MNEMONICA

WHITEPAPER

Safer, and simpler.

Why passkeys mark the coming of age of the internet of services, and why it matters so much to the film industry.

93%	2.8×	0
of passkey sign-ins succeed, against 78% with passwords	faster than a sign-in without a passkey	secrets on the server for an attacker to steal

A **Mnemonica** position paper
on authentication, identity and content security
Figures: FIDO Alliance, Passkey Index 2026 and passkey documentation

November 2026
mnemonica.com

SUMMARY

For the first time, the safest way in is also the easiest one.

Passwords protect the most valuable files in our industry with a secret that can be guessed, reused, stolen or handed over to a fake page. Passkeys remove that secret.

Mnemonica houses unreleased films and series, dailies, cuts in progress and masters, which are the most important business assets of the companies that make them. We are well aware that they are among the most coveted content on the network, and that stolen credentials are still one of the most common ways in. Every account in a film's supply chain, from the studio to the last freelancer, is a door.

Passkeys, the open standard of the FIDO Alliance supported by Apple, Google and Microsoft, replace the password with a cryptographic key that never leaves the user's device and only works on the real website. Nothing to phish, nothing to steal from a server, nothing to remember.

On 17 October 2026 Mnemonica removed passwords and MFA codes and moved to passkeys, the latest step of a path that began ten years ago and has always put our clients' work ahead of convenience, even when it cost us. This paper explains why the whole industry should take the same step.

IN BRIEF

1. We still treat the digital infrastructure the way early motorists treated cars: without seatbelts.
2. Attackers rarely break in. They log in, with stolen credentials, often through a third party.
3. A password is a shared secret. A passkey is a key pair: the private half never leaves your device.
4. Passkeys are phishing-resistant by design, and they succeed more often and faster than passwords.
5. Real identity is the answer to bots and fakes, and the condition for knowing who did what.
6. Mnemonica has said no to links to content for ten years. Passkeys make the safe way the easy way.



01

THE NAIVE AGE

Driving without seatbelts

Many of us use a global digital infrastructure every day with the habits of its first years: passwords on sticky notes, files sent by link, one login shared by family and friends. Part of the problem is scale. The network is too vast and too invisible for us to feel its risks, so we give them little weight.

Cars went through the same phase. The three-point seatbelt only arrived in 1959; crash tests, airbags and ABS came later, and today nobody would drive without them. Hospital hygiene went through it too. When Ignaz Semmelweis asked the doctors of Vienna to wash their hands in 1847, many took offence. Today a surgeon who skipped it would not be allowed to operate.

Security online is at that turning point. The question is no longer whether precautions are worth the effort, but why we still go without them.

02

WHAT IS AT STAKE

The most coveted files on the network

For a producer, a film's files are the capital invested in it: years of work, financing and rights. In production they are secret, restricted material, the most appealing to pirates. In distribution and preservation they are the asset on which every future sale depends. At every stage, they are a potential hostage for ransomware gangs. In April 2026 *The Legend of Aang: The Last Airbender* leaked months before release, after a suspected break-in at a third-party screening company.[2]

Attackers rarely break in: they log in. In Verizon's 2025 Data Breach Investigations Report, compromised credentials were the initial access vector in **22% of breaches**. Third-party involvement in breaches doubled, to **30%**.[1] A production is a chain of vendors, freelancers and festivals: every weak account, every phishable login, is everyone's problem.

03

THE WEAK LINK

The trouble with secrets

A password is a shared secret: you know it, and the service stores a version of it. It can be guessed, reused, stolen from a breached database, captured by malware, or typed into a convincing fake page.

Codes sent by SMS or email made attacks harder, not impossible: a fake page, or a fake colleague on the phone, can ask for the code too, and most second factors in use today are still phishable.[4] Each layer also added friction, and friction breeds workarounds.

04

HOW PASSKEYS WORK

A key that fits one lock

A passkey replaces the secret with a pair of cryptographic keys: the **private key** stays on the user's device or password manager, the service keeps only the **public key**. To sign in, the device signs a challenge from the service once the user unlocks it with a fingerprint, face or PIN. Three things follow.[3]

> **Nothing to phish, nothing to hand over.** A passkey only answers the real domain it was created for, and you never see it, so you cannot be tricked into giving it away. Credential phishing becomes impossible: no one can steal a secret you don't have.
>
> **Nothing to steal from the server.** The service holds only a public key, which is useless to an attacker.
>
> **Your biometrics stay with you.** Fingerprint and face never leave the device.

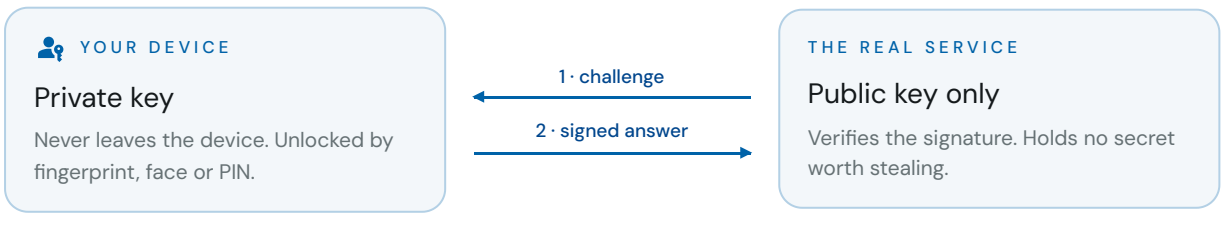

Figure 1. A challenge and a signature, bound to the real domain: a look-alike site gets no answer.[3]

05

SAFER, AND SIMPLER

The end of a false trade-off

For thirty years security and convenience pulled in opposite directions: every protection was one more step. Passkeys break that rule. Signing in takes the same gesture as unlocking a phone, and there is nothing to forget or reset.

The data now confirms it. In the FIDO Alliance Passkey Index 2026, passkey sign-ins succeeded **93%** of the time against **78%** for passwords and traditional MFA, and were about **2.8 times faster**, saving around 27 seconds each. Passkeys already carried **36%** of sign-ins at the participating services.[5] Microsoft made passkeys the default for Entra ID users relying on SMS or voice from 1 September 2026.[6]

> *Security and simplicity used to pull in opposite directions. They no longer do.*

THREAT	PASSWORD	PASSWORD + SMS OR EMAIL CODE	PASSKEY
A fake sign-in page	Password captured	Password and code captured	Nothing to capture
The service's database is breached	Scrambled passwords exposed, often crackable	Passwords exposed, but the code still stands in the way	Public keys only, useless
The same credential on other sites	Common, and enough to get in	Common, but not enough without the code	Impossible: one key per site
Malware on the laptop	Typed secret recorded	Typed secret recorded	No typed secret to record
Forgotten, reset, help desk	Frequent	Frequent, plus lost or changed phones	Nothing to remember

Figure 2. What each method exposes to the most common attacks. Services store passwords in scrambled form (hashes), which attackers can often reverse by trial and error. Passkeys are phishing-resistant whether synced across devices or bound to one.[3]

06

IDENTITY

Knowing who is really there

Bots made up **53%** of internet traffic in 2025, and bad bots alone **40%**.[7] Generative AI makes fakes cheap: fake accounts, fake voices, fake people. Proving that a real, specific person is on the other side is no longer bureaucracy. It is the basis of trust online.

A passkey is personal: it lives on one person's device and is unlocked by that person's fingerprint, face or PIN. That is why it matters so much in Mnemonica. Every account on the platform is personal, and every operation is tied to a name: who uploaded, who approved, who shared, who downloaded. Traceability is only as strong as the identity beneath it. And identity is only as strong as the device that holds it: a passkey can only be saved on a device protected by a lock, so securing the device is no longer optional.

07

OUR POSITION

Ten years of saying no

Security at Mnemonica was not added later: it is why the platform exists. It was born in 2015 to give filmmakers a solid alternative to consumer platforms, where previews could easily be found and attacked.[10] From the first line of code: registered users only, personal accounts, encryption at rest, burned-in watermarks, every view tracked to the second.

And no direct links to content. Never. Clients asked for them, often, and we faced a good deal of disappointment and a few defections. We still think it was right. A doctor protects a patient's health even when the patient would rather not think about it; we protect our clients' work in the same way. Instead of opening holes that let strangers in, we built easy ways out.

In the end, this is why Mnemonica was the first European SaaS platform ever to earn **TPN Gold Shield**, and holds **ISO 27001** certification.[10]

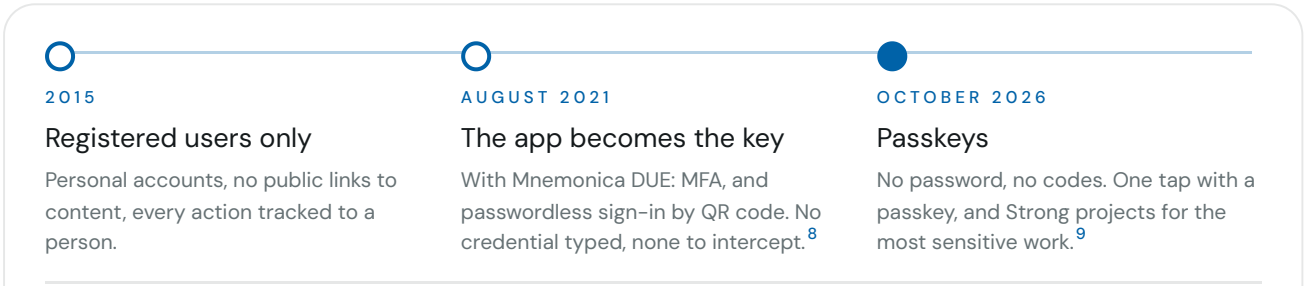

Figure 3. Each step removed a secret from the sign-in, and made it simpler.

08

THE NEW SIGN-IN

One tap, and a lock for what matters most

Since 17 October 2026 the password field and every MFA code are gone.[9] Each session now has its own security level, depending on how you signed in. A session is strong when it was opened with a phishing-resistant method (a passkey, the Mnemonica app unlocked on your device, or a QR code approved in the app) and basic otherwise. A manager can mark a project **Strong**: from then on only strong sessions open it, for everyone and even just to watch.

About the email link. First sign-in uses a one-time link, valid for 15 minutes. It contains no secret a fake page could capture, but it only proves you can read a mailbox, so it opens a basic session, never a Strong project. Links to content remain what they have always been at Mnemonica: absent.

HOW YOU SIGN IN	SESSION	WHAT IT OPENS
Email link · Google · Apple	Basic	Projects that are not Strong, as your role allows
Passkey · Mnemonica app with device unlock · QR code approved in the app	Strong	Strong projects, company management, devices and keys

Figure 4. Session strength in the new Mnemonica sign-in. Losing every strong method leads to a reset with a 24-hour basic-only window.[9]

09

YOUR TURN

Still in the naive age of online security?

A few questions to check how far your own data hygiene has come:

- [ ] Do you and your team work on devices that are locked and kept up to date?
- [ ] Is every login personal, or still shared with colleagues, family or friends?
- [ ] Have you replaced passwords with passkeys wherever a service offers them?
- [ ] Does unreleased material still travel by link, in either direction?

10

NORTH STAR

Security is how we care for the work

Producers, distributors and archives do not need to become security experts: that is what technical teams and trusted partners are for. They need the same reflex the industry already has offline, where nobody questions closed sets, embargoed screenings or locked vaults. Passkeys make that reflex effortless online. Mnemonica will keep evolving in that direction, because protecting our clients' work is the reason we exist.

MNEMONICA

Built around the same principles

Mnemonica is the secure European content hub for film and HETV: review and approval, fast file transfer, and a masters library with deliveries, all in one place, with more than 30,000 registered film professionals.

Made in the EU · ISO 27001 · TPN Gold Shield

PASSWORDLESS SIGN-IN WITH PASSKEYS

NO LINKS TO CONTENT

STRICTLY PERSONAL ACCOUNTS

LEARN MORE

mnemonica.com

info@mnemonica.com

NOTES AND SOURCES

1. Verizon, *2025 Data Breach Investigations Report*: compromised credentials as initial access vector in 22% of breaches; stolen credentials in 88% of basic web application attack breaches; third-party involvement doubled to 30%. verizon.com/business/resources/reports/dbir
2. Singapore Police Force, *Man arrested for unauthorised access to a media-content server*, press release, 24 April 2026. police.gov.sg/media-hub/news/2026/04/20260424_man_arrested_for_unauthorised_access_to_a_media_content_server · W. Cho, *The Lost 'Airbender': How Paramount's Movie Hack Spiraled Into a Crisis*, The Hollywood Reporter, 4 June 2026. hollywoodreporter.com/business/digital/last-airbender-movie-hack-paramount-1236604522
3. FIDO Alliance, *Passkeys*: public key cryptography, challenge-response sign-in, biometrics kept on the device, phishing resistance for synced and device-bound passkeys. fidoalliance.org/passkeys · passkeycentral.org
4. Apple, WWDC24 session 10125, *Streamline sign-in with passkey upgrades and credential managers*: most additional factors used today are still phishable. developer.apple.com/videos/play/wwdc2024/10125
5. FIDO Alliance, *Passkey Index 2026*, October 2026: success rate 93% vs 78% (n=12); 2.8× faster, about 27 s saved, indicative (n=9); 36% of sign-ins (n=12). fidoalliance.org/passkey-index-2026
6. Microsoft Learn, *Passkeys by default and retirement of Microsoft-provided SMS and voice authentication*, Microsoft Entra ID. learn.microsoft.com/en-us/entra/identity/authentication/concept-sms-voice-retirement
7. Thales, *2026 Bad Bot Report* (covering 2025): bots 53% of internet traffic, bad bots 40%. cpl.thalesgroup.com/resources/application-security/2026-bad-bot-report
8. Mnemonica, *Access without credentials: passwordless login*, 8 August 2021. mnemonica.com/updates/access-without-credentials-passwordless-login
9. Mnemonica, *Goodbye passwords. Goodbye MFA. Hello, one-tap sign-in*, 9 October 2026. mnemonica.com/updates/new-sign-in
10. Digital Production, *Mnemonica sets out to fix digital cinema memory*, 13 February 2026, interview with Piero Costantini and Stefano Diana. digitalproduction.com/2026/02/13/mnemonica-sets-out-to-fix-digital-cinema-memory

Figures from third parties are reported as published by their sources. FIDO and passkey are terms of the FIDO Alliance; other names belong to their owners. © 2026 Mnemonica · mnemonica.com