Team!

Ready for our 3rd session in our Cyber Readiness Program training series? Only one more lesson and before our recap and wrap of this training!

Core Cyber Issue #3 - Phishing
Phishing is one of the most widely used cyber attacks. **Anyone with an email account or smartphone can receive a phishing email or text. Phishing attacks use deceptive messages to get sensitive information or access to a network**. These messages try to trick people into **clicking a link, downloading an attachment in the message, or even directly providing sensitive information** like banking details.

Most of us know that the Nigerian prince emailing you asking for a $5,000 wire transfer to his bank account is a scam. **But phishing scams are often really clever and hard to detect** if you don't know what to look for. These messages are **often well-disguised as real communications that a person may legitimately receive.**

In fact, **9 out of 10 cyber attacks start with phishing** because how they do it works so well. While the methods scammers use to launch phishing attacks are always evolving, **most phishing messages use a handful of tricks you can learn to look for** so you don't get duped.

Watch this short video clip to learn some tricks for spotting a "phish" in your messages. [VIDEO LINK]

Our company policies and practices surrounding phishing awareness have been updated, which will apply to all employees and contractors of [[ORG]].

Some highlights from this new policy are:

- Do not provide any personal information via email or take action by opening an attachment, clicking on a link, or entering information in a pop-up box.
- Always check the identity of the sender before clicking on any attachment in the email.
- Look at the full email address of the sender and check for grammar or spelling mistakes.
- If any email doesn't look legitimate, don't open any attachments or follow any directions in the email.
- When receiving a document from an external source, only open it in read/only protected view.
- Bring any suspicious emails to the attention of [CYBER LEADER NAME] or IT staff.

The attached is a Phishing Awareness Checklist PDF provides you with the Phishing Tips from the training, which you can access here [LINK]. Please note that policy adherence and completing the training video and Phishing Awareness PDF is required for all [ORG] employees. This should only take 5-10 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you've completed this checklist.

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

[EMAIL SIGNATURE]

Training Email 5

Subject: Core Cyber Issue #4 - USBs & Removable Media

Hi Team!

Today we're covering the last core cyber issue in our Cyber Readiness Program training series!

Core Cyber Issue #4 - USBs & Removable Media
USBs are a popular and easy way to store and transport files, but they're also easy targets for malicious software.

Hackers can infect USBs with malicious software, such as viruses, spyware, rootware and more that can cause irrevocable damage. Someone who finds a "lost" USB in the parking lot might plug it into their computer to see what's on it and return it to the owner, without knowing the risk before it's too late.

USBs aren't the only kind of removable media device, they can also include:

- Optical Discs (Blu-Ray discs, DVDS, CD-ROMs)
- Memory Cards (Compact Flash card, Secure Digital card, Memory Stick)
- Zip Disks/ Floppy disks
- USB flash drives
- External hard drives (DE, EIDE, SCSSI, and SSD)
- Digital cameras
- Smart phones
- Other external/dockable devices which contain removable media capabilities

We've updated our company policy for USBs/removable media, which will apply to all employees and contractors of [[ORG]]. Some highlights from this new policy are:

- **[[ORG]] prohibits all employees from using USBs and removable media devices,** except in rare and pre-approved circumstances.
- **Employees must exclusively use cloud applications and/or secure email encryption** to share and store all files.
- **Any removable media devices currently in use must be discontinued immediately** and first scanned before transferring the files to the cloud for storage.

The attached is a USB Checklist PDF provides you with the key takeaways on handling removable media, which you can access here [LINK].

Please note that policy adherence and completing the training video and USB Checklist PDF is required for all [ORG] employees. This should only take 5-10 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you've completed this checklist.

If you have any questions about this training or how to use and manage software updates, then feel free to reach out to me directly to discuss.

Next week, we'll be covering our new Incident Response Plan, which will help us prepare for and respond to cyber events and issues that can happen.

[EMAIL SIGNATURE]

Training Email 6

Subject: Our Cyber Incident Response Plan

Hi Team!

Today we're going to cover our Cyber Incident Response Plan!

This will serve as a roadmap for our company as a whole and for every person to determine what to do and how to act when a cyber or security issue occurs.

The cyber hygiene practices we've been learning during this training and our new cyber readiness policies go a long way in reducing our risk of a security breach. But even with the best measures in place, it's important to assume that we will likely have to deal with a security incident at some point.

Our Incident Response Plan equips us to quickly respond, resolve, and learn from every issue that comes up. A crisis can be chaotic and stressful, but having a step-by-step plan ensures that our response to a breach is strategic and effective vs than reactive or unhelpful.

There are three main elements to our incident response:

1. **Prepare**
   - Always make sure to keep backups current and to sync cloud accounts
   - Always stay on alert for suspicious or odd activity
2. **Respond**
   - Always reach out to [CYBER LEADER OR IT CONTACT] if something is acting strange or seems off (computer crashed after opening a file, etc)
   - Immediately stop using/get the device off the network
3. **Recover**
   - Notify all affected parties
   - Reset all passwords and IDs
   - Reinstall software, synced accounts and data backups as needed

We've updated our company handbook with this Incident Response, which must be reviewed and used for all employees and contractors of [[ORG]], which you can access here [LINK].

Please note that policy review and adherence is mandatory for all [ORG] employees. This should only take 5 minutes to do and should be completed by [MM/DD]. Be sure to inform your supervisor after you've reviewed the IRP.

If you have any questions about our Incident Response Plan, then feel free to reach out to me directly to discuss. Next week we'll have a quick recap of what we've learned during this program, and then [ORG] will officially receive Cyber Readiness Certification!

[EMAIL SIGNATURE]

Training Email 7

Subject: Cyber Readiness Recap

Hi Team!

We've now completed the Cyber Readiness Program training series! Let's take a moment to quickly review what we've learned in our journey to Cyber Readiness.

The 4 Core Cyber Issues

Issue #1 - Passwords

- Passwords are doors to our network and data, and weak passwords are easy ways for hackers to gain access. Using weak passwords for user accounts and devices at work can compromise the entire network.
- Use passphrases for each account and turn multi-factor authentication for any account, app or device you use.

Issue #2 - Software Updates

- Software updates fix security vulnerabilities and add new features to your devices, eliminating security weak spots and protecting against malware stealing your data.
- Set all devices to auto-update to ensure software updates are downloaded as soon as they are available

Issue #3 - Phishing Awareness

- Phishing targets individuals by tricking someone into clicking a link or downloading an attachment. These links or attachments can infect the device with malware or allow a hacker to gain access to a person's systems or accounts.
- Knowing how to identify and handle phishing attempts helps protect against any messages that get through email spam filters from succeeding in their attack.

Issue #4 - USBs & Removable Media

- USBs and other removable media can be infected with malicious software and there's no way to tell until it's too late. Many times, people will plug an unknown USB into their computer to see what's on it and infect the entire network.
- Avoid using USBs and removable media devices unless given prior permission and use secure solutions like Cloud and encrypted email for file sharing and storage.

Incident Response Plan

1. Prepare - Always stay on alert & make sure to keep backups current and cloud accounts synced
2. Respond - Always reach out to if something seems off immediately stop using/get the device off the network
3. Recover - Reset all passwords and IDs after any breach
4. Appreciate everyone's time and effort in completing this training as we continue to improve our cyber readiness!

As always feel free to reach out to me directly to discuss if you have any questions.

[EMAIL SIGNATURE]

Workforce Training Resources

Cyber Readiness Training Agenda

Here's a quick rundown of what you'll learn and accomplish in just a short time with this training:

Know the Four Core Cyber Issues for Business Security

- Learn the 4 biggest sources of cyber breaches and how simple behavior changes can make all the difference

Understand the Core Cyber Policies in your Cyber Readiness Playbook

- Get informed on the new company policies surrounding these areas and understand how these cyber issues should be handled.

Know the 3 Steps in Incident Response & Who To Contact

- Every employee should be aware of the company Incident Response Plan and should know what to do in response to a cyber event, who to contact for support and when to reach out to a third party for help.

Understand Your Role in Practicing Cyber Hygiene

- Understand the responsibility that each employee's personal work habits and behaviors play in preventing company data from being compromised, exposing sensitive customer data along with their own personal security.

Learn How to Maintain Cyber Readiness & Empowered to Improve

- Training resources should be carefully read and periodically reviewed to ensure consistency and dedication for maintaining and improving your organization's cyber readiness.

The effort spent on this training is well worth the time. This Program will improve our overall cybersecurity awareness and help to prevent against attacks and reduce the risk associated with the most common cyber issues.

Password Checklist

- [ ] **Always Use A Strong Password or Passphrase**
  - [ ] **Always change default passwords** before first use
  - [ ] **Use a passphrase of at least 15 characters to create your passwords.** A passphrase is part of a sentence, such as “FavVacationYosemite” or a sentence, such as “I like basketball.”
  - [ ] **Check the strength of passwords** before using

- [ ] **Use a Different Password for Every Account**
  - [ ] Make sure **every account uses a different strong password**/passphrase that is **either completely impersonal** or **randomly generated**
  - [ ] **Do NOT use formulas** to create “unique” passwords for your accounts - they are easy to remember but just as easy to crack (PasswordFB, PasswordYT, PasswordGmail, etc)

- [ ] **Enable multi-factor authentication (MFA)**
  - [ ] Enable multi-factor authentication (MFA) on all your accounts, where available

- [ ] **Password Security Tips**
  - [ ] **Delete accounts and uninstall applications** that you no longer use
  - [ ] **Ensure that all your accounts use strong passwords** and that no passwords are being used more than once
  - [ ] Check the security settings on your connected devices, accounts, and applications to see the current or default settings in place
  - [ ] **Check the strength of your current passwords** and update them as necessary
  - [ ] **Never disclose company passwords with anyone.** Always apply new passwords before and after any trip where company data is being utilized on a device.

Software Update Checklist

☐ Download & Turn On Automatic Updates

Ensure all your systems, apps and devices are patched and configured for automatic updates

- ☐ **Apple Products** - iPhone, iPad, Apple Watch or macOS products and software
- ☐ **Android Products** - Any devices, apps or systems powered by Android (can include: smartphones, laptops, tablets, smart watches, home appliances, cars, smart home systems and security monitoring, cameras, smart TVs, game consoles)
- ☐ **Microsoft Products** - Windows operating systems - laptops, desktops, tablets, smartphones, game consoles and more
- ☐ **Other Apps/Platforms/Devices** - Apply patches and configure automatic updates across all other devices and applications (i.e. Office365 suite on a Mac)

☐ Make Prompt Software Updates a Standard Practice

We've added a Software policy from the Cyber Readiness Program to the employee handbook, which outlines expectations surrounding software updates and other important security issues.

- ☐ Turn on auto-updates notifications and don't ignore them
- ☐ Install software updates as soon as you can, ideally within 24 hours
- ☐ Always keep business and personal devices that you use for work updated

Phishing Awareness Checklist

Stay on alert and use this checklist to quickly determine if a strange message could be a phishing attack.

4 Ways to Spot A Phish

1. Check the Header

- ☐ Have I given my email address to this company before?
- ☐ Do I have an account with this company?
- ☐ Does the sender identity match the purpose of email?
- ☐ Is my email listed as the From: address?
- ☐ Is the To: address to undisclosed-recipients or to a large number of recipients you are not familiar with?

2. Check the Content

- ☐ Do links provided in the body of the email look valid?
- ☐ Are there misspelling and typos? How is the grammar and is the tone appropriate?
- ☐ Am I being promised a lot of money for little or no effort on my part?
- ☐ Am I asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process?
- ☐ Is someone asking me for my bank account number, other personal financial information or passwords? ("Verify your account." or "Click the link below to gain access to your account." are common)

3. Consider the purpose of the email

- ☐ Is the issue really as urgent as the sender makes it to be?
  - ☐ "If you don't respond within 48 hours, your account will be closed."
  - ☐ "Failure to do this may automatically render your account deactivated."
- ☐ Why does the sender request confidentiality? How can I tell if the proposed activity is legitimate and authentic?

4. Be cautious with attachments

- ☐ Do not open unexpected attachments.
- ☐ Do not open attachments from strangers. Always be absolutely certain you know the sender first.
- ☐ Do not open unusual attachments.
- ☐ Don't open attachments that come with strange-looking messages.

USB & Removable Media Checklist

Follow these guidelines for using and managing removable media and devices at work

When to Use:

- ☐ **Do NOT use USBs without prior permission** for work or at work
- ☐ **Avoid using removable media** whenever possible
  - ☐ If you are using USBs currently in your role, work with the right people to securely transfer any sensitive data to a secure drive and promptly delete the data from the device after finishing.
- ☐ **Never connect unknown media devices you've found** to a computer. Give any unknown storage device to security or IT personnel.

How to Protect:

- ☐ **Disable Auto-run and Autoplay features** for all removable media or devices. These features automatically run when plugged into a USB port or drive.
- ☐ **Ensure anti-virus solution(s) are installed** on your computer to actively scan for malware when any type of removable media or device is connected.
- ☐ **Ensure that all removable media and devices are encrypted.** This will render any data useless to unauthorized users should the device be lost or stolen.
- ☐ **Always apply new passwords before and after any trip** where company data is being utilized on removable media or device. Never disclose the passwords used with removable media or devices to anyone.
- ☐ **Keep personal and business data separate.** Do not store work data on any personal device and vice versa

Maintaining Cyber Readiness

Measuring & Maintaining Cyber Readiness

Congratulations! Your workforce is now educated on the four core cyber issues and fully equipped with practices and policies that reduce risk from cyber attacks! If you haven't already, take a moment to recognize and appreciate these efforts and the positive impact this work will have for your organization.

Post-Training Reassessment

Now it's time to reassess your organization's cyber readiness so you can see the impact of the program and identify areas to improveand reinforce with employees.

Take the post-training assessment in the online leadership training Program and compare this against the initial baseline to determine progress and areas for improvement.

How often you reassess depends on your time and resources. We recommend evaluating your organization's cyber readiness at
least every six months, with quarterly check-ups.

Establishing A Culture of Cyber Readiness

Cyber Readiness as a Practice

It's important to note that cyber readiness is not a one-time fix, but a continual practice that must be consistently reinforced. To be cyber ready, your people must practice the cyber readiness policies, behaviors, and good habits that have been discussed in the Program every day.

Incorporating these best practices so that they become a habit will be a process for employees. Even with well-executed initial training of your workforce, it will require time, tenacity, and a positive attitude to maintain a culture of cyber readiness.

Tips for Improving Cyber Readiness

- Make these practices part of your new employee onboarding process so that as your workforce grows, your cyber readiness expands
- Conduct a survey at least twice a year to gauge awareness and consistency across your organization
- Periodically check-in, assess, and remind your workforce, either through periodic retraining sessions or with email campaigns at least twice a year
- Use and implement CRI guides and resources to help your organization continue to improve your security posture

Helpful Cybersecurity Resources

Cyber Readiness Institute Guides

- Creating a Cyber Ready Culture in Your Remote Workforce
- Cloud FAQ
- Data Protection Basics for Remote Workers
- Ransomware Playbook
- Securing a Remote Workforce
- Making Your Remote Workforce Cyber Ready
- Top Three Dos & Don'ts for Remote Workers

Reference Links

- 5 Reasons Why You Should Use Cloud Storage Every Day
- How Cloud Storage Works
- Trusted Information Protection on the Cloud
- Use a Passphrase
- Cyber Resilience and Financial Organizations: A Capacity-building Tool Box
- 3 Steps to Block Phishing Scams
- Cybersecurity: 10 Tips to Prepare for Big and Small Threats

About CRI

The Cyber Readiness Institute (CRI) is an 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 businesses. Advancing the cyber readiness of small and medium-sized businesses improves the security of global value chains.
Learn more at: CyberReadinessInstitute.org