Stafrace Managment & Marketing Consultancy

Trust
Learning
Innovation

20th Apr 2026 to 3rd July 2026

Welcome To

Wesley Mission Technologies Smartphones Term 2 2026

JOE STAFRACE
WWW.STAFRACEMMC.COM
Joe.Stafrace@gmail.com
0497 093 465

WIFI Password

Go to your Settings

Locate WiFi

Choose Network **WM_Guest**

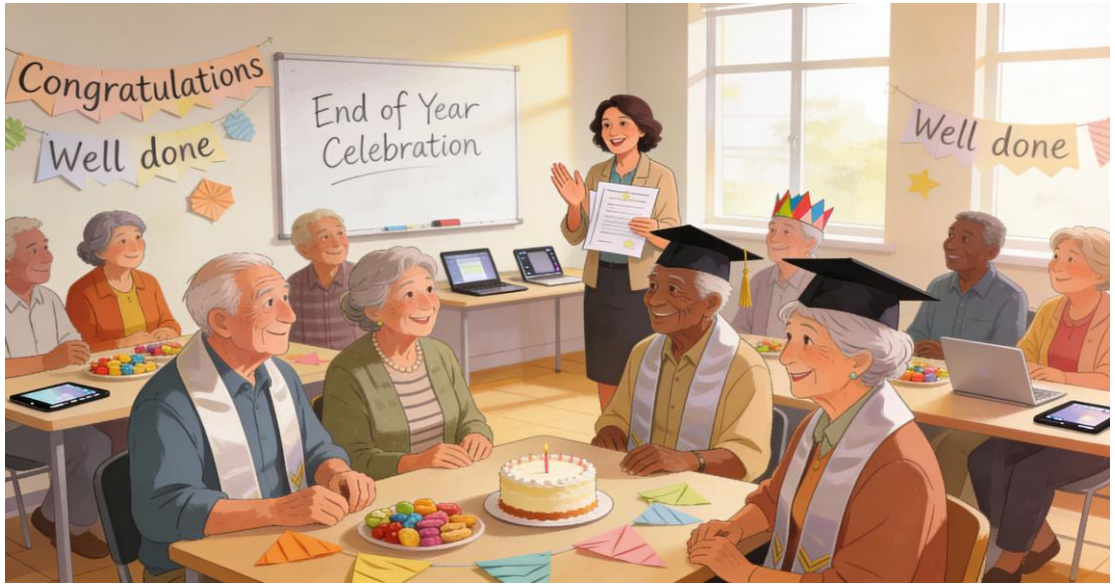
Enter Password as shown below

ST@ngryBr!an7#

SMART TECHNOLOGIES CLASSES

10:00 TO 11:30
SMART PHONES

11:35 TO 1:00
COMPUTERS/TABLETS
TECHNOLOGIES



TERM 1 CLASSES

Apr 21

Apr 28

May 5

May 12

May 19

May 26

Jun 2

Jun 9

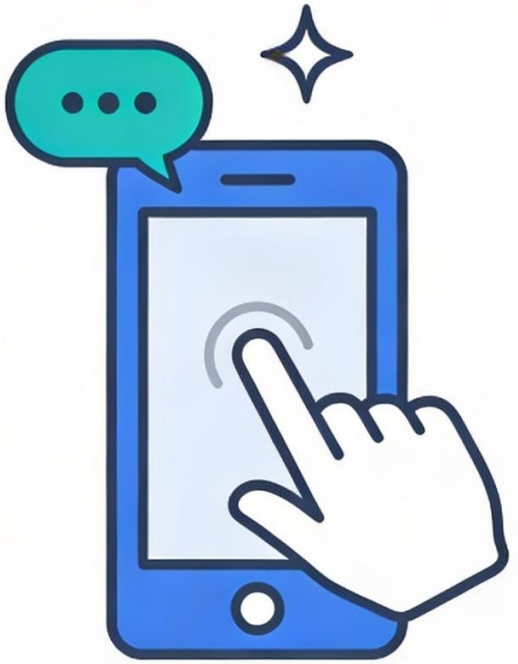
Jun 16

Jun 23

Jun 30

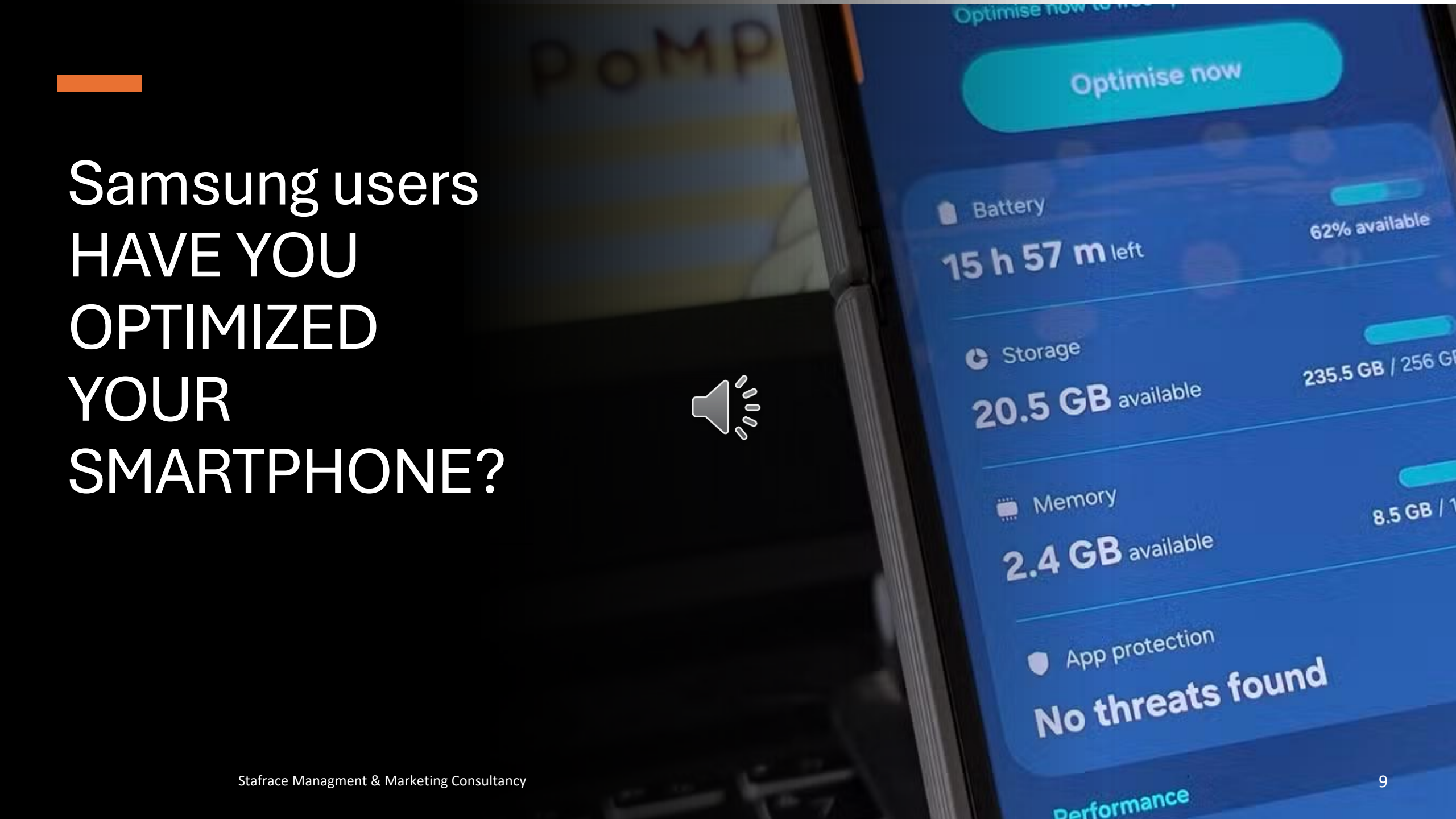
Some topics in this course may feel familiar to those who have attended previous classes. However, since technology continues to evolve at a rapid pace, revisiting the basics ensures that everyone stays up to date and confident with the latest tools and features

- “**Your questions are important — we’re here to answer them.”**



Smartphone Basics

Samsung users HAVE YOU OPTIMIZED YOUR SMARTPHONE?

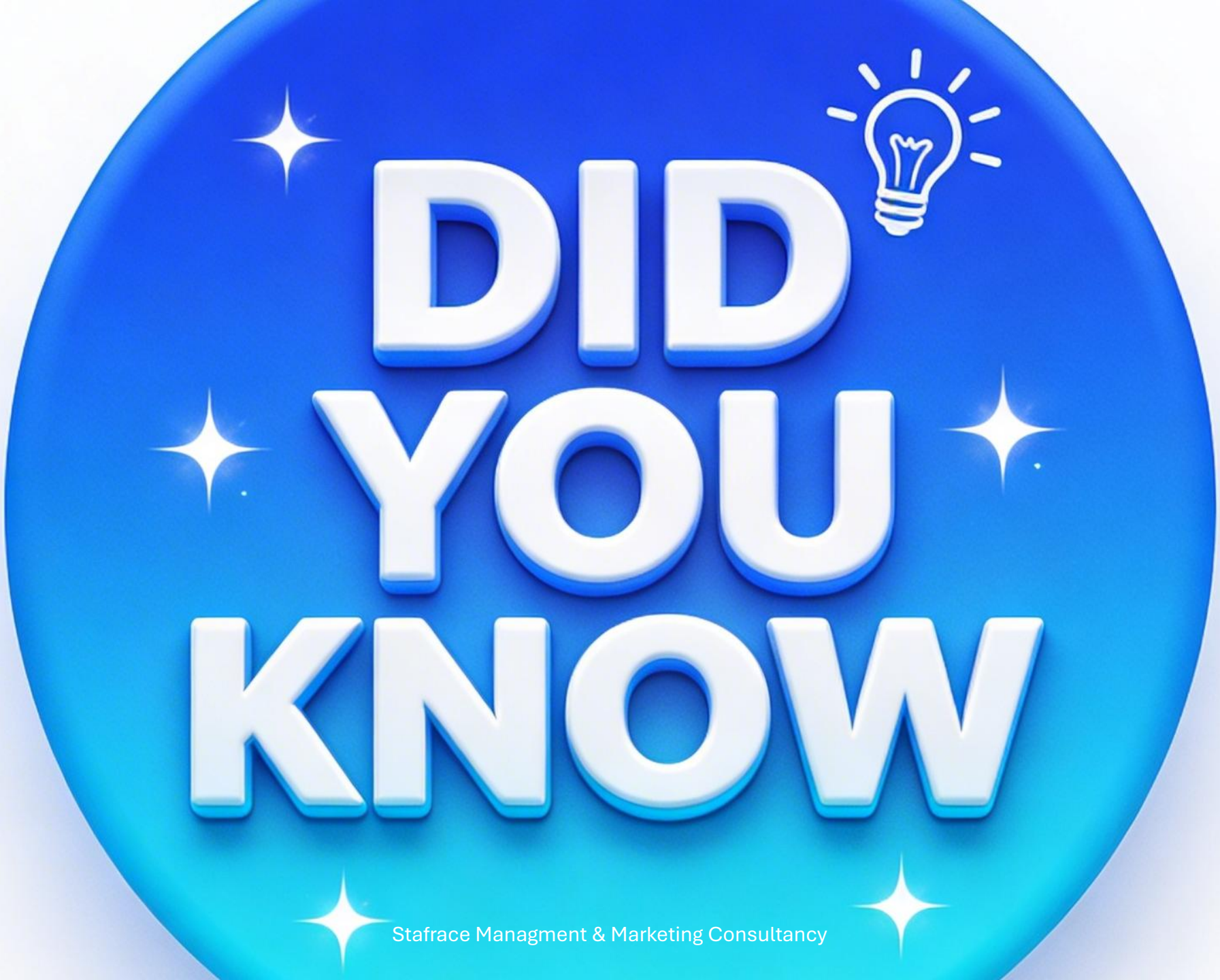



Tech
News


26.4.2


26.5


iOS
27



Stafrace Managment & Marketing Consultancy

To export contacts to external storage, the usual path is in the phone’s Contacts app, where you choose Export or Import/Export and save the contacts as a VCF/vCard file to SD card, USB storage, or internal storage first, then copy the file to your external drive if needed.

Android phones
Open the Contacts app.

Tap the menu or three dots, then choose Settings, Manage contacts, or Import/Export contacts depending on the phone brand.

Select Export or Export to .VCF file.

Choose the destination: SD card, USB storage, or internal storage.

Confirm, then look for the saved VCF file in Files/My Files and copy it to a USB drive or other external device if it was saved internally first.

iPhone
iPhones do not usually offer a direct “export to SD card/USB” option inside Contacts the way Android does. The common method is to sync contacts to iCloud or another account, then export them from a computer as a contact file and copy that file to external storage.

On the iPhone itself
Open Contacts.

Tap the Lists button at the top left.

Touch and hold a contact list, or create a new list, then tap Export.

Choose the fields you want included, then save or share the exported contact file.

If your USB drive is connected to the iPhone, choose Save to Files and select the USB drive in Locations.

https://www.samsung.com/ph/support/mobile-devices/how-to-backup-and-restore-contacts-on-your-samsung-galaxy-smartphone/

https://support.apple.com/en-au/guide/iphone/iph075ddebf2/ios

https://www.techcommuters.com/how-to-import-and-export-phone-contacts-on-android-iphone/

The safest official way is Samsung’s remote unlock through Find My Mobile / SmartThings Find if it was enabled on your phone before you got locked out. If that wasn’t set up, the usual fallback is a factory reset, which erases the phone’s data.

https://youtu.be/6bQngMZ87aM

What “USB” means
USB stands for Universal Serial Bus. It defines:

How devices talk to each other for data (keyboards, mice, drives, phones, printers).

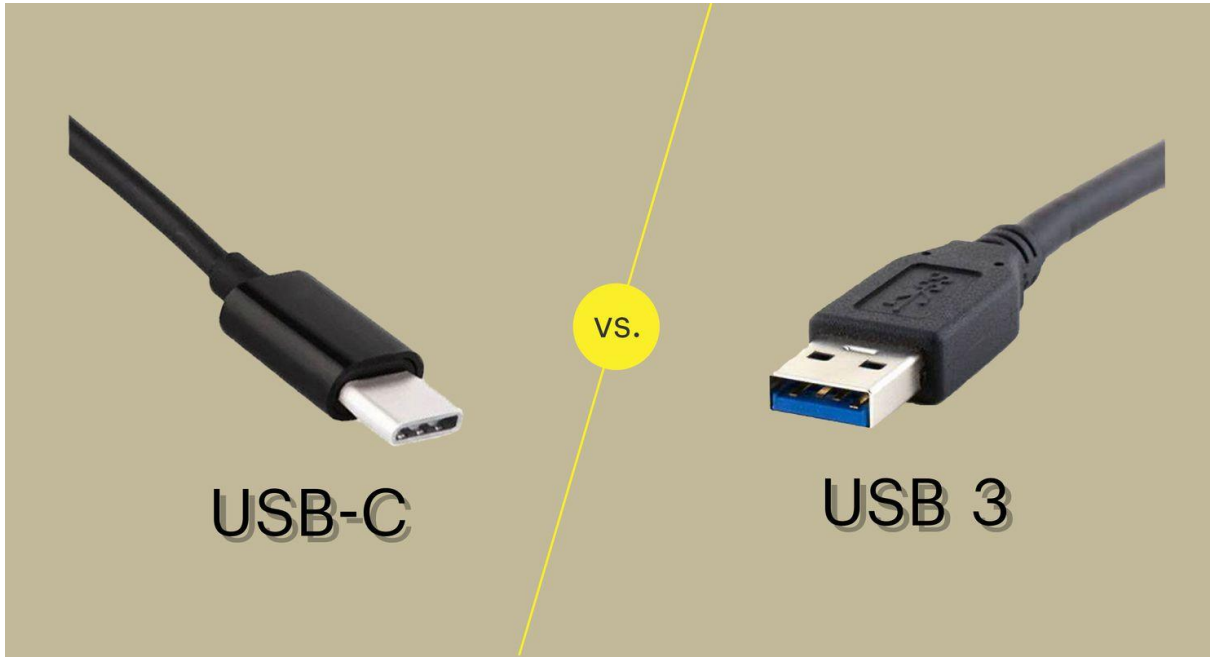
How much power can be sent to charge things (earbuds, phones, tablets, laptops).

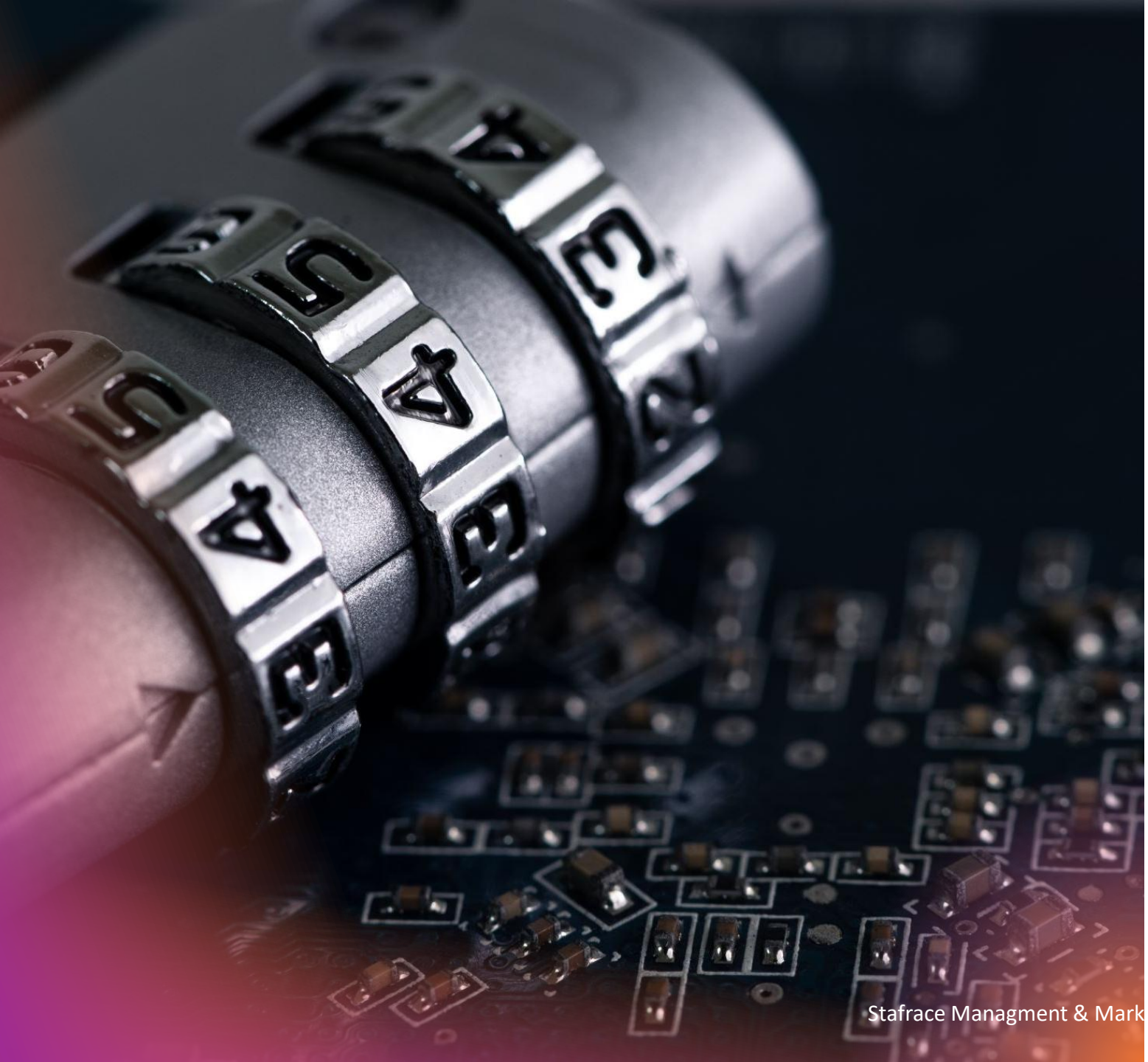
Different connector shapes:

USB-A: big flat rectangle found on older PCs, chargers.

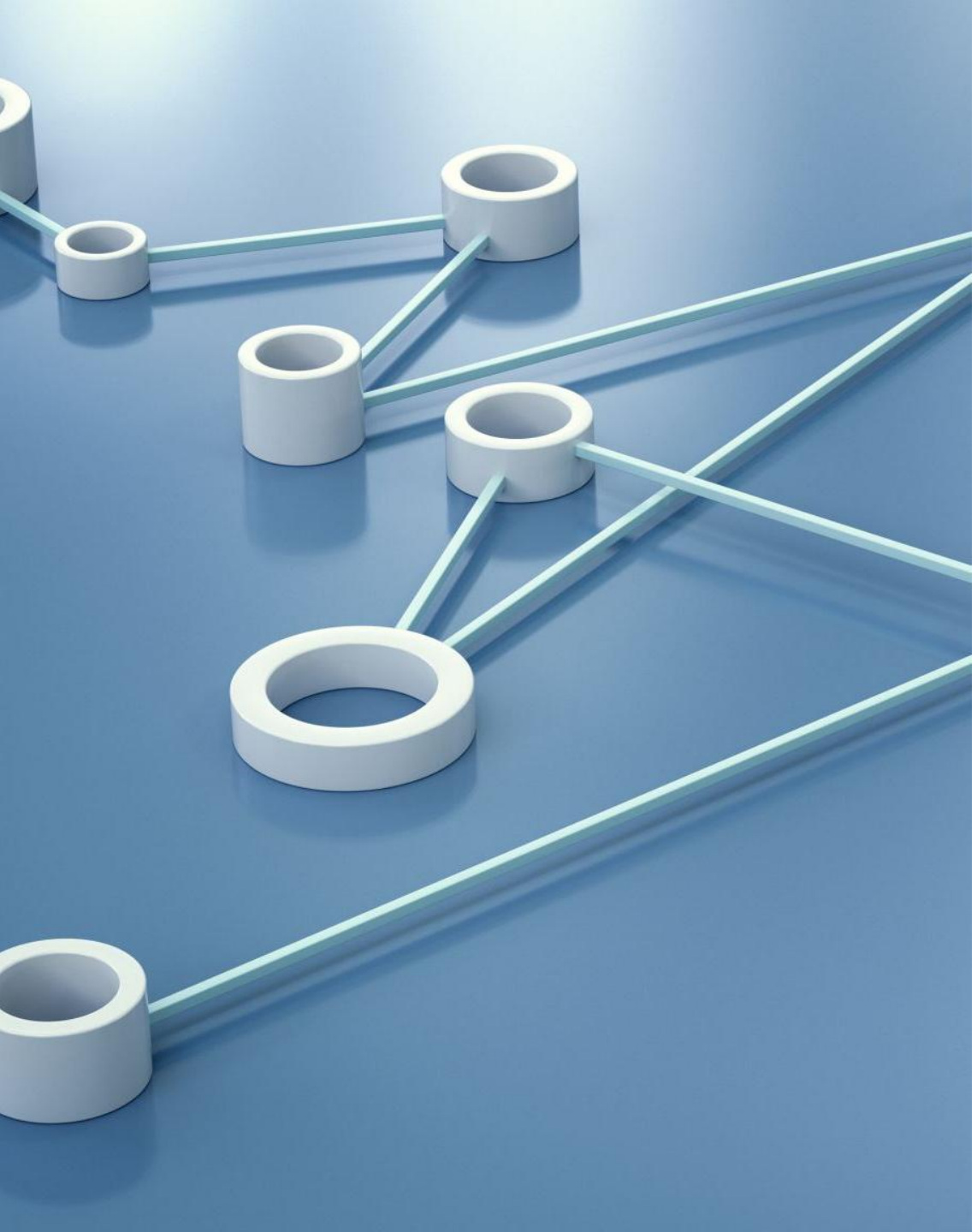
USB-B: squarish, often on printers and some external hard drives.

Mini/Micro USB: small older phone/connectors.





- Stop changing weak passwords. Start replacing them with passkeys
- Passwords are a pain. You should ditch ’em.



- PCWorld advocates replacing traditional passwords with passkeys, which use public-key encryption and biometric authentication for superior online security.
- Passkeys are phishing-resistant and site-specific, preventing malicious fake sites from accessing your credentials during data breaches.
- Starting with major services like Google, Apple, and Microsoft is recommended for frequently accessed accounts before expanding adoption.

- Passkeys don’t require memorization, can be stored directly on your phone, and are stronger than passwords. One particular advantage: They’re phishing-resistant. Also, if a website gets hacked (all too common these days), your credential information shouldn’t be crackable nor usable by anyone else.

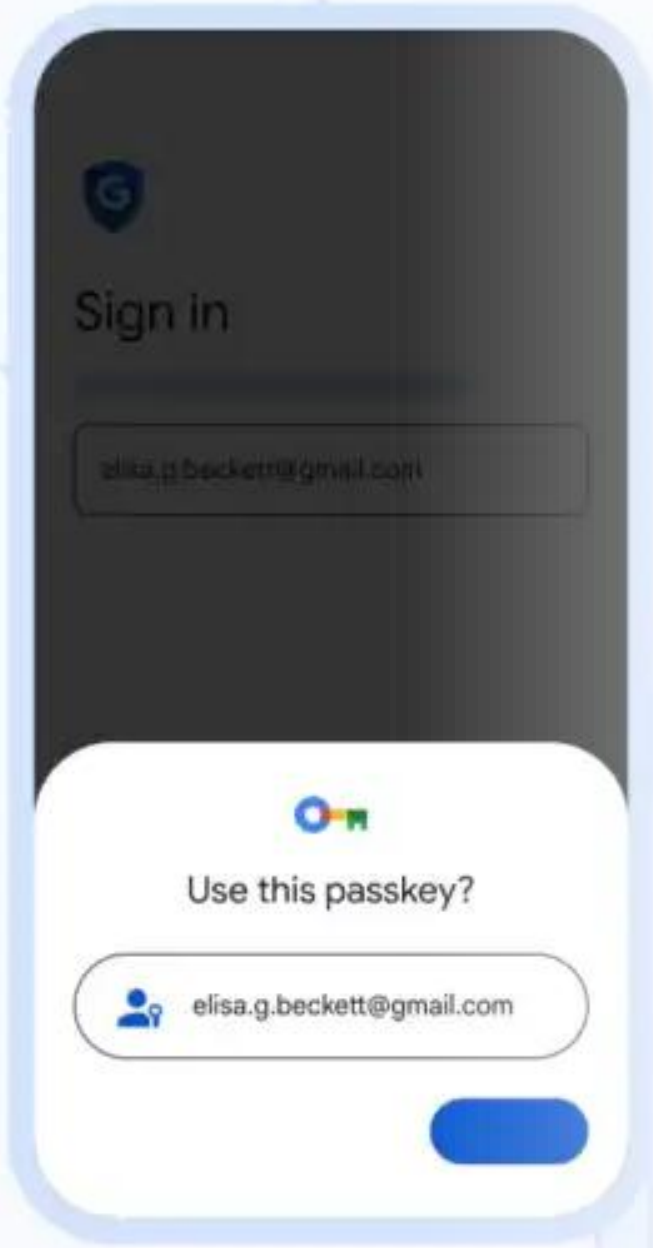
- When you create a passkey, both a public and a private key are generated. (This is known as public-key or asymmetrical encryption.) The private key is kept by your device or password manager. Supported devices include phones, tablets, hardware dongles like YubiKeys, and compatible PCs. You can choose to store passkeys locally on your device or in the cloud.

- These secret keys are secured by your device's biometric authentication (e.g., fingerprint or face), or the method that secures your password manager.

- Meanwhile, the public key is shared with the website it’s generated for. You need both the public and private key to log in to the account they’re tied to. Whenever you log on, the website will ask for proof you’re the account owner, via the following steps:

- A request is sent to your device (or password manager) to begin the verification process.
- Your fingerprint, facial scan, or other authentication method is required to authorize the request.
- If you approve, your private key (aka secret key) is used to create a digital signature, which is then sent to the website.
- The website then uses the digital signature to try unencrypting the public key you gave it. If successful, you’re in.

- When passkeys are implemented correctly, no one can deduce your private key based on the public key—which means data leaks and breaches aren’t as dangerous. (At least, in regard to password health.) Passkeys also only work for the specific site they’re generated for, so they can’t be captured or used by fake malicious sites, which is how phishing schemes steal passwords.



- Passwords have one big flaw: If anyone guesses what your password is, you're left with no defense. It's why we use password managers and two-factor authentication to better safeguard our accounts.

- If that sounds exciting, you’re in luck. Passkey support beginning to pick up steam, and Google is the latest big corporation to let you log into an account with a passkey.

Here is a simple, step-by-step way to set up a Google passkey on a smartphone. This works for both Android and iPhone as long as you can sign into your Google account on the phone and you use a screen lock (PIN, fingerprint, Face ID, etc.).

Step 1 – Open Google's Passkey page on the phone
On the smartphone, open Chrome or Safari (or your usual browser).

In the address bar, type:
g.co/passkeys and go.

If asked, sign into the Google account you want to protect.

You should now see a page called "Passkeys" for your Google Account

- Does Your Device Support Passkeys?
- Before you start, you should ensure the devices you want to create a passkey with are supported. Google's documentation lays out three important categories. You'll need at least Windows 10 (2015) or macOS Ventura (2022) for desktops and laptops. For mobile devices, you'll need at least Android 9 (2018) or iOS 16 (2022).

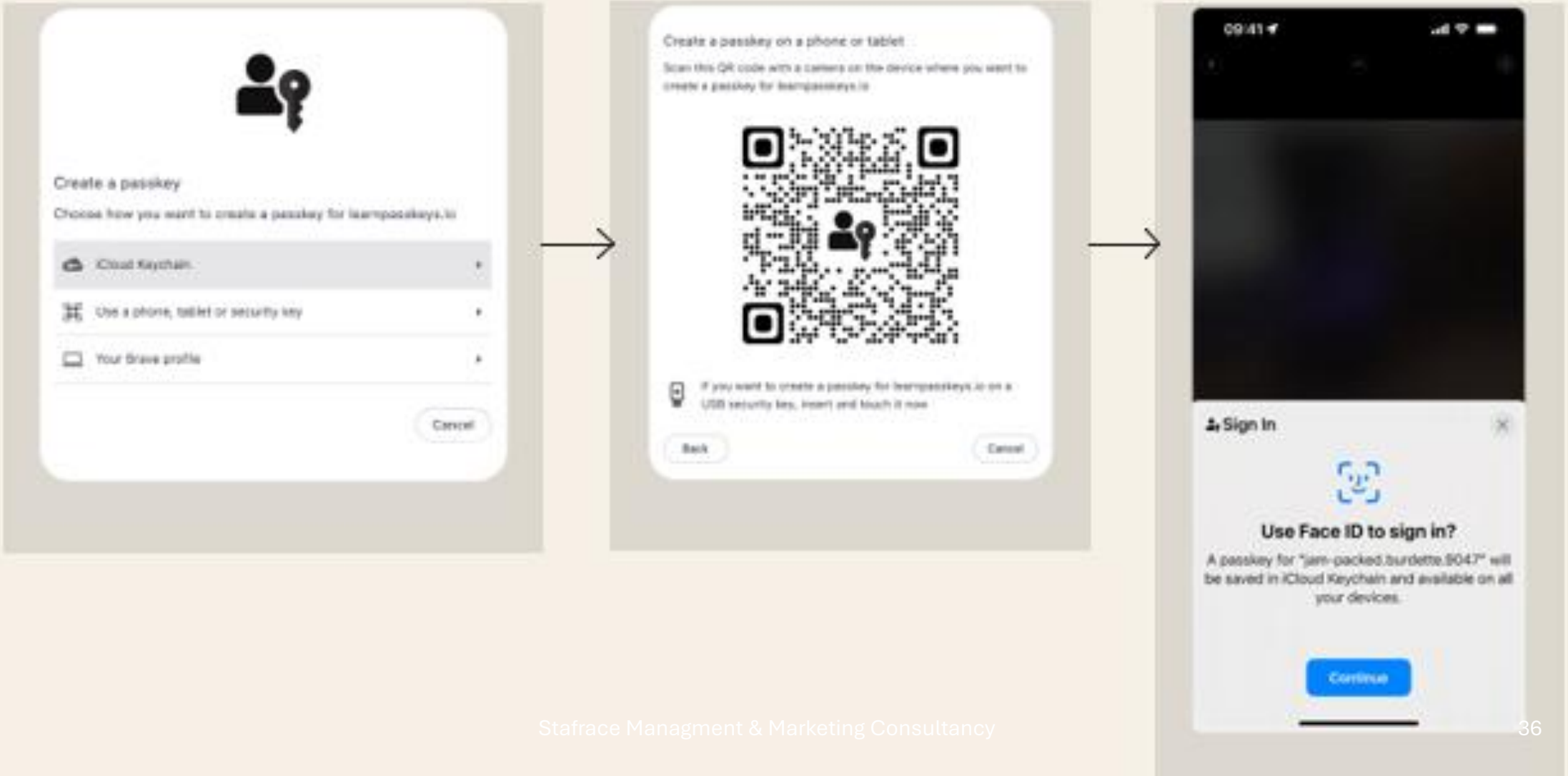
- https://youtu.be/Wj2z-hQHcIw

- https://www.google.com/account/about/passkeys/

The user is prompted to select an authenticator since they may have multiple devices capable of handling passkeys.

When the user selects their phone, they get a QR code to launch the passkey creation process on the phone.

The phone prompts the user for authentication, which will rely on biometrics or a PIN code to lock the newly created passkey.



- A lot of services still do not support passkeys in 2026, especially smaller websites, legacy business systems, many banks, government portals, and niche retailers. Even among big consumer brands, support is still incomplete, and password login remains the default for many accounts

- Common holdouts
- Many banks and financial institutions still lack passkey support, though this varies by institution.
- Government and public-service portals are often still password-only.
- Legacy workplace systems, HR platforms, and older enterprise apps frequently do not support passkeys yet.
- Smaller e-commerce sites and one-off online stores commonly still rely on passwords.

Examples mentioned as not supporting

ChatGPT.

Claude.

DeepSeek.

Reddit.

Spotify.

Instagram.

AliExpress.

Temu.

Shein.