

# CYBERSECURITY

## CYBERSECURITY TIPS

By taking basic cybersecurity precautions, you can prevent most cyberattacks. Here are some very basic things to do and not do:

- 1. Create different passwords for each account:**

While it may seem like a lot of trouble remembering all your passwords, multiple accounts should never have the same password. If you use the same password over and over again, a cybercriminal has a much easier time accessing all your accounts. They only have to figure it out once.
- 2. Create long complicated passwords made up of letters, numbers, and other characters:**

Avoid using your pet's name, your birthday, anniversary, phone number, or something else a hacker could easily figure out.
- 3. Never enter your password if you are connected to an unsecured public Wi-Fi network:**

Cybercriminals are constantly trolling for passwords entered on public Wi-Fi networks. system via an email attachment.
- 4. Continually back up the data on your hard drive:**

Also, make sure that it can easily be restored. The best backups mirror what's stored on your server. This way nothing gets lost.
- 5. Never click on a link or open an attachment on an email from an unfamiliar sender:**

You should even be careful when you know the sender, because their email could in fact be compromised.
- 6. When shopping online, make sure you verify the URL of the website before buying:**

Also, check to see if the website is secure. You can do this by clicking on the padlock icon located in the toolbar.

## 7. Never tell anyone what your passwords are, even your coworkers:

If an emergency occurs and a coworker must access your computer in your absence, immediately change the password upon your return.

## 8. Never keep your passwords where they might be discovered:

If you can't remember them, you can safely store them with 1Password or LastPass, both of which are secure password managers.

## 9. The operating systems and software programs on your computer and mobile devices must be kept up to date at all times:

We all agree that it can be a pain to shut down programs when you're notified of an update. But because updates often contain vital security patches, it's important that these be taken care of immediately.

## 10. Make sure your computer is locked each time you leave:

Even though your IT team can set it up so your computer locks after a certain period of time being idle, it helps if you make a habit of locking it yourself before stepping away.



**Cyberattacks are real and damaging to your company.**

**One cyberattack can put a company out of business. Small to midsize businesses (less than \$50 million in revenue) are targeted over 50% of the time.**

**Cybercriminals are aware that SMBs often lack the robust data security measures in place at larger corporations, making them easy targets.**