FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Cybersecurity for small business: Physical security

Share This Page

Andrew Smith, Director, FTC Bureau of Consumer Protection
Nov 9, 2018

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security | Small Business

An employee catches up on some work while visiting the local coffee shop. She grabs her Double Mocha to go, but accidentally leaves behind a flash drive with hundreds of Social Security numbers on it. When she returns, the flash drive is gone. Then there's the staff member who needs to free up file room space. After he tosses a stack of old company bank records into the garbage, a dumpster diver spots the trash and walks away with a windfall.

At meetings with small business owners across the country, you told us you wanted straightforward guidance on how to step up cybersecurity at your company. To help meet that need, the FTC has introduced new resources on a dozen topics. This week's focus: A key component of cybersecurity is effective physical security, as the examples above illustrate. And it begins with a plan to safeguard your equipment and paperwork.

How to protect equipment and paper files

As our factsheet describes, the starting point for any business is an up-to-date inventory of computers, flash drives, point-of-sale devices, files, etc. If they contain sensitive information, they belong in a secure part of your facility or in a locked file or cabinet. Make it office policy to log out of your network and applications when not in use. Never leave sensitive data unattended and limit access to employees who need the data to do their jobs.

How to protect data on your devices

The second step is to protect the data on those devices. Require passwords that are long, complex, and unique. To access parts of your network where sensitive information is kept, use multi-factor authentication. In other words, in addition to logging on with a password, require something extra like a temporary code on a smartphone or a key inserted into a computer. To stymie hackers, block access after several unsuccessful login attempts. Use encryption on laptops, flash drives, etc., that store sensitive data. Also encrypt confidential information you send outside of your company.

Train your employees

Finally, the FTC's new resources make it easier to enlist your staff in your cybersecurity efforts. Talk about physical security at an upcoming staff meeting. There's no need to start from scratch when you can use the factsheet to guide the discussion. Train your staff to maintain effective physical security even if working remotely from home or on business travel. And every employee should know what to do if a device or confidential file goes missing.

Next week: Ransomware – What is it? How can you protect against it? And what if it strikes your small business?

ftc.gov