FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

# Data Security

Many companies keep sensitive personal information about customers or employees in their files or on their network. Having a sound security plan in place to collect only what you need, keep it safe, and dispose of it securely can help you meet your legal obligations to protect that sensitive data. The FTC has free resources for businesses of any size.

## FEATURED

### Stick with Security: A Business Blog Series

Nov 16, 2017

START WITH SECURITY

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

### Start with Security: A Guide for Business

Jun 29, 2015

## GUIDANCE

### App Developers: Start with Security

App developers: How does your app size up? Have your built security in from the start? The FTC has a dozen tips to help you develop kick-app security for your product.

### Buying or selling debts? Steps for keeping data secure

For debt buyers and sellers, keeping sensitive information secure should be business as usual. The FTC has seven tips for members of the industry to help reduce the risk of unauthorized disclosure.

### Careful Connections: Keeping the Internet of Things Secure

Advice for businesses about building and keeping security into products connected to the Internet of Things, including proper authentication and access control, secure data management, and the importance of communicating with users effectively.

## Complying with the FTC's Health Breach Notification Rule

Guidance for business on complying with the FTC's Health Breach Notification Rule. Who's covered by the Rule and what companies must do if they experience a breach of personal health records.

## Consumer Reports: What Information Furnishers Need to Know

If you report information about consumers to consumer reporting agencies (CRAs) — like a credit bureau, tenant screening company, or check verification service — you have legal obligations under the Fair Credit Reporting Act's Furnisher Rule.

## Cybersecurity for Small Business

Learn the basics for protecting your business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with the National Institute of Standards and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.

## Data Breach Response: A Guide for Business

This guide addresses the steps to take once a breach has occurred. For advice on implementing a plan to protect consumers' personal information, to prevent breaches and unauthorized access, check out the FTC's *Protecting Personal Information: A Guide for Business* and Start with Security: A Guide for Business.

## Digital Copier Data Security: A Guide for Businesses

Does your company keep sensitive data — Social Security numbers, credit reports, account numbers, health records, or business secrets? If so, then you've probably instituted safeguards to protect that information. Your information security plans also should cover the digital copiers your company uses. If the data on your copiers gets into the wrong hands, it could lead to fraud and identity theft.

## Disposing of Consumer Report Information? Rule Tells How

Once your business is finished with sensitive information derived from consumer reports, what happens to it then? Under the Disposal Rule, your company must take steps to dispose of it securely.

## Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

Tips for organizations under FTC jurisdiction to determine whether they need to design an identity theft prevention program.

## Financial Institutions and Customer Information: Complying with the Safeguards Rule

Under the Safeguards Rule, financial institutions must protect the consumer information they collect. Learn if your business is a “financial institution” under the Rule. If so, have you taken the necessary steps to comply?

## Health Breach Notification Rule

Under the FTC's Health Breach Notification Rule, companies that have had a security breach must: 1. Notify everyone whose information was breached; 2. In many cases, notify the media; and 3. Notify the FTC.

## Medical Identity Theft: FAQs for Health Care Providers and Health Plans

Explains how medical identity theft occurs, and how health care providers and insurers can minimize the risk and help their patients if they’re victimized.

## Mobile Health App Developers: FTC Best Practices

When developing a health app, sound privacy and security practices are key to consumer confidence. Here are some best practices to help you build privacy and security into your app. These practices also can help you comply with the FTC Act.

## Mobile Health Apps Interactive Tool

You’re developing a health app for mobile devices and you want to know which federal laws apply. Check out this interactive tool.

## Peer-to-Peer File Sharing: A Guide for Business

Most businesses collect and store sensitive information about their employees and customers. If you use Peer-to-Peer (P2P) file sharing software in your business, consider the security implications and minimize the risks associated with it.

## Protecting Personal Information: A Guide for Business

Practical tips for business on creating and implementing a plan for safeguarding personal information.

## Security Check: Reducing Risks to Your Computer Systems

It’s just common sense that any company or organization that collects personal information from customers or employees needs a security plan. Learn more about designing and implementing a plan tailor-made to your business.

### Slip Showing? Federal Law Requires All Businesses to Truncate Credit Card Information on Receipts

What’s on the credit and debit card receipts you give your customers? Under federal law, you must delete the card’s expiration date and shorten the account information to include no more than the last five digits of the card number.

### Small Business Computer Security Basics

If you’re running a small business with only a few employees, you’ve learned about a lot of things – accounting, marketing, HR, you name it. And you probably depend on technology, even if it’s only a computer and a phone. You can’t afford to get thrown off-track by a hacker or scammer.

## RESOURCES

Start with Security: A Guide for Business

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved...

Data Breach Response: A Guide for Business

You just learned that your business experienced a data breach. Whether hackers took personal information from your corporate server, an insider stole customer information, or information was inadvertently exposed on your company’s website, you are probably wondering what to do next. What steps...

Cybersecurity for Small Business

## RELATED

### Corporate boards: Don’t underestimate your role in data security oversight

Apr 28, 2021

### Identity Theft Awareness Week starts today

Feb 1, 2021

### FTC says flight service winged it by leaving data unprotected in the cloud

Dec 16, 2020

Will your research take centerstage at PrivacyCon 2021?

Dec 16, 2020

Better safeguard than sorry

Dec 15, 2020

## LEGAL RESOURCES ON DATA SECURITY

View All ›

CASES

PUBLIC EVENTS

REPORTS

PRESS RELEASES

CLOSING LETTERS

PUBLIC STATEMENTS

FEDERAL REGISTER NOTICES

ADVOCACY FILINGS

PUBLIC COMMENT INITIATIVES

## VIDEOS

More Videos ›

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
FEDERAL TRADE COMMISSION UNITED STATES OF AMERICA MCMXV

The NIST Cybersecurity Framework and the FTC

Implement Strong Password Policies

Secure Devices and Paper