Passkeys for Business: Starter Guide (2026 Edition)

This guide helps small businesses start using passkeys without confusion or disruption.

Passkeys Adoption Checklist

1. Understand What Passkeys Replace

- ☐ Passkeys replace passwords, not just strengthen them
- ☐ No password is typed, stored, or shared during login
- ☐ Authentication happens using a trusted device (phone, laptop, or security key)

Why this matters:
Passkeys remove the most common attack target passwords themselves.

2. Identify Which Systems Support Passkeys

- ☐ Review core tools (Google, Microsoft, Apple, SaaS apps)
- ☐ Enable passkeys where already supported
- ☐ Track which apps still require passwords

Why this matters:
Adoption starts with what's already available. Many major platforms already support passkeys.

3. Require Strong Device Security First

- ☐ Devices use PIN, biometrics, or secure login
- ☐ Screen lock is enforced
- ☐ Lost or stolen devices can be secured remotely

Why this matters:
Passkeys rely on device trust. If the device is weak, the authentication is weak.

4. Enable Passkeys for High-Risk Accounts First

□ Email accounts
□ Admin or privileged accounts
□ Financial and payment systems
□ Cloud and business-critical apps

Why this matters:
Start where the risk is highest to get immediate security value.

5. Keep MFA as a Backup Layer

□ MFA remains enabled during transition
□ Backup authentication methods are documented
□ Recovery options are secure and tested

Why this matters:
Not all systems fully support passkeys yet. Redundancy prevents lockouts.

6. Train Employees on the New Login Experience

□ Explain how passkeys work in simple terms
□ Demonstrate login on phone and computer
□ Reinforce that no passwords should be typed

Why this matters:
Employees must understand the difference or they will fall back to insecure habits.

7. Eliminate Password Habits Gradually

□ Reduce password use where passkeys are active
□ Remove saved browser passwords
□ Stop sharing passwords between employees

Why this matters:
Mixing old and new methods creates confusion and risk.

8. Manage Access Through Identity, Not Shared Credentials

□ Each employee has their own login
□ No shared accounts are used
□ Access is controlled through roles

Why this matters:
Passkeys work best in environments with clear identity control.

9. Monitor Account and Device Activity

□ Review login activity regularly
□ Investigate unusual device access
□ Ensure only approved devices are used

Why this matters:
Passkeys reduce risk but monitoring still matters.

10. Plan for Device Loss or Replacement

□ Backup authentication method is available
□ Employees know how to regain access
□ Replacement device setup is documented

Why this matters:
The most common failure point is not hacking, it's losing access.

11. Integrate Passkeys into Onboarding and Offboarding

□ New employees are set up with passkeys on day one
□ Departing employees lose device-based access immediately
□ Old devices are removed from trusted device lists

Why this matters:
Passkeys must be managed as part of the employee lifecycle.

12. Continue Using a Password Manager

□ Password manager is still used for unsupported systems
□ Passkeys are stored and managed where supported
□ Transition is tracked over time

Why this matters:
Most businesses are in a hybrid state. Password managers still play a role during transition.

What Passkey Success Looks Like

Employees no longer type or remember passwords
Phishing attacks fail because credentials can't be stolen
Login is faster and easier for the team
Security improves without adding friction

Quick Rule of Thumb

If your employees are still typing passwords everywhere, you haven't started the transition.

SofTouchSystems.com

No-Surprise IT — Predictable. Proactive. Proven.