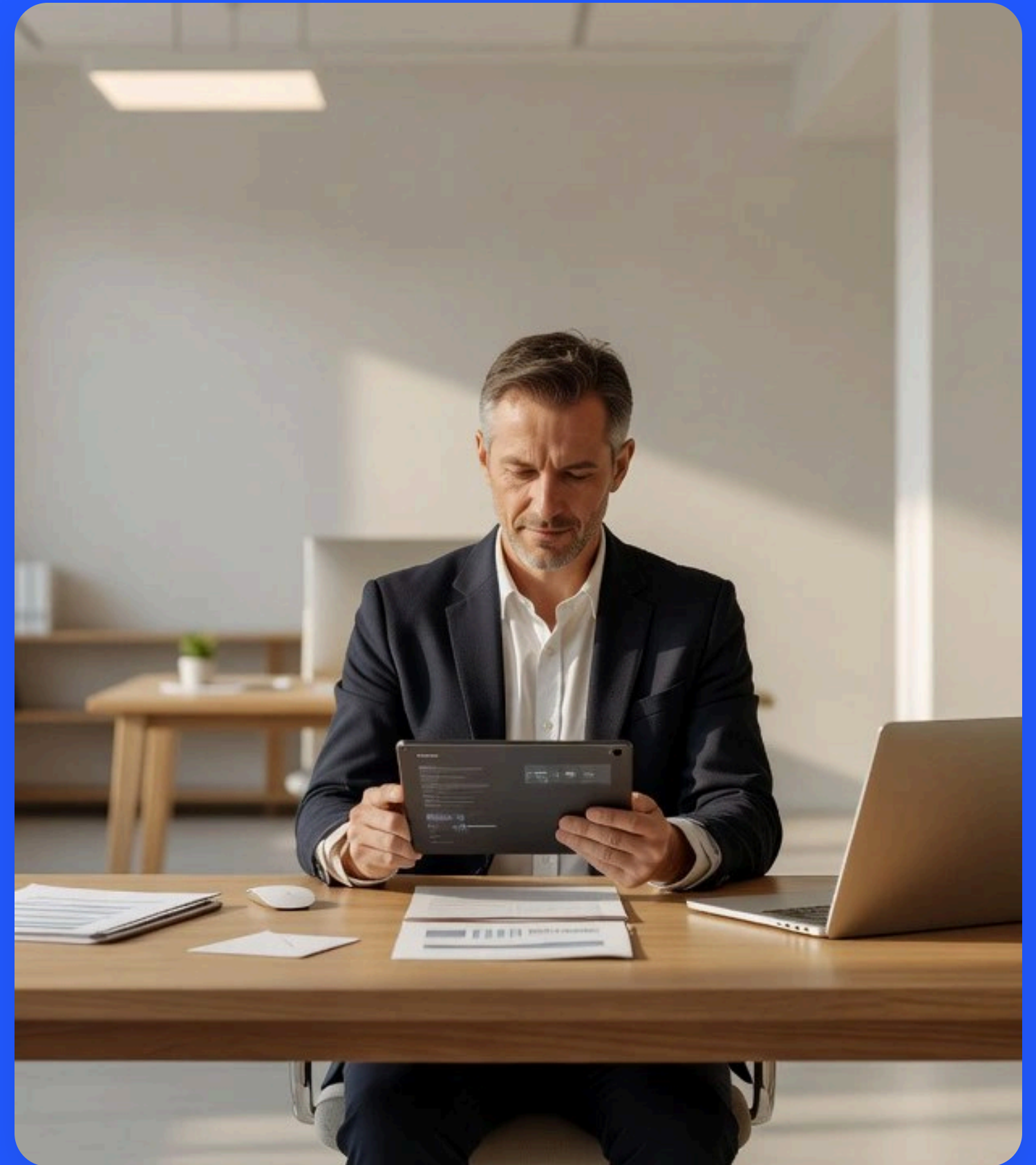

Customer Data Security

A practical buyer conversation grounded in FTC guidance.



Conversation

01 Your customer information.

02 The FTC security foundation.

03 Practical protection priorities.

04 A sensible first step.

Customer information is essential—and worth protecting.



Information supports business.

Names, account data, and payment information may be needed to serve customers and operate the business.

Protect what the business needs to keep.

FTC guidance gives a practical security foundation.

5

PLAN PRINCIPLES.

Take stock, scale down, lock, pitch,
plan ahead.

10

SECURITY LESSONS.

Fundamental practices for
reducing data security risks.

50+

FTC ACTIONS CITED.

Lessons distilled from announced
law enforcement actions.

A sound plan follows five connected principles.

1

Take stock.

Trace information, locations, flows, and access.

2

Scale down.

Keep only information needed for business.

3

Lock it.

Protect information through its full lifecycle.



Less data and less access reduce exposure.

- **Collect less:** Do not collect unneeded personal information.
- **Retain less:** Keep data only for legitimate business needs.
- **Use substitutes:** Use fictitious data for training and development.
- **Limit access:** Apply least privilege and need-to-know access.

Access controls protect information from unnecessary exposure.



Control entry points.

Strong passwords, secure credential storage, multi-factor authentication, and login limits help restrict access to authorized users.

Administrative access should match job responsibilities.

Protection must cover data at rest, in transit, and on the network.

Secure the data.

Encrypt sensitive information during storage and transmission.

Secure the network.

Segment systems and monitor inbound and outbound activity.

Remote access and service providers need clear guardrails.



Extend controls outward.

Secure remote endpoints, limit third-party access, document security expectations, and verify service-provider compliance.

Outside access deserves the same attention.

Security spans people, products, devices, and paper.



Secure development.

Train engineers and test common vulnerabilities.



Employee training.

Build a culture of security awareness.



Physical security.

Lock files, media, and sensitive devices.



Secure disposal.

Make information unreadable and devices wiped.

Security stays current through response and improvement.

1

Update.

Patch software and maintain current protections.

2

Receive reports.

Use an effective vulnerability reporting process.

3

Respond quickly.

Investigate incidents and close vulnerabilities promptly.



Start with security.

Begin by taking stock of customer information and access.