CYBERSECURITY FOR
SMALL BUSINESS

PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

Store securely

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

Limit physical access

When records or devices contain sensitive data, allow access only to those who need it.

Send reminders

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

Keep stock

Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.

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

HOW TO PROTECT DATA ON YOUR DEVICES

A burglary, lost laptop, stolen mobile phone, or misplaced flash drive — all can happen due to lapses in physical security. But they're less likely to result in a data breach if information on those devices is protected. Here are a few ways to do that:

Require complex passwords

Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.

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.

Limit login attempts

Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.

Encrypt

Encrypt portable media, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside of the company, like to an accountant or a shipping service.

TRAIN YOUR EMPLOYEES

Include physical security in your regular employee trainings and communications. Remind employees to:

Shred documents

Always shred documents with sensitive information before throwing them away.

Erase data correctly

Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don't rely on "delete" alone. That does not actually remove the file from the computer.

Promote security practices in all locations

Maintain security practices even if working remotely from home or on business travel.

Know the response plan

All staff should know what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. Use *Data Breach Response: A Guide for Business* for help creating a response plan. 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