

Safeguarding Health Information

NIST/OCR Conference

September 3, 2015



Cora Han
Division of Privacy and Identity Protection
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC



**START
WITH**

SECURITY

LESSONS LEARNED FROM FTC CASES

**START
WITH**

SECURITY

A GUIDE FOR BUSINESS

FEDERAL TRADE COMMISSION | [BUSINESS.FTC.GOV](https://business.ftc.gov)



1

Start with security.

1

Start with security.

- Don't collect personal information you don't need.
- Hold on to information only as long as you have a legitimate business need.
- Don't use personal information when it's not necessary.

2

Control access to data sensibly.



2

Control access to data sensibly.

- Restrict access to sensitive data.
- Limit administrative access.

3

Require secure passwords and authentication.

3

Require secure passwords and authentication.

- Insist on complex and unique passwords.
- Store passwords securely.
- Guard against brute force attacks.
- Protect against authentication bypass.

4

Store sensitive personal information securely and protect it during transmission.

4

Store sensitive personal information securely and protect it during transmission.

- Keep sensitive information secure throughout its lifecycle.
- Use industry-tested and accepted methods.
- Ensure proper configuration.

5

Segment your network and monitor who's trying to get in and out.

5

Segment your network and monitor who's trying to get in and out.

- Segment your network.
- Monitor activity on your network.

6

Secure remote access to your network.

6

Secure remote access to your network.

- Ensure endpoint security.
- Put sensible access limits in place.

7

Apply sound security practices when developing new products.

7

Control access to data sensibly.

- Train your engineers in secure coding.
- Follow platform guidelines for security.
- Verify that privacy and security features work.
- Test for common vulnerabilities.

8

Make sure your service providers implement reasonable security measures.

8

Make sure your service providers implement reasonable security measures.

- Put it in writing.
- Verify compliance.

9

Put procedures in place to keep your security current and address vulnerabilities that may arise.

9

Put procedures in place to keep your security current and address vulnerabilities that may arise.

- Update and patch third-party software.
- Heed credible security warnings and move quickly to fix them.

10

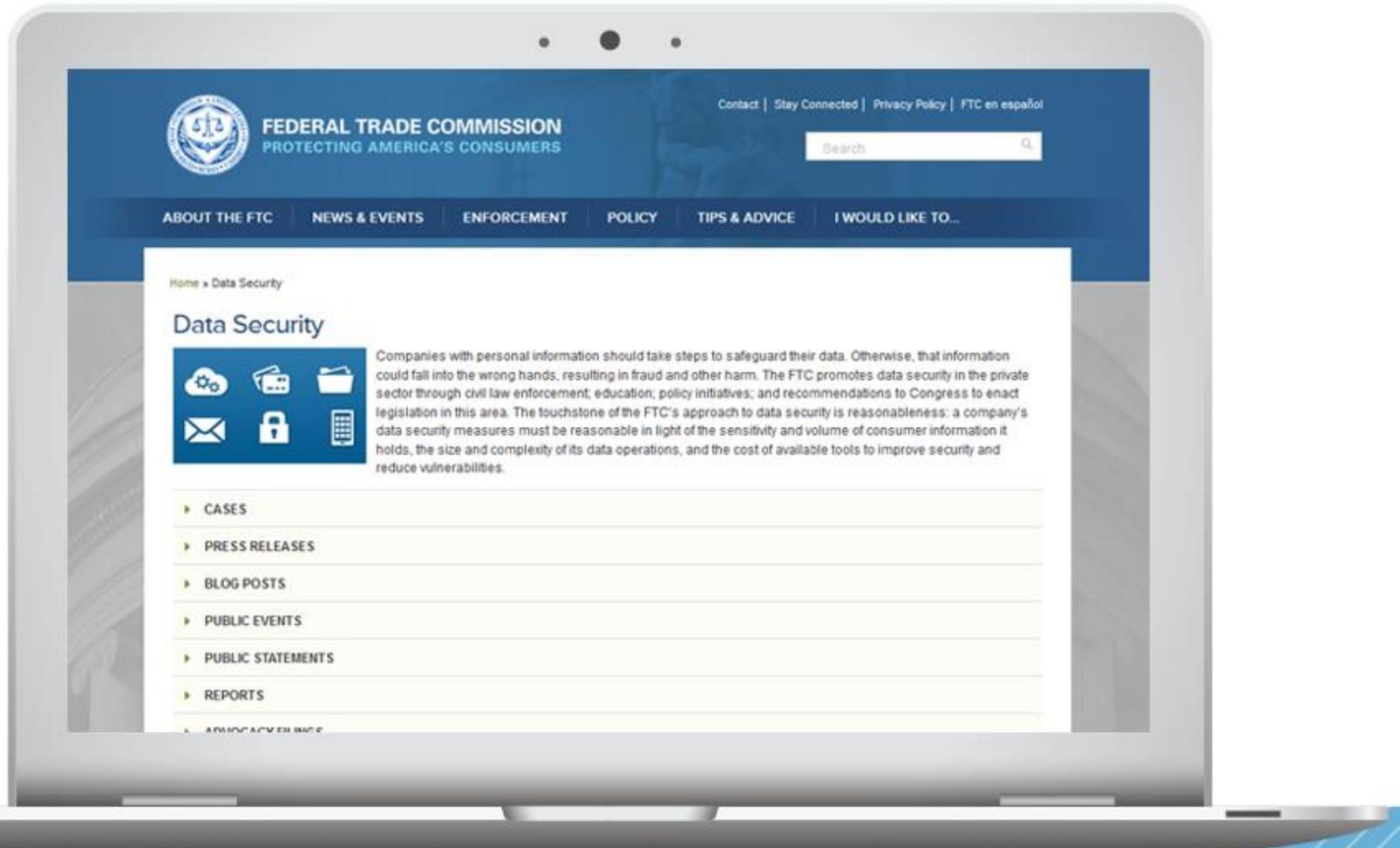
**Secure paper, physical media,
and devices.**

10

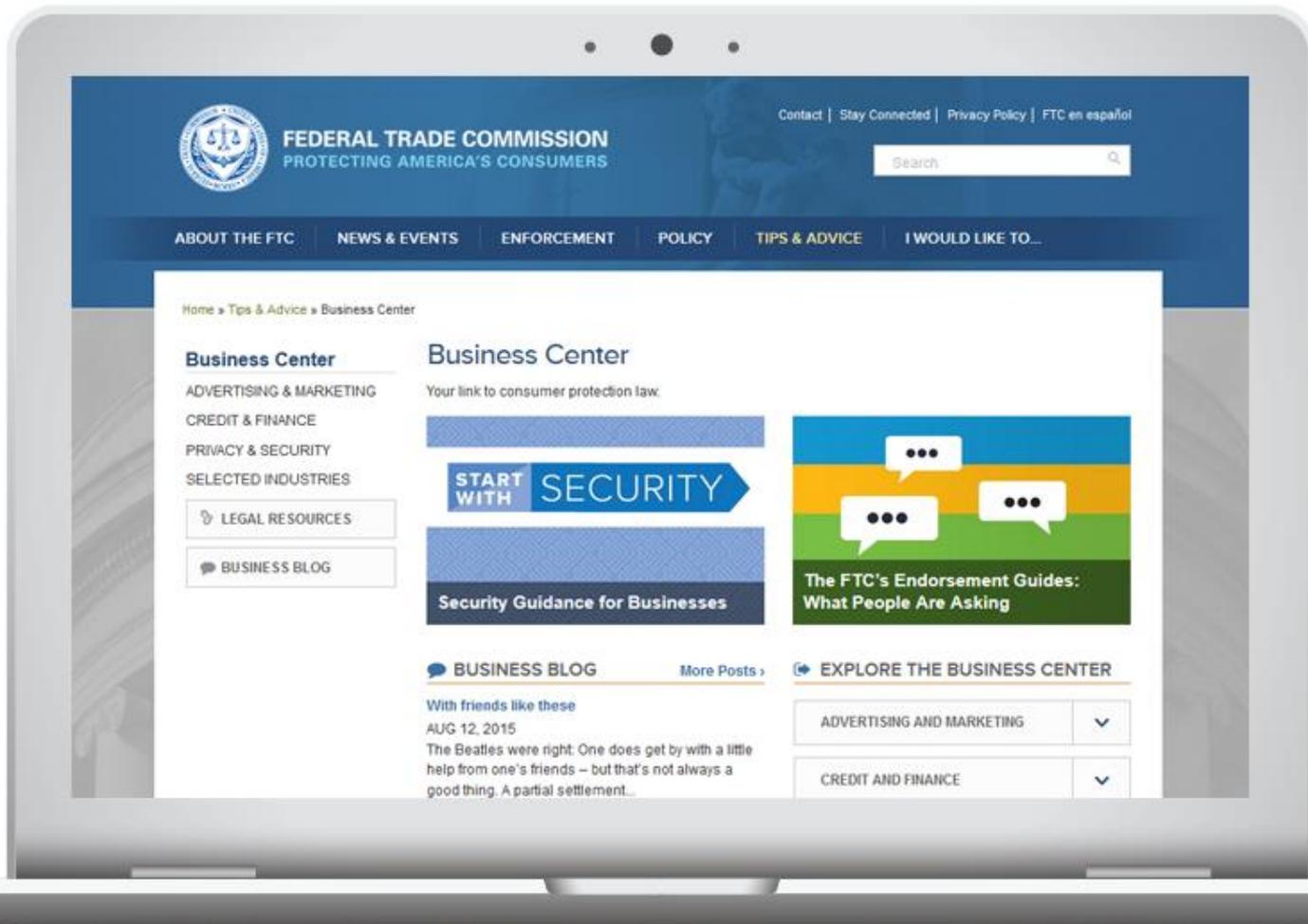
Secure paper, physical media, and devices.

- Securely store sensitive files.
- Protect devices that process personal information.
- Keep safety standards in place when data is en route.
- Dispose of sensitive data securely.

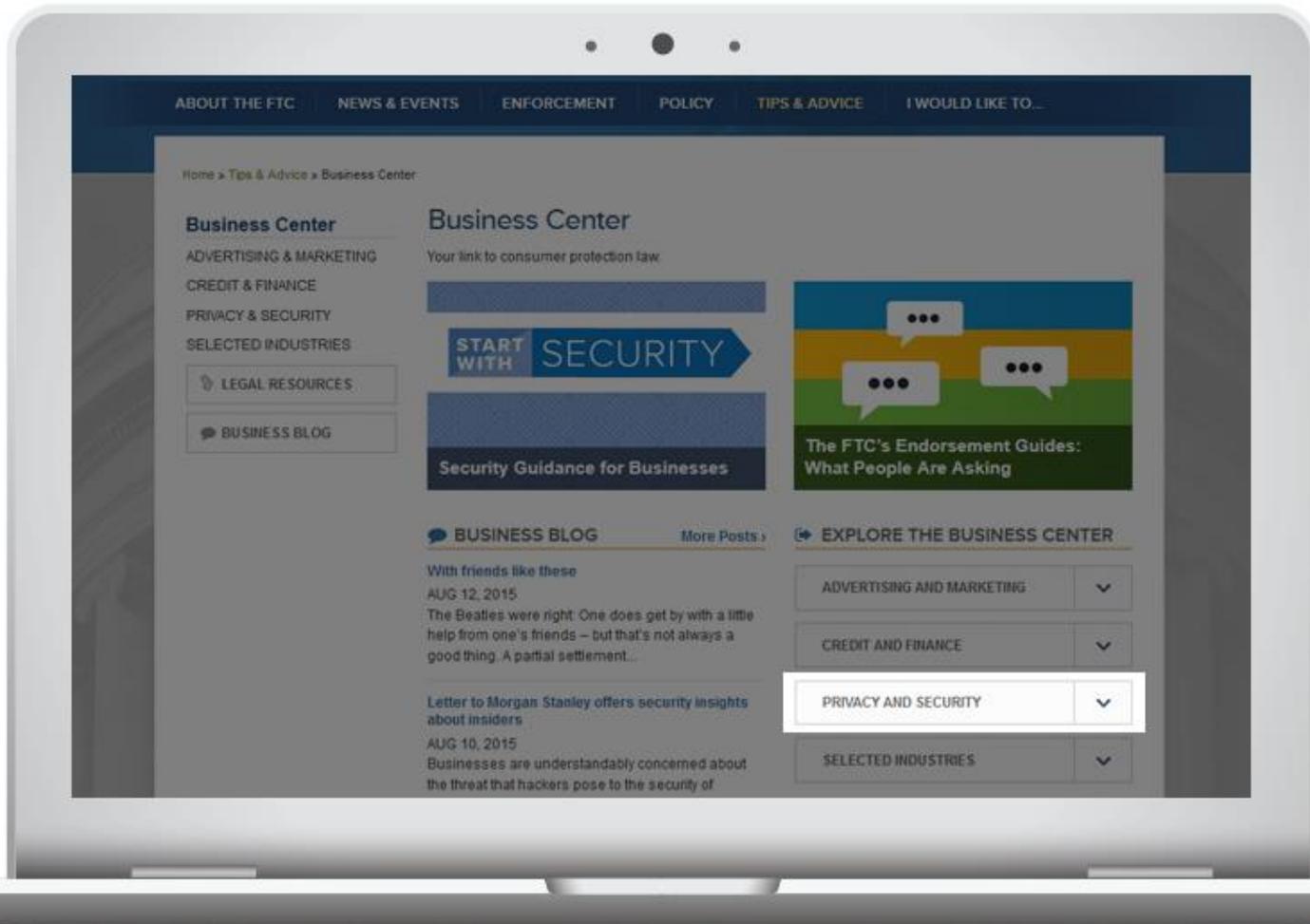
ftc.gov/datasecurity



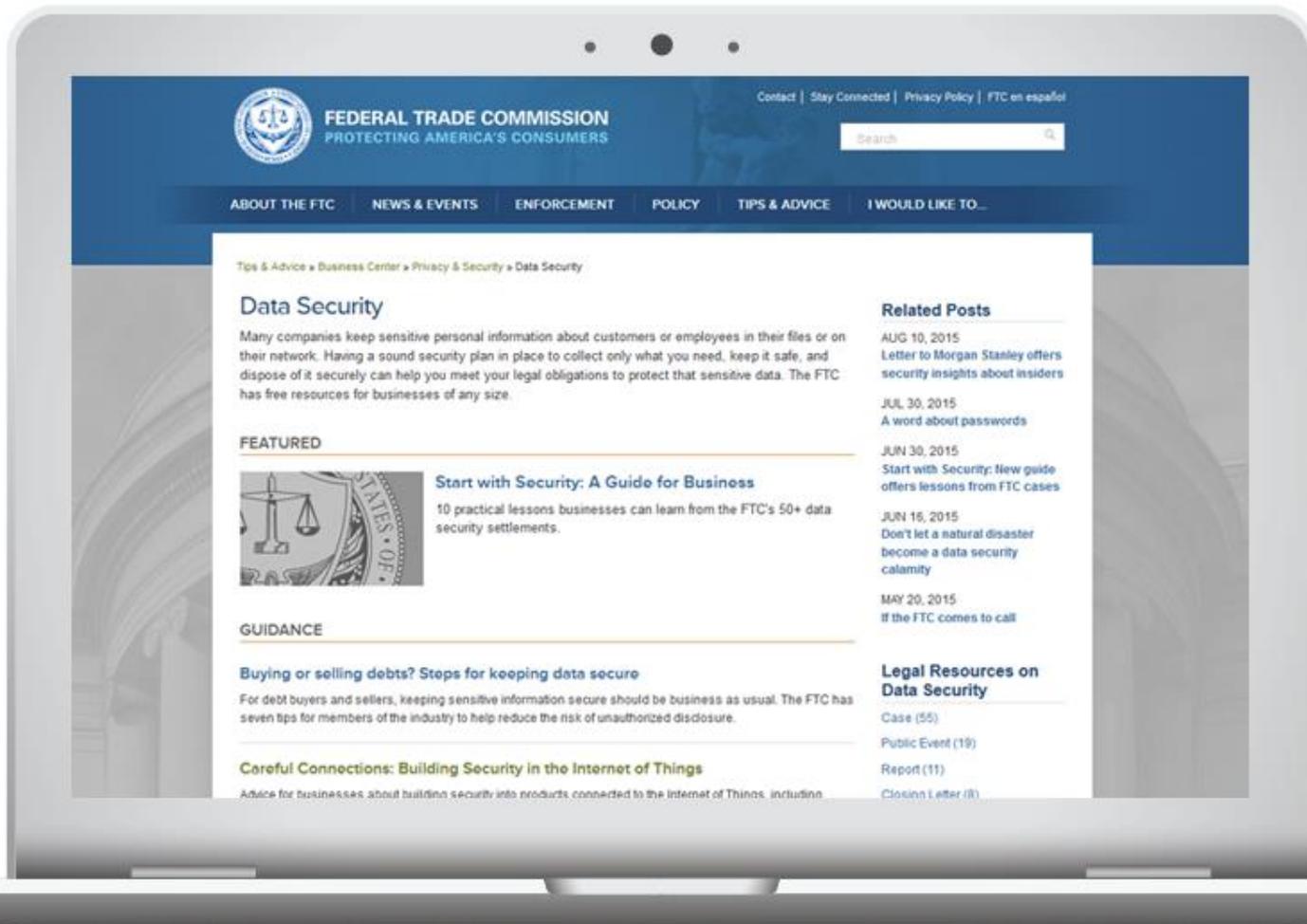
business.ftc.gov



business.ftc.gov



business.ftc.gov



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Tips & Advice » Business Center » Privacy & Security » Data Security

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



Start with Security: A Guide for Business

10 practical lessons businesses can learn from the FTC's 50+ data security settlements.

GUIDANCE

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: Building Security in the Internet of Things

Advice for businesses about building security into products connected to the Internet of Things, including

Related Posts

AUG 10, 2015
Letter to Morgan Stanley offers security insights about insiders

JUL 30, 2015
A word about passwords

JUN 30, 2015
Start with Security: New guide offers lessons from FTC cases

JUN 15, 2015
Don't let a natural disaster become a data security calamity

MAY 20, 2015
If the FTC comes to call

Legal Resources on Data Security

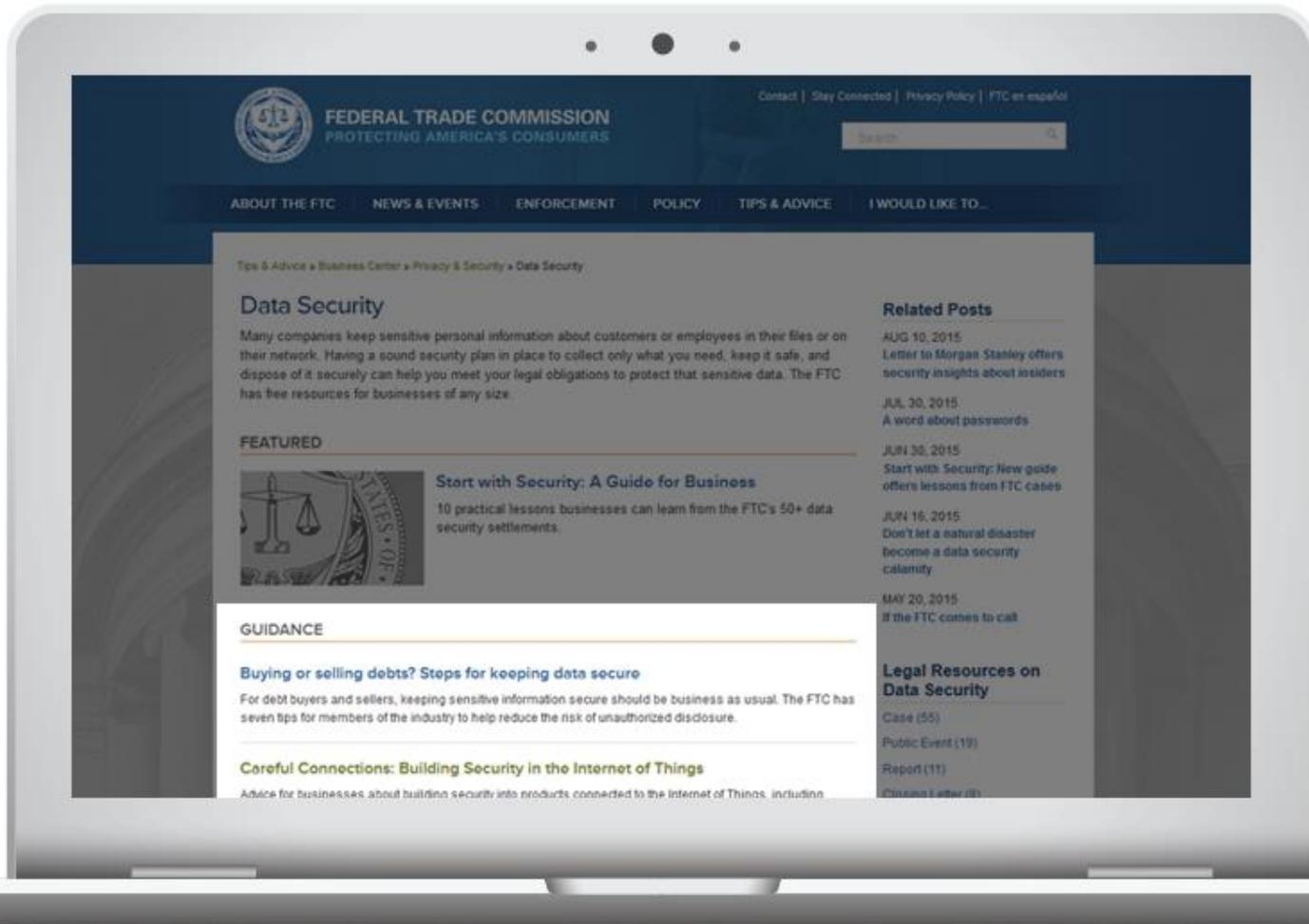
Case (55)

Public Event (19)

Report (11)

Closure Letter (8)

business.ftc.gov



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC in español

Search

ABOUT THE FTC NEWS & EVENTS ENFORCEMENT POLICY TIPS & ADVICE I WOULD LIKE TO...

Tips & Advice » Business Center » Privacy & Security » Data Security

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



Start with Security: A Guide for Business

10 practical lessons businesses can learn from the FTC's 50+ data security settlements.

GUIDANCE

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: Building Security in the Internet of Things

Advice for businesses about building security into products connected to the Internet of Things, including

Related Posts

AUG 10, 2015
Letter to Morgan Stanley offers security insights about insiders

JUL 30, 2015
A word about passwords

JUN 30, 2015
Start with Security: New guide offers lessons from FTC cases

JUN 16, 2015
Don't let a natural disaster become a data security calamity

MAY 20, 2015
If the FTC comes to call

Legal Resources on Data Security

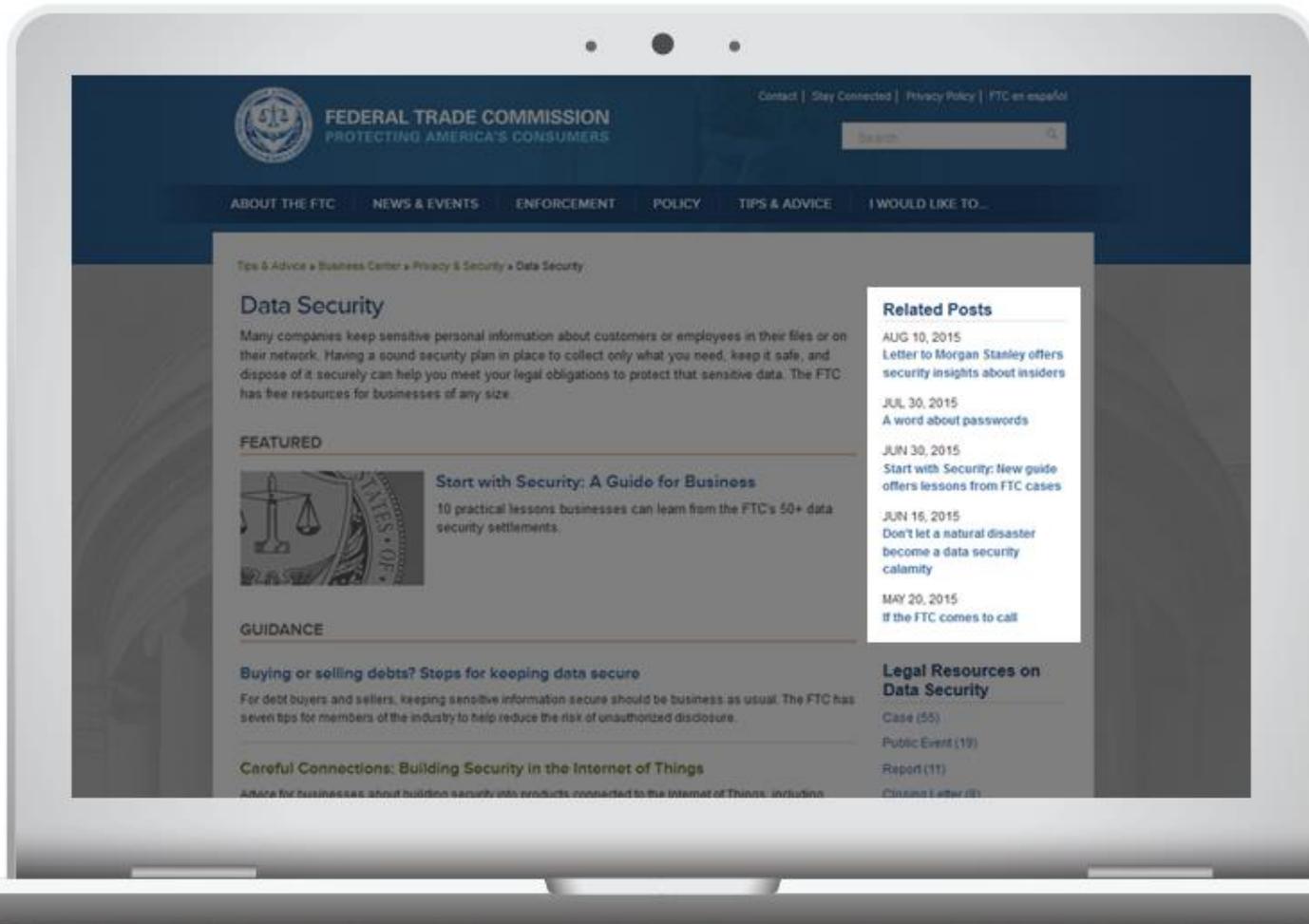
Case (55)

Public Event (19)

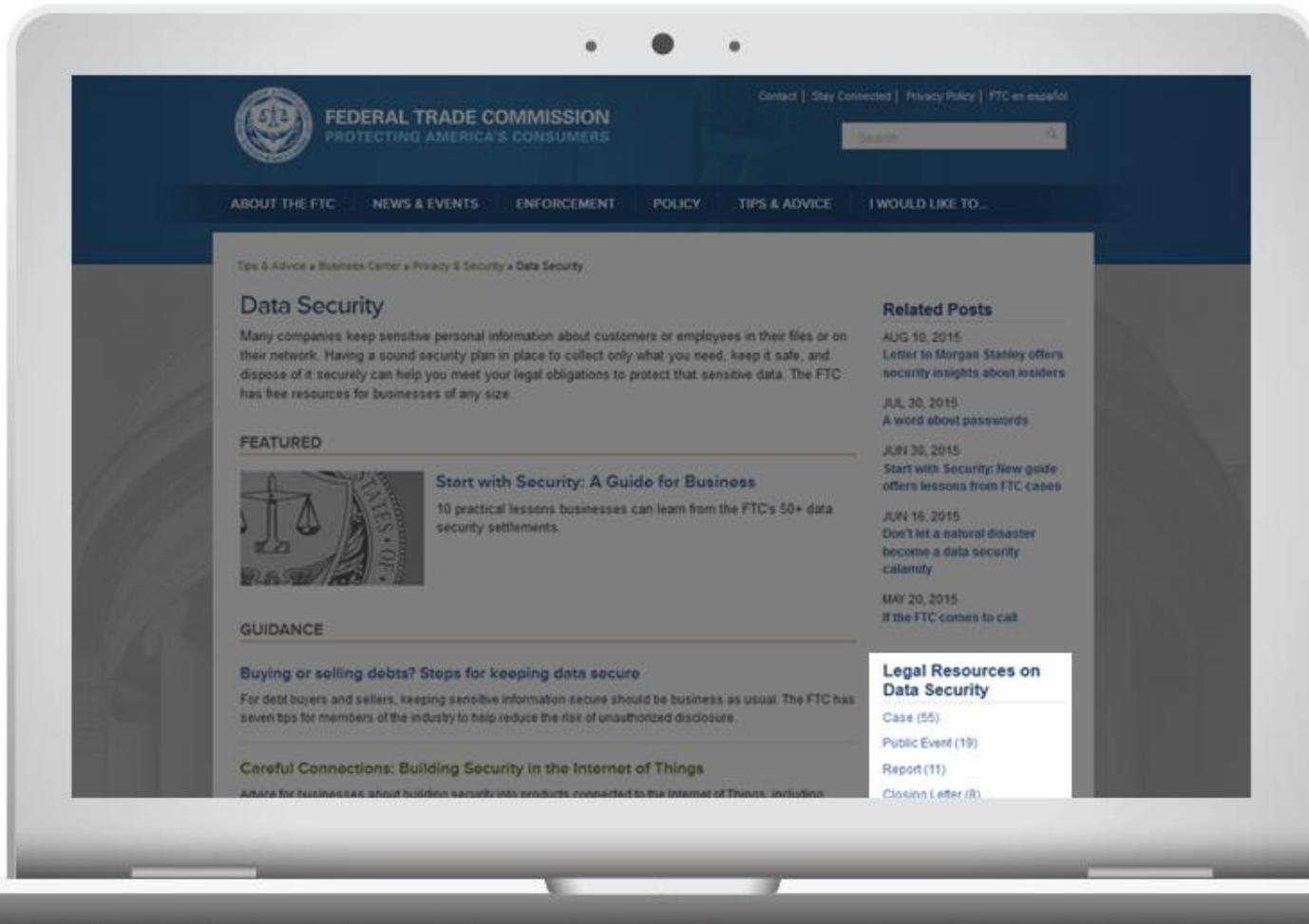
Report (11)

Business Letter (8)

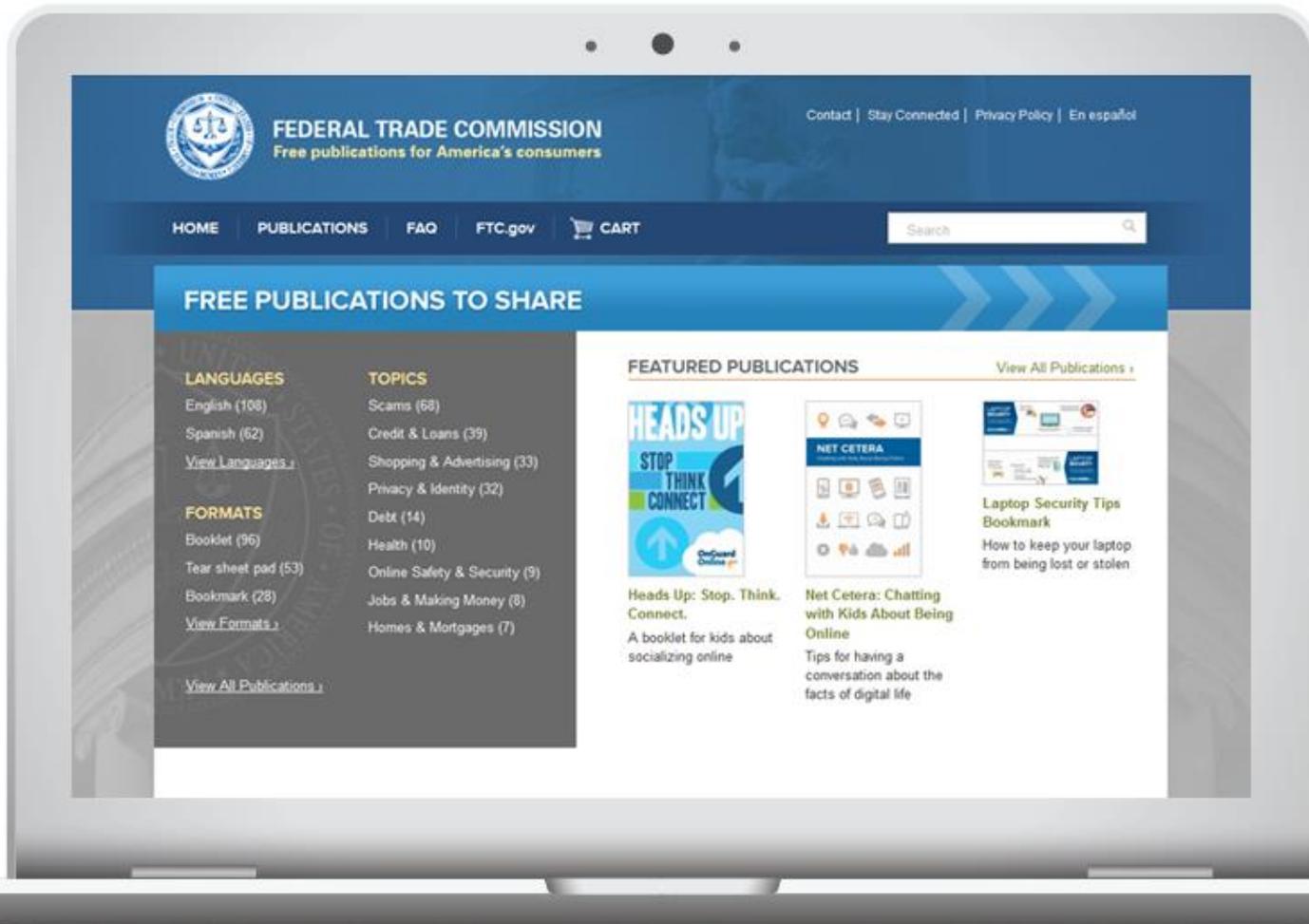
business.ftc.gov



business.ftc.gov



bulkorder.ftc.gov





chan@ftc.gov





T H A N K S !

