yubico

Considering Passkeys for your Enterprise?

Avoid common pitfalls of synced passkeys

Different passkey implementations

What’s the difference between synced and hardware-bound passkeys?

Passkeys are more secure than passwords and enable a move to passwordless authentication. To learn more about them you can click here.

There are two types of passkeys, synced and hardware-bound.

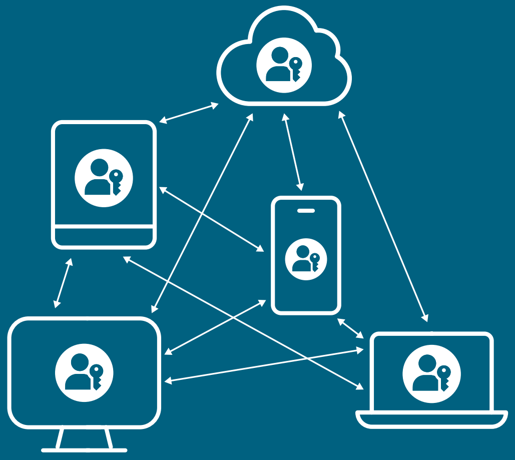
Synced passkeys are copyable across various devices such as smartphones, laptops, tablets connected to a user account. This may create some chilling failure points for the enterprise.

A few common scenarios when your passkey might be vulnerable at work:

- Remote or hybrid workers getting phished
- Insider threat risks with employees sharing passkeys
- Supply chain vendors sharing passkeys when they shouldn’t
- Privileged users sharing passkeys with administrative assistants to complete tasks

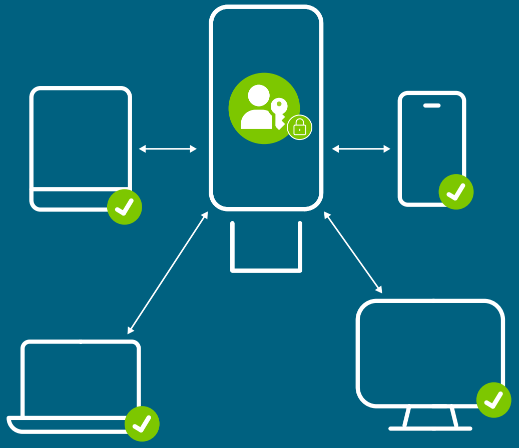
Read each of the four scenarios below to see how one common mistake can lead to passkeys getting shared with the wrong people.

Synced vs Hardware-bound Passkeys



Synced Passkeys

Lives on a smartphone, tablet, laptop or other device where it can be copied and synced across many devices.



Hardware-bound Passkeys

Lives on a USB key or other piece of hardware separate from everyday devices and delivers higher security assurance.

Scenario 1

Remote Worker Account Compromised

A passkey syncs between all owned devices on a single iCloud account. Here's a story of how that proved dangerous for Jim, a full-time remote worker for a tech company.

Jim works at home, where his whole family uses the same iCloud account with six different devices.

1. Jim logs onto his work account with his work phone in his home office. But he uses his personal iCloud account on his work phone.
2. Next door, Jim's son Ben gets an email with a cool link about an app-based game he likes to play. He clicks the link.
3. Ben gets phished – the link allows an attacker to register his own account on the family's iCloud account.
4. When Jim's work phone syncs to the cloud, his work passkey is transferred with everything else, syncing with all devices on the iCloud account. That includes the attacker's device!
5. Once the attacker has Jim's work credentials, he can log onto work sites as Jim and then seek other credentials with higher privileges. Jim got some warnings about other devices being added but noticed too late.

DID YOU KNOW?

89% of organizations experienced a phishing attack in the past year.

HYPR, 2022 State of Passwordless Security Report

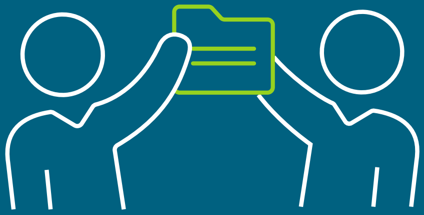
Scenario 2

Insider Threat: Sharing Between Employees

A passkey can be easily shared with another device through the AirDrop feature on iPhone, SMS, or a Bluetooth pairing. Here's a story of what happened when Neil got a bit careless with his credential.

1. Neil was feeling like he needed a day off but knew he had to retrieve a file at work and send it to a vendor.

2. He stayed home to rest, but asked his friend Derek to log in as him to complete the task instead. He shared his work credential with Derek over a text message.



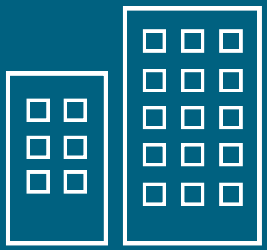
3. When a third person needed a file from the same folder Neil had access to, Derek thought he was being helpful by sharing Neil's credential with that third person. Neil is unaware this ever happened.

4. Now Neil's credential, which is highly privileged, exists on three devices, which are syncing on three different iCloud accounts! It's three times as likely to be stolen, and no one who is monitoring the system can know who the "real Neil" is.

Scenario 3

Supply Chain Vulnerability: What Vendors Do When You're Not Looking

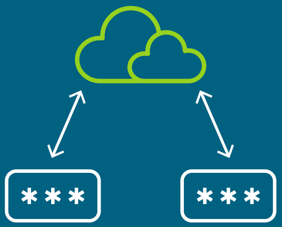
A passkey's shareability is convenient in some situations, but when vendors have access to systems without following good passkey security guidelines, that system becomes compromised. Listen to Kira's story.



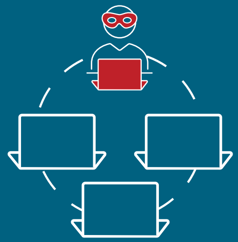
1. A large retailer with a complex supply chain allows their HVAC system monitor (an outside vendor) to log into essential systems to check real-time conditions.

2. Kira, a new employee at the vendor, forgot her work-issued phone with her passkey on it. So she has someone at home send the credential to her friend's work-issued phone since they do the same kind of work.

3. But the friend's phone was a personal phone that also had a work credential. The friend's iCloud account had already been compromised through an earlier phishing attack, and a bad actor's device was listed on the account without her knowing.



4. When Kira's iCloud account automatically syncs, the bad actor gets two work credentials – Kira's and her friend's.



5. The attacker has full access to the large retailer's systems and can find other angles of attack.

Scenario 4

Let the Admin Do It

Privileged users are often executives that are pressed for time and rely on their staff to take care of administrative hassles online. Here’s a story of how a C-suite executive delegated herself into a cybersecurity crisis.

DID YOU KNOW?

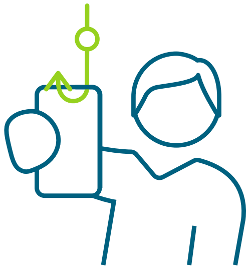
60% of large and global enterprises, and 90% of midsize enterprises are implementing passwordless methods in more than half of their use cases — up from 5% in 2018.

Ant Allan, Vice President Analyst, Gartner.

1. COO, Kim relies a lot on Dave, her administrative assistant.

2. On her way to the airport, Kim remembers an incomplete expense report from her last trip. She shares her passkey in a text message to Dave’s personal phone so he can fill in the details.

3. Dave sees it as part of his job to log in as Kim and take care of it, even though he knows it’s technically against the in-house security guidelines.



4. Dave’s personal phone was phished earlier in the month when he logged onto a sports betting Web site and his iCloud account was compromised without his knowledge.

5. All the passkeys on Dave’s phone (including Kim’s) are synced to all devices on his account, including the one added during the phishing attack.

6. A bad actor now has privileged access – he can access Kim’s email to send fake payment requests that funnel straight into his account.

Key Takeaways

Passkeys are better than passwords because they're based on modern FIDO protocols and offer stronger defense against phishing.

However, synced passkeys that are easily copyable and can be shared easily leave enterprises open to lapses in security. Hardware-bound passkeys, like the YubiKey, offer the strongest security assurance and meet the most stringent compliance needs.

How to Choose the Right Passkey Solution

SERVICE PROVIDERS

Consumers

Synced passkeys on their devices are probably okay

Consumers at Risk

High risk users - e.g. journalists - may require extra security for passkeys, such as those residing in security keys

ENTERPRISES

First line workers

Need a solution that is not dependent on their personal device to authenticate

Office workers

Require security keys with hardware attestation to ensure credentials cannot be copied

Privileged users

Highest risk users – require security keys with hardware attestation to know where the credentials are stored yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company is a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, FIDO Universal 2nd Factor (U2F) and other open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: yubi.co/passkey.