

Cyber Hygiene: Data Security

Data privacy is a huge component of customer trust for your company. We should work with due diligence to protect that trust and their data.



Don't use unsecure data sharing apps

Not all data sharing apps are equal in security. If you have to communicate private data, make sure the app you are using has:

1. End-to-End encryption
2. Secure and encrypted storage
3. Password protection

Always encrypt data in motion

Taking your work computer home to do some extra work? Be sure to encrypt private data on the device before you leave. If a device is stolen, your login password won't be enough to protect the data. Breaches from stolen devices are more common than you think.



Strengthen your human firewall

In a world of high technology, we forget that low tech breaches still happen, accounting for 60% of data loss. Steps to prevent this are:

1. Use a screen shield to prevent inadvertent viewing of your screen
2. Insure all devices utilize encryption, especially mobile devices that may be lost or stolen
3. Do not leave devices unattended, even in a locked car

Don't use public wifi

Open networks are just that - open. Meaning if you share a network with a decent hacker, they can use that connection to access your computer. If you have to use public wifi when working on private data, be sure to connect to a Virtual Private Network (VPN) in order to protect yourself.



CyberCompass[®]
S E C U R I T Y

CyberCompass navigates businesses to cyber resilience across their business ecosystem of their people, processes, technology and vendors. We are a one-stop solution for a cybersecurity, compliance and privacy program.

©2021 Cyber Compass, LLC—All Rights Reserved Worldwide