

No. 105

CYBERSECURITY

Passwordless and Passkeys

Replacing passwords with phishing-resistant sign-in

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 105

Passwordless and Passkeys

Replacing passwords with phishing-resistant sign-in

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Passwordless and Passkeys
Replacing passwords with phishing-resistant sign-in

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product and company names mentioned in this book are trademarks of their respective owners. FIDO and passkey-related marks belong to their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · WHY PASSWORDLESS

1 The trouble with passwords 5
2 What passwordless means 7
3 What a passkey is 8
4 How passkeys work 10
5 Why passkeys stop phishing 11
6 Adoption so far 13
7 From passwords to passkeys 15

PART II · PASSKEYS IN DEPTH

8 Synced and device-bound passkeys 17
9 Hardware security keys 19
10 The standards behind passkeys 20
11 Using passkeys across devices 22
12 Password managers and passkeys 23
13 Recovery 24
14 Limits of passkeys 25

PART III · FOR ORGANIZATIONS

15 A workforce strategy 27
16 Administrators first 29
17 Rolling out to staff 30
18 Shared devices and frontline workers 32
19 Legacy applications 33
20 The help desk 34
21 Policy and enforcement 35
22 Measuring progress 36
23 Regulation and guidance 37

FREE SAMPLE · ojayo.com

PART IV · FOR APPS AND PEOPLE

24 Adding passkeys to apps 39
25 User experience 40
26 Barriers and solutions 41
27 Common myths 42
28 A personal plan 43
29 What comes next 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Passwords have been the main way to sign in for over sixty years, and they have been failing for most of that time. People reuse them, type them into fake websites and forget them; criminals steal them by the billion. **Passkeys** offer a better way: sign-in credentials that cannot be phished, guessed or reused, unlocked with a fingerprint, face or PIN.

By 2026 passkeys had moved into the mainstream, with billions in use across major platforms and services. This book explains passwordless sign-in and passkeys for beginners: how they work, why they are safer, how to use them personally, and how organizations can roll them out to staff and customers.

What this book covers

- Why passwords fail and what "passwordless" means.
- How passkeys work, in plain language.
- Synced and device-bound passkeys, security keys and the standards behind them.
- Using passkeys across devices, and recovery when devices are lost.
- Workforce rollout, consumer apps, barriers and a practical plan.

Who this book is for

- **Everyone** who wants safer, easier sign-in.
- **IT and security teams** planning passwordless authentication.
- **Developers and product managers** adding passkeys to apps.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Why passwordless** (Chapters 1–7): password problems, what passwordless means, what a passkey is, how it works, why it resists phishing, adoption so far, and a short history.
- **Part II — Passkeys in depth** (Chapters 8–14): synced and device-bound passkeys, security keys, standards, using passkeys across devices, password managers, recovery, and limits.
- **Part III — For organizations** (Chapters 15–23): workforce strategy, admins first, rollout, shared devices, legacy apps, help desks, policy, measuring progress, and regulation.
- **Part IV — For apps and people** (Chapters 24–29): adding passkeys to apps, user experience, barriers, myths, a personal plan, and the future.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in a real organization.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Platform menus change often; follow each service's current instructions. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Why passwordless

These chapters explain why passwords fail, what passkeys are, how they work and why they stop phishing.

FREE SAMPLE · ojayo.com

CHAPTER 1

The trouble with passwords

Passwords are hard for people and easy for attackers.

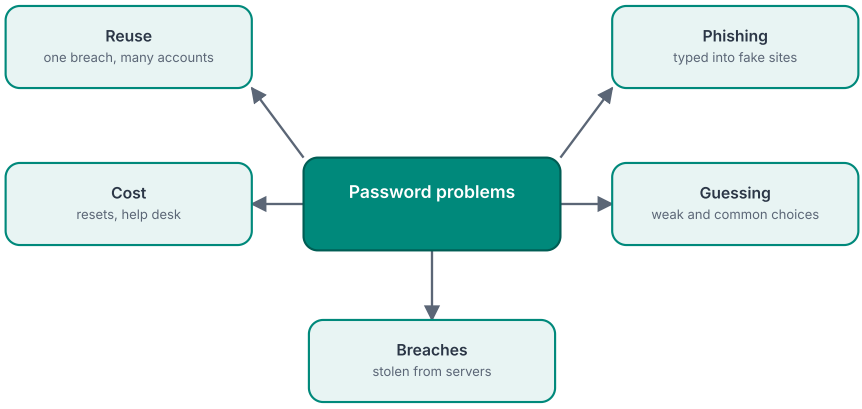


Figure 1.1 Why passwords fail

Human limits

Nobody can remember hundreds of long, unique passwords, so people reuse them or choose predictable ones.

Attacker advantages

- **Phishing** tricks people into typing passwords into fake sites.
- **Credential stuffing** tries leaked passwords on other sites automatically.
- **Infostealer malware** captures saved passwords from devices.
- **Server breaches** expose password databases.

FREE SAMPLE · ojayo.com

Hidden costs

Password resets are one of the most common help-desk requests, and forgotten passwords make people abandon purchases and sign-ups.

KEY IDEA

The problem is not careless users. It is that a shared secret typed by a human is easy to steal.

FREE SAMPLE · ojayo.com

CHAPTER 2

What passwordless means

Passwordless means signing in without a password to type.

A definition

Passwordless authentication means signing in without entering a password, using something you have, such as your phone or a security key, unlocked by something you are or know locally, such as a fingerprint or device PIN.

Not all passwordless is equal

Magic links by email and one-time codes by text remove the password but can still be intercepted or phished. The strongest passwordless methods are **phishing-resistant**: passkeys, security keys and smart cards.

Passwordless and MFA

A passkey is itself multi-factor: possession of the device plus a biometric or PIN.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys (you are reading th…
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Passwordless and Passkeys

Enjoyed it? The full book has 52 pages and 29 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.