CYBERSECURITY FOR
SMALL BUSINESS

CYBERSECURITY BASICS

Cyber criminals target companies of all sizes.

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT
YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR

SMALL BUSINESS

PROTECT YOUR WIRELESS NETWORK

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take. You can find it at FTC.gov/DataBreach.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security