

# 10 Steps for Being a CYBERSAFE Superhero

Cybercrime has cost the world nearly a trillion dollars in damages, and it has ruined countless lives and businesses. Fortunately, employees like you have the power to fight back against cybercrime by staying CYBERSAFE with your online and data habits.

This checklist for being C-Y-B-E-R-S-A-F-E will help you become a cybercrime-fighting superhero every day, whether you're working from home or the office.

## Constant Updates

Most cyberattacks happen to out-of-date software, so please download updates immediately when they pop up on your computer, tablet, and phone.

## Yucky Links

"Phishing" is when hackers try to steal your login credentials by sending you to a fake website that asks you to log in. Spot fake websites by looking for "yucky links" with typos or weird letters.

## Backups

Make sure to back up your files regularly as part of your routine. You could try making sure a backup happens before you break for lunch or at the end of your workday.

## Engaged Attention

Cybercriminals want to catch you off your guard. Make sure that you're never "going through the motions" when you're on the internet or working with sensitive data. Pay close attention.

## Router Updates

Not sure when your router / internet modem was last updated? Check with your Internet Service Provider (CenturyLink, Xfinity, Cox, etc.) to figure out how to update your router or call our IT Help Desk for assistance.

## Strong Passwords

Combine at least 8 uppercase and lowercase letters with numbers and symbols to create strong passwords, and please change your passwords often. Use a secure password manager to store those complex, impossible-to-remember passwords.

## Authentication

Multifactor authentication (MFA) helps stop the thieves who purchased your passwords from shady online sources. Most authentication methods text or email you a code to confirm your identity, but some methods use a special authentication app on your phone.

## Physically Secure Hardware

Keep unwelcome eyes off your files by password protecting all your devices and putting your computer out of sight when you're not using it. You should be the only person using your work computer. And, uh, just go with us on the "F" here.

## Endpoint Protection

Endpoint (device) protection solutions, including antivirus, EDR, and MDR, help you access company data more securely with less hassle. Use Intune to securely "enroll" your personal and work devices to access company data, so you can complete your work tasks with fewer pesky login requests.