CYBER READINESS
INSTITUTE

# Time for the Talk

**HOW TO**
discuss cyber
readiness with
your employees

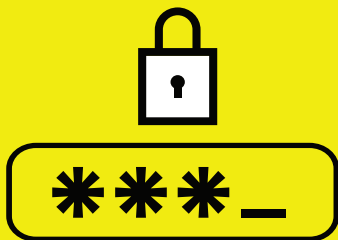# It's important to take cyber readiness SERIOUSLY.

## Your businesses' reputation depends on it.

**BUT HOW DO YOU START
A CONVERSATION IF YOU'RE NOT A CYBER EXPERT?**

It doesn't have to be complex or intimidating. Refer to the questions and answers in this document to talk with your employees about cyber risks, protections and good cyber readiness practices.
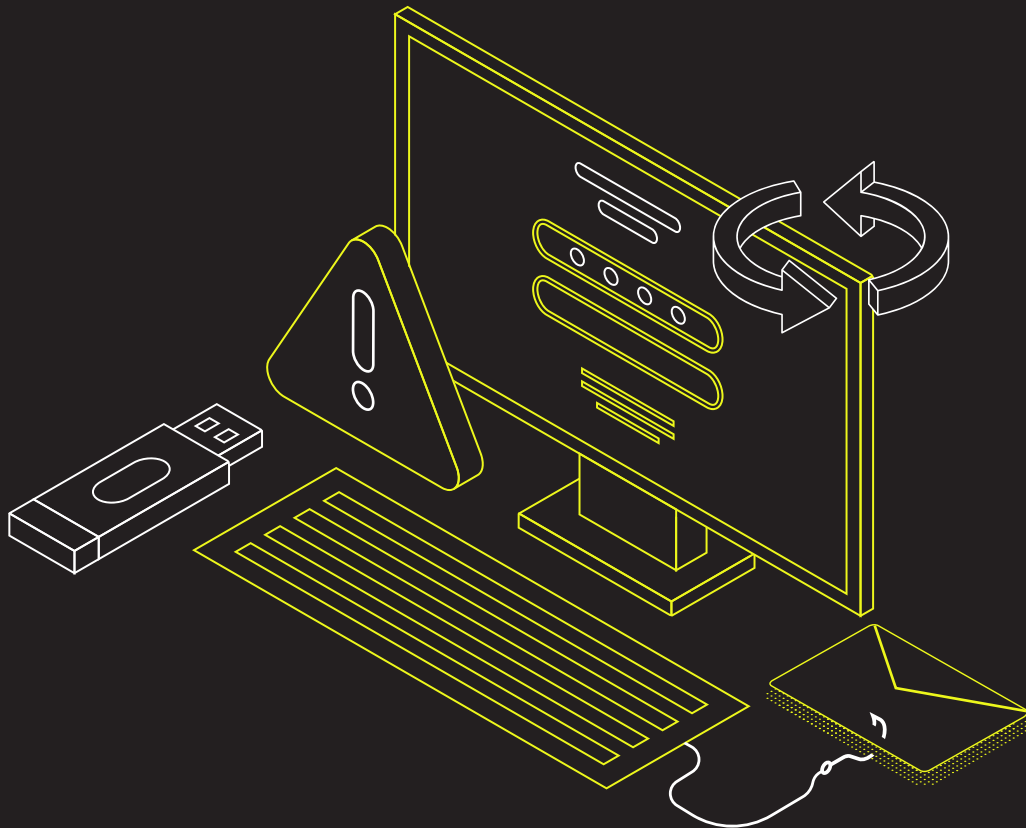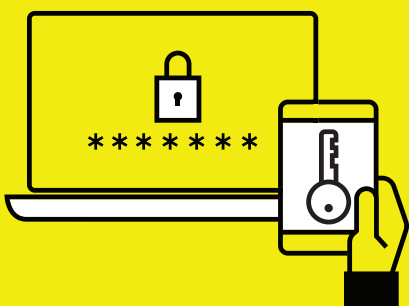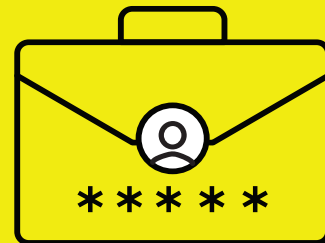
# Passwords

## What is the strongest type of password?

The strongest passwords are: phrases vs single words, random thoughts that form a sentence, a mixture of numbers and characters, uppercase and lowercase letters.

## Should you use the same password for business and personal purposes?

No, do not repeat passwords whenever possible.

## What is two-factor authentication?

Two-factor authentication is a way to confirm your identity through your password as well as another method, such as a text message or email. Two-factor authentication is easy to set up and significantly reduces your chances of being hacked.

# Updates
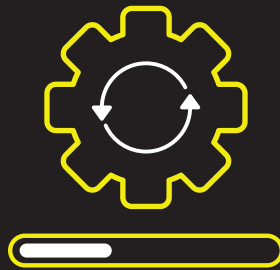
## What are updates?

Put simply, "updates" are new versions of the software and applications on your phone and computer. These updates fix problems and improve security. Installing updates is one of the easiest and most critical cyber readiness measures you can take.

## How can you ensure your devices are updated?

Turn on auto-update notifications and don't ignore the update notifications. Also remember to check third-party applications for updates.

# — 3 —
# Phishing
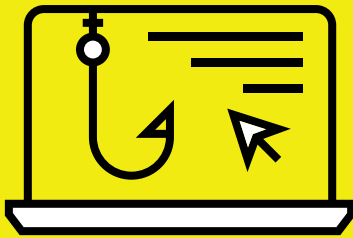
## What is `phishing?`

Phishing is a cyber attack delivered through a phony email. Phishing attacks attempt to use your account to steal personal data or take over your computer. These attacks are often difficult to detect.

## What are `common signs` of a phishing attempt?

- Suspicious email address
- Emails from strangers that include attachments or links
- Spelling errors or broken sentences
- Suspicious emails that ask for personal data

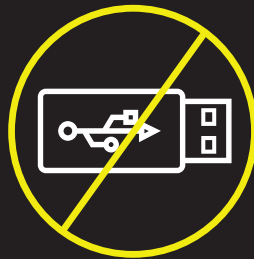## Why is it so important to `be aware` of phishing risks?

91% of all cyber attacks start with a phishing email. 81% of companies that fall for a phishing attack lose customers.

# USBs
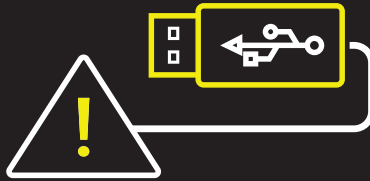


## What's so bad about USB drives?

Over ¼ of malware infections start with an infected USB.
What's more, 87% of employees report losing a USB and not
telling their employers.



## How can you limit USB attacks?

| **Don't use** | **Never use** | **If used,** |
|---|---|---|
| USB drives unless approved by your Cyber Leader | or accept a USB from any external person or company | USBs should be routinely checked for malware |

# CYBER READINESS
## INSTITUTE

**Learn more at**
`https://cyberreadinessinstitute.org`