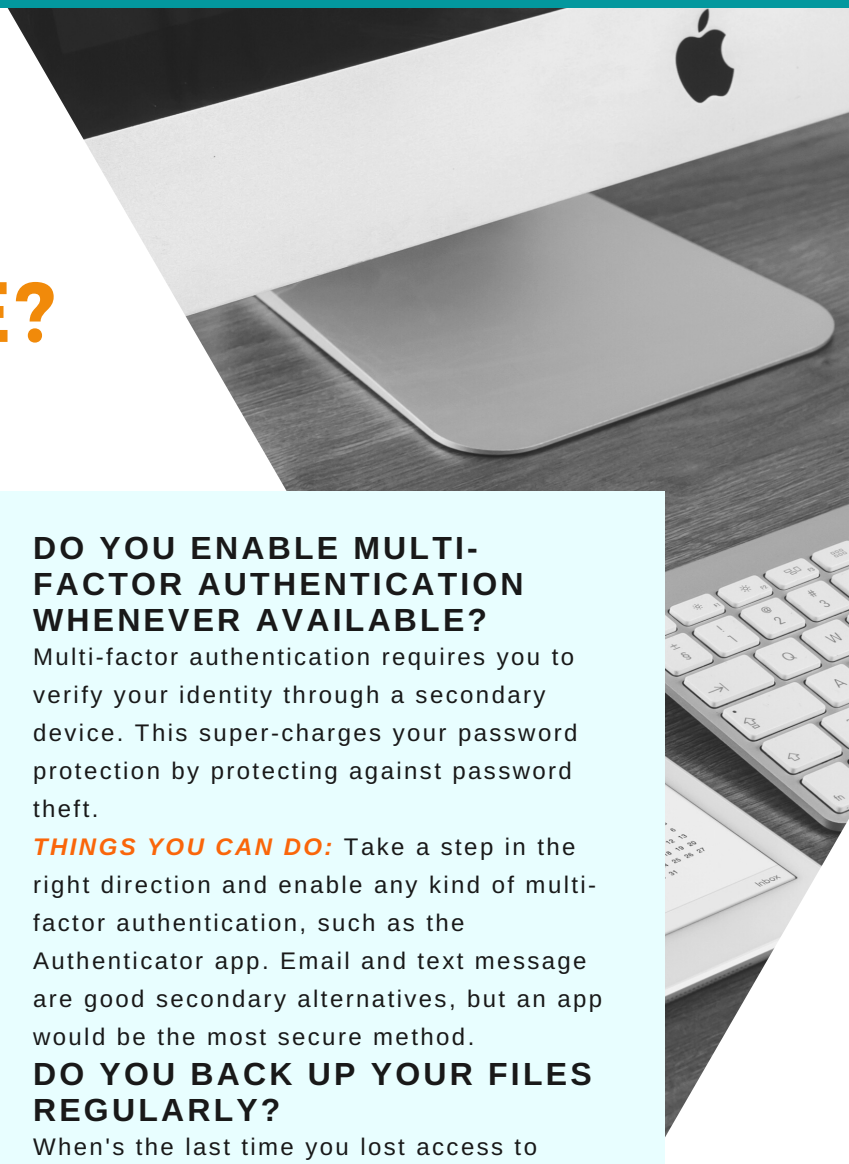
HOW SECURE IS YOUR OFFICE?

Here are four low-effort ways you can make a big impact on your cybersecurity.



DO YOU TAKE ACTION TO SECURE COMPUTERS?

Do you know how many devices your organization uses? Can you uniquely identify each one? Does each device have proper security settings enabled to protect it from malware and other threats? Are all devices updated with the latest software and security settings enabled?

THINGS YOU CAN DO: Enable screen lock under screen saver settings to prevent unauthorized users from accessing your confidential data when you leave your workstation unattended. Encrypt physical hard drives. Keep track of all office computer devices, apply updates when prompted, and document each assigned user.

DO YOU USE UNIQUE PASSWORDS FOR EACH ONLINE SERVICE?

Using unique passwords is a must. If you use the same password for multiple accounts and one account gets hacked, all accounts become vulnerable. Consider single sign-on and password manager software instead of writing your password on a post-it and leaving it by your desk where anyone can see it.

THINGS YOU CAN DO: Use a password manager such as LastPass to securely keep track of all your unique passwords. Avoid reusing passwords.

DO YOU ENABLE MULTI-FACTOR AUTHENTICATION WHENEVER AVAILABLE?

Multi-factor authentication requires you to verify your identity through a secondary device. This super-charges your password protection by protecting against password theft.

THINGS YOU CAN DO: Take a step in the right direction and enable any kind of multi-factor authentication, such as the Authenticator app. Email and text message are good secondary alternatives, but an app would be the most secure method.

DO YOU BACK UP YOUR FILES REGULARLY?

When's the last time you lost access to important files or confidential documents? Saving files to your computer is not enough to guarantee their safety. Accidental data loss can happen due to hardware failure, accidental damage, or human error. Malicious data loss can happen by getting infected with ransomware, which makes your files unrecoverable unless you pay a ransom to restore them.

THINGS YOU CAN DO: Use a cloud storage service such as OneDrive or Box (with multi-factor authentication enabled) instead of a physical backup device, which can still fail. With any backup method, test the backup at least once per year.