CYBER READINESS
INSTITUTE

Time for the Talk

HOW TO discuss cyber readiness with your employees

cyberreadinessinstitute.org

It’s important to take cyber readiness SERIOUSLY.

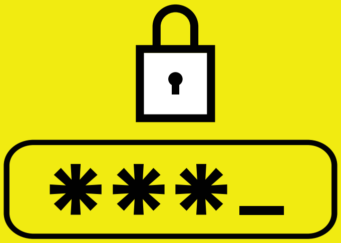
Your businesses’ reputation depends on it.

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.

– 1 –

Passwords+

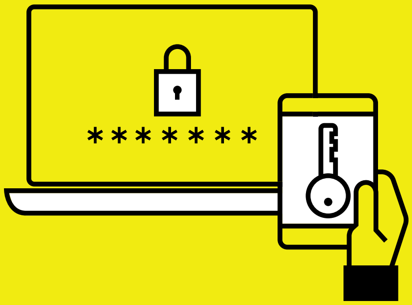


What is the strongest type of password?

The strongest passwords are passphrases: random thoughts that form a sentence. Passphrases should be at least 15 characters in length.

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

No, do not repeat passwords whenever possible.



What is Multi-Factor Authentication (MFA)?

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

– 2 –

Updates

What are updates?

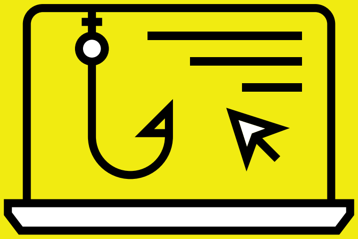
Put simply, “updates” are new versions of the software and applications on your phone and computer. These updates fix problems and improve security. Installing updates is one of the easiest and most critical cyber readiness measures you can take.

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?

Just over one in four employees (26%) said they had fallen for a phishing scam at work in the last 12 months – Tessian Research (2022)

Most phishing attacks are sent during the afternoon slump, between 2pm and 6pm, when people are more likely to be tired or distracted. – Tessian Research (2022)

— 4 —

Secure Storage & Sharing

What’s so bad about USB drives?

The use of USB removable media increased by 30% last year, and 79% of cyber threats originating from removable media could critically impact operations.

How can you limit USB attacks?

Don’t use
USB drives unless approved by your Cyber Leader

Never use
or accept a USB from any external person or company

If used,
USBs should be routinely checked for malware

CYBER READINESS
INSTITUTE

Learn more at

BeCyberReady.com