



دليل

التوعية السيبرانية

لضيوف الرحمن



الشريك الاستراتيجي



وزارة الحج والعمرة
MINISTRY OF HAJJ AND UMRAH



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority



يتوفر هذا الدليل باللغات التالية
ويمكنك تحميلها بالضغط عليها:

English

ENG

عربي

AR

বাংলা

BEN

Bahasa Indonesia

IND

Français

FRA

Hausa

HAU

Türkçe

TUR

اُردُو

URD

Español

SPN

Русский язык

RUS

Bahasa Malaysia

MAY

සිංහල භාෂාව

SIN

አማርኛ

AMH

فارسی

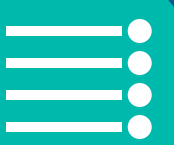
PER

o'zbek

UZB

हिंदी

HIN



محتوى دليل التوعية السيرانية



اضغط على العنوان للوصول إلى الصفحة المطلوبة

أهمية الوعي بالأمن
السيراني في موسم
الحج والعمرة



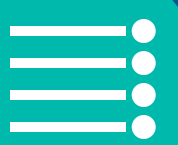
أساليب الهندسة
الاجتماعية والتصيد
وكيفية تجنبها



تعيين رمز الدخول
وإعداد السمات
الحيوية



التصفح الآمن
لشبكة الإنترنت



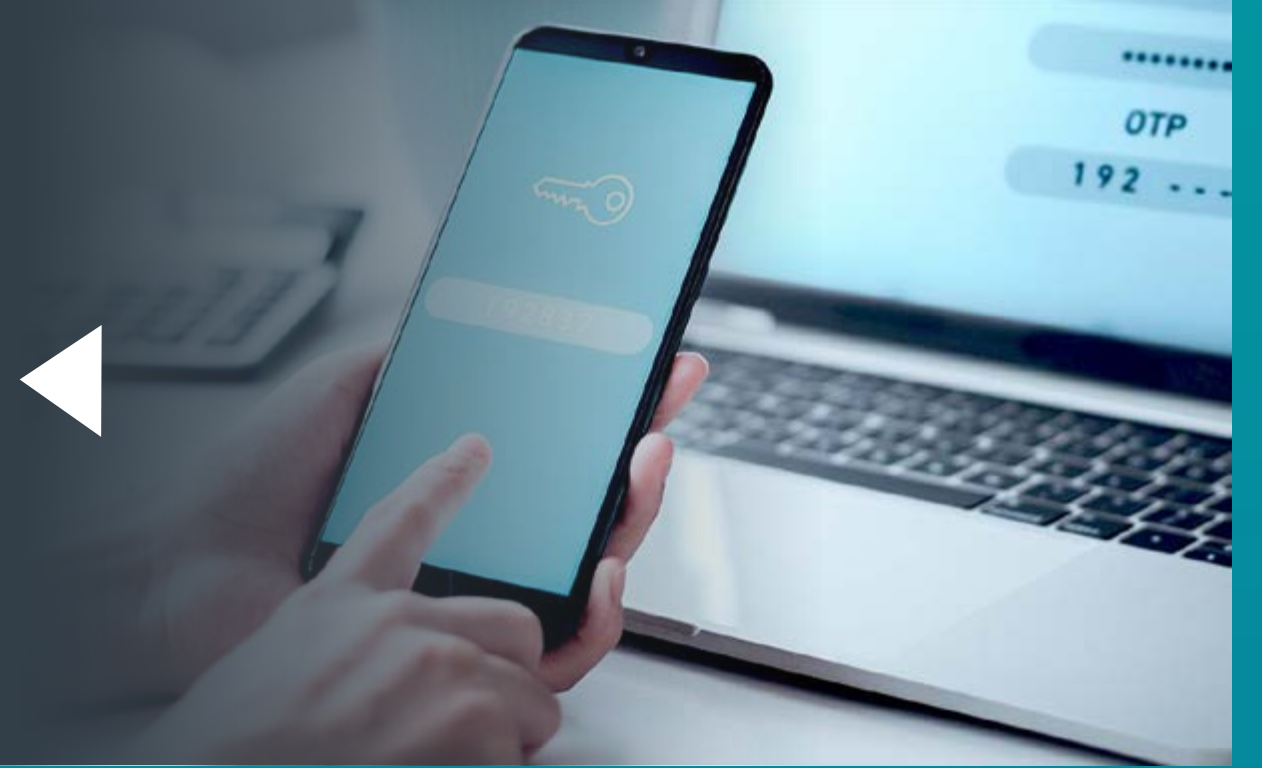
أمن التطبيقات



تثبيت التحديثات للأجهزة



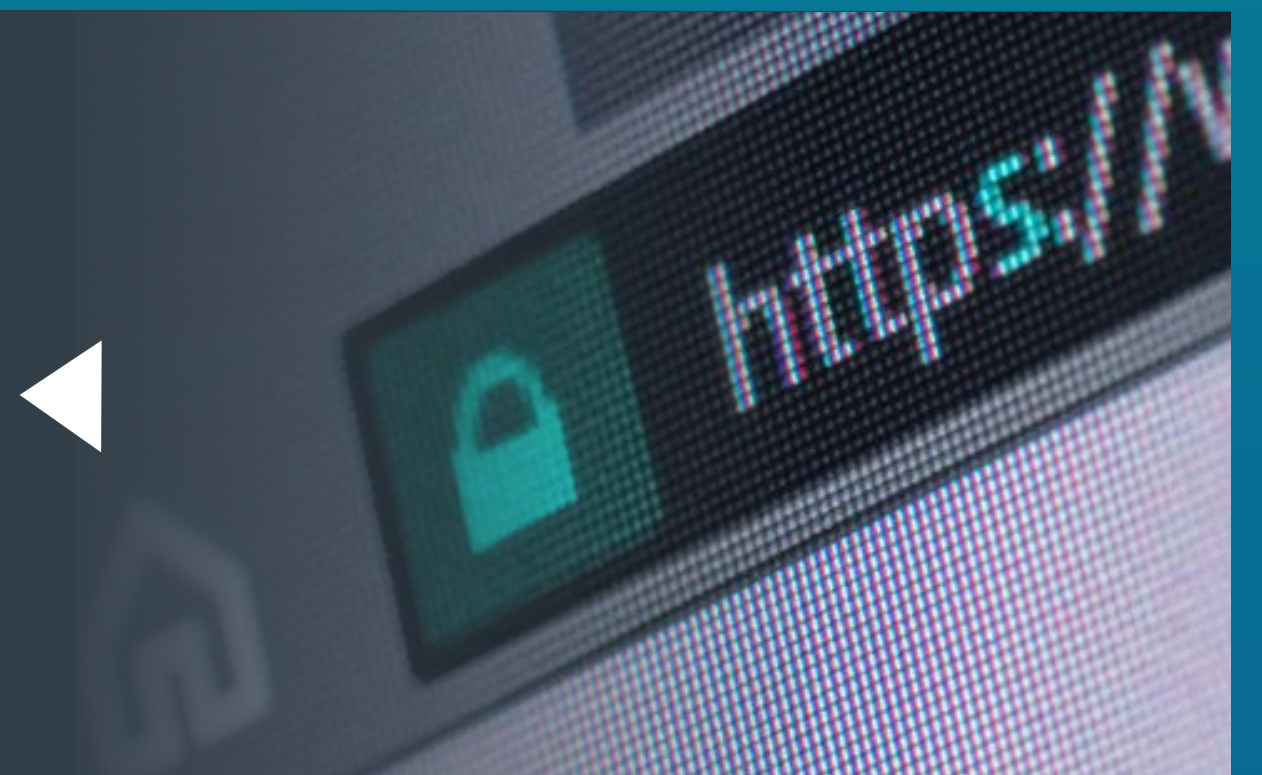
رمز الوصول لمرة واحدة OTP



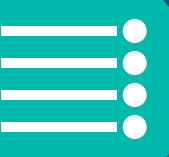
فقدان الهاتف وأهمية عمل النسخ الاحتياطي



مواقع وتطبيقات تهتمك



أرقام تهتمك





أهمية الوعي بالأمن السيبراني

في موسم الحج والعمرة

يستخدم المهاجمون حيل متجددة

لشن الهجمات السيبرانية

سواءً من خلال المواقع والتطبيقات المزيفة أو الرسائل التصيدية أو غيرها من الحيل.

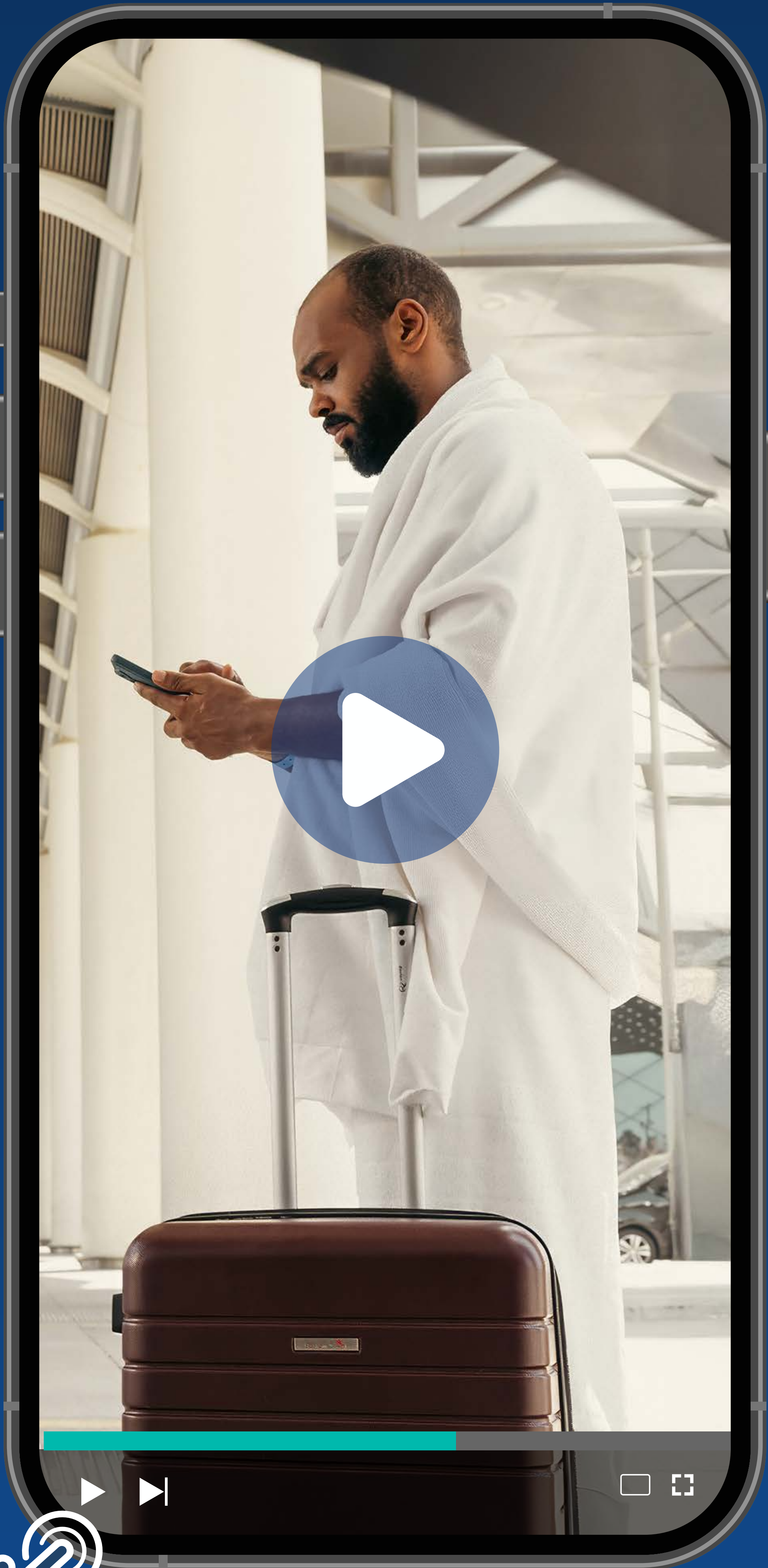
ويعتمدون غالباً على استغلال العنصر البشري والممارسات السيبرانية غير الآمنة التي قد يقومون بها.

لذلك،

تأتي أهمية الوعي بالأمن السيبراني كأحد أوائل خطوات الدفاع للحد من المخاطر السيبرانية المتجددة التي يشهدها الفضاء السيبراني.



يُعدُّ الوعي السيبراني من أوائل خطوات الدفاع للحد من التهديدات المتجددة في الفضاء السيبراني



اضغط للوصول إلى الفيديو



6



أساليب الهندسة الاجتماعية

والتصيد وكيفية تجنبها

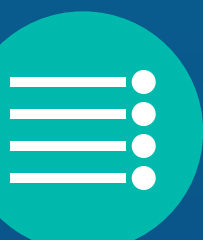


تقوم الهندسة الاجتماعية على استخدام حيل وأساليب التلاعب تجاه الأشخاص المستهدفين.

لدفعهم على الإفصاح عن معلومات حساسة أو لحثهم على القيام بإجراءات خاطئة تعرض أمنهم السيبراني للخطر.

ومن الأساليب التي قد يستخدمها المهاجم لشن هجمات الهندسة الاجتماعية:

- التظاهر بأنه من جهة معروفة وموثوقة.
- التظاهر بأنه أحد الأشخاص المعروفين لديك.
- التظاهر بأنه من جهة ترغب في تحديث أو تأكيد بياناتك.
- الوعود بتقديم خصومات مغرية تتعلق بالحج والعمرة.
- التظاهر بأنه من الجهات الحكومية أو الشركات التي تقدم خدمات الحج والعمرة.



أساليب الهندسة الاجتماعية

والتصيد وكيفية تجنبها



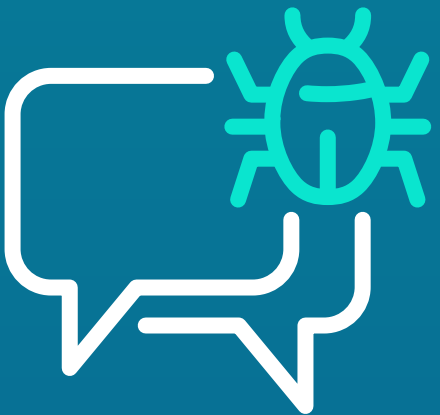
يُعتبر **التصيد الإلكتروني** أحد أبرز أشكال الهندسة الاجتماعية ويتم من خلاله محاولة سرقة البيانات الحساسة أو الاستيلاء على الحسابات أو اختراق الأجهزة.

من قنوات التواصل التي تستخدم لغرض التصيد:



1

الروابط والمواقع والتطبيقات المزيفة.



2

منصات التواصل الاجتماعي.



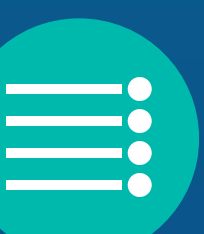
3

الرسائل النصية.



4

التواصل الهاتفي.



أساليب الهندسة الاجتماعية

والتصيد وكيفية تجنبها

للحد من مخاطر التصيد الإلكتروني.. احرص على:

استخدام المواقع
الرسمية والموثوقة.



تحميل التطبيقات من
المتاجر المعروفة.



عدم الضغط على الروابط
مجهولة المصدر.



الحد من مشاركة البيانات
الشخصية والحساسة.



تعيين رمز الدخول وإعداد السمات الحيوية

يُعد أمراً بالغ الأهمية ويُسهّم في:



1 التحقق من هوية المستخدم.



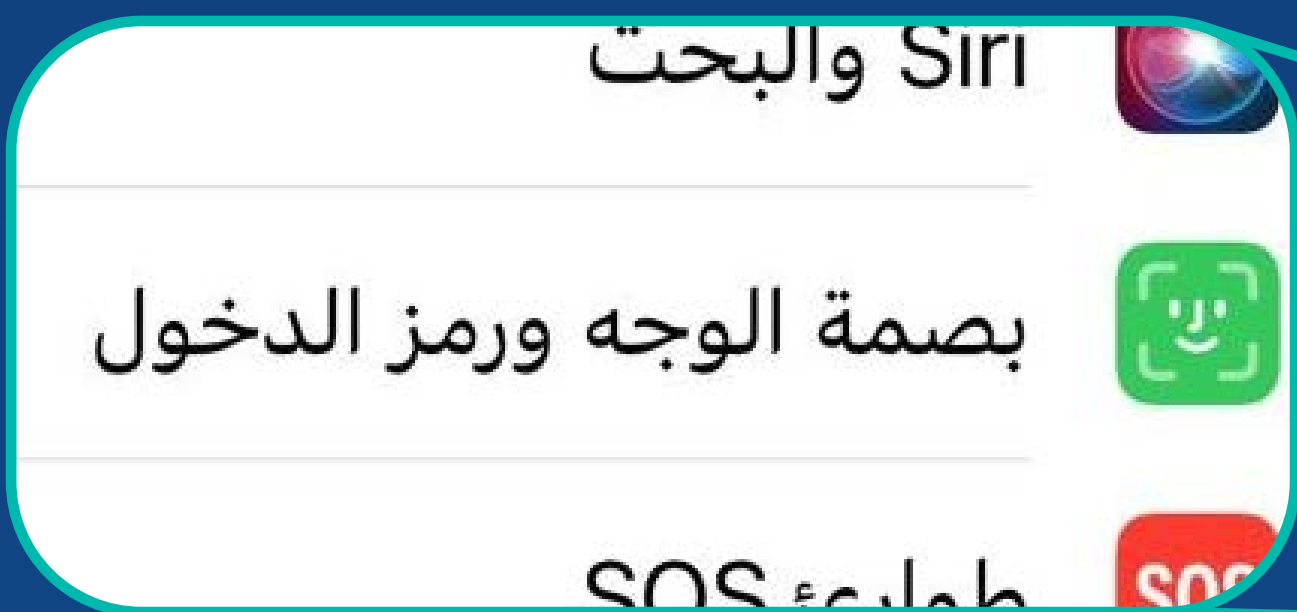
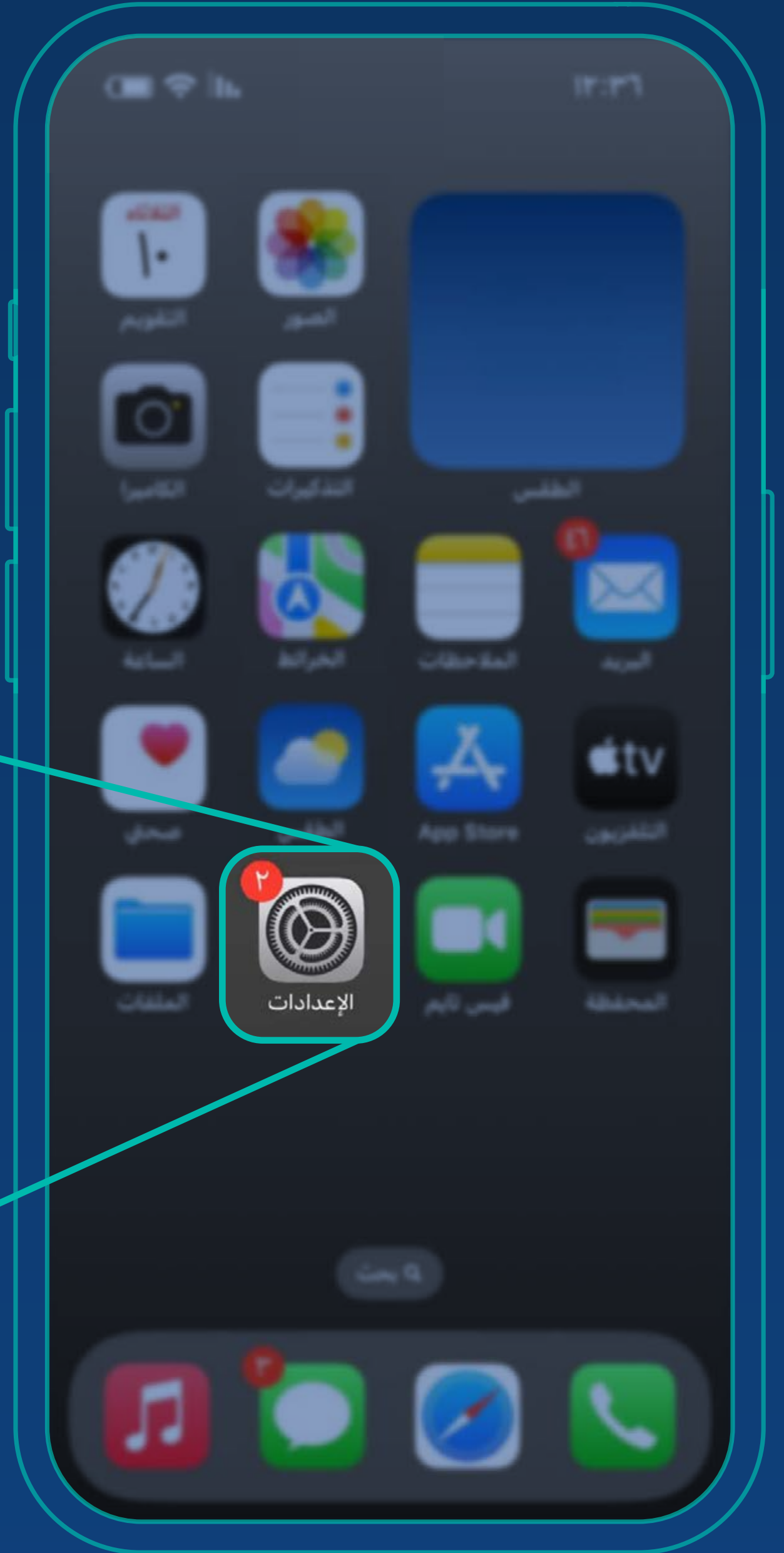
2 الحماية من الوصول غير المصرح به.



3 حماية البيانات الحساسة.

تعيين رمز الدخول

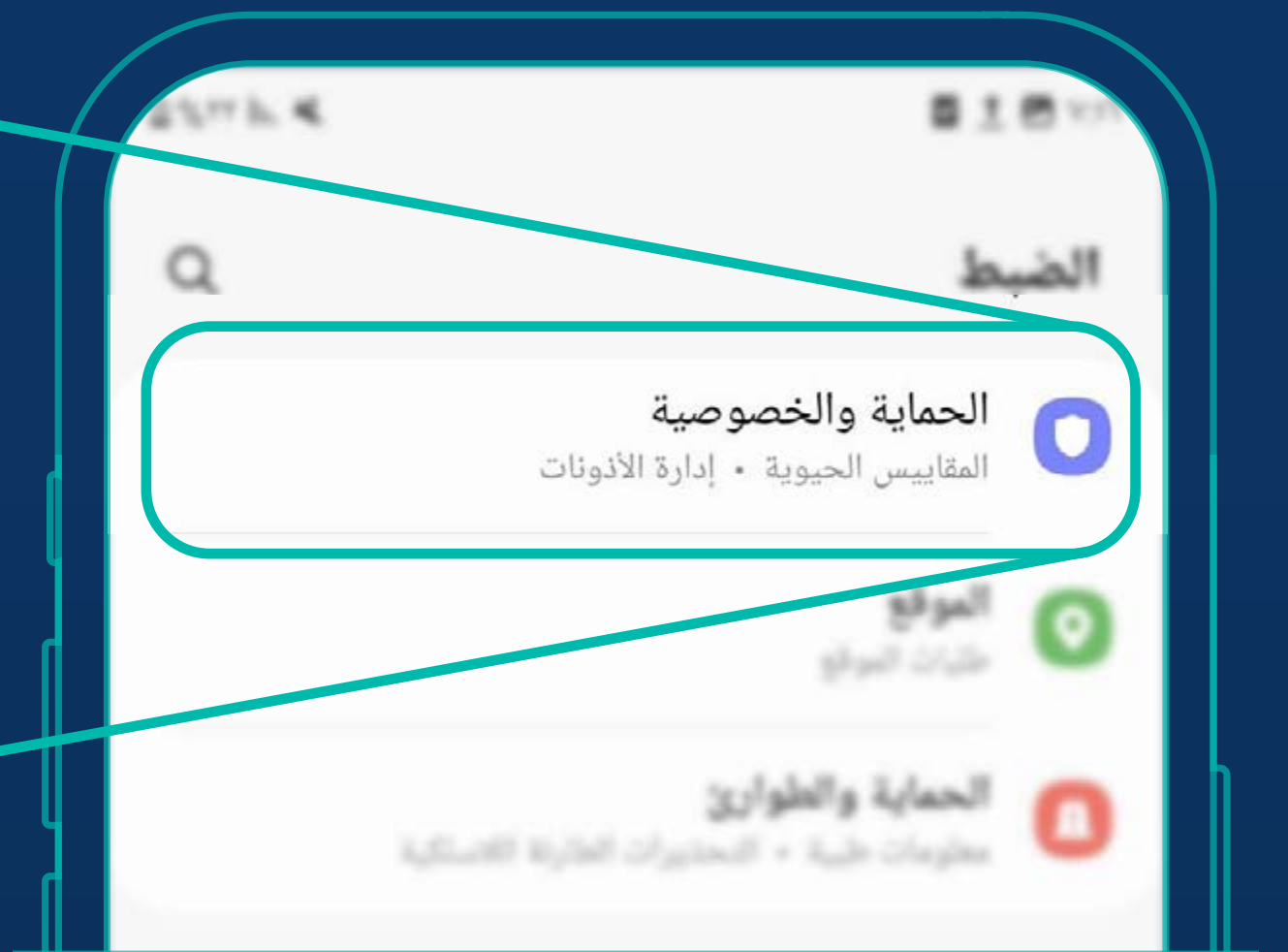
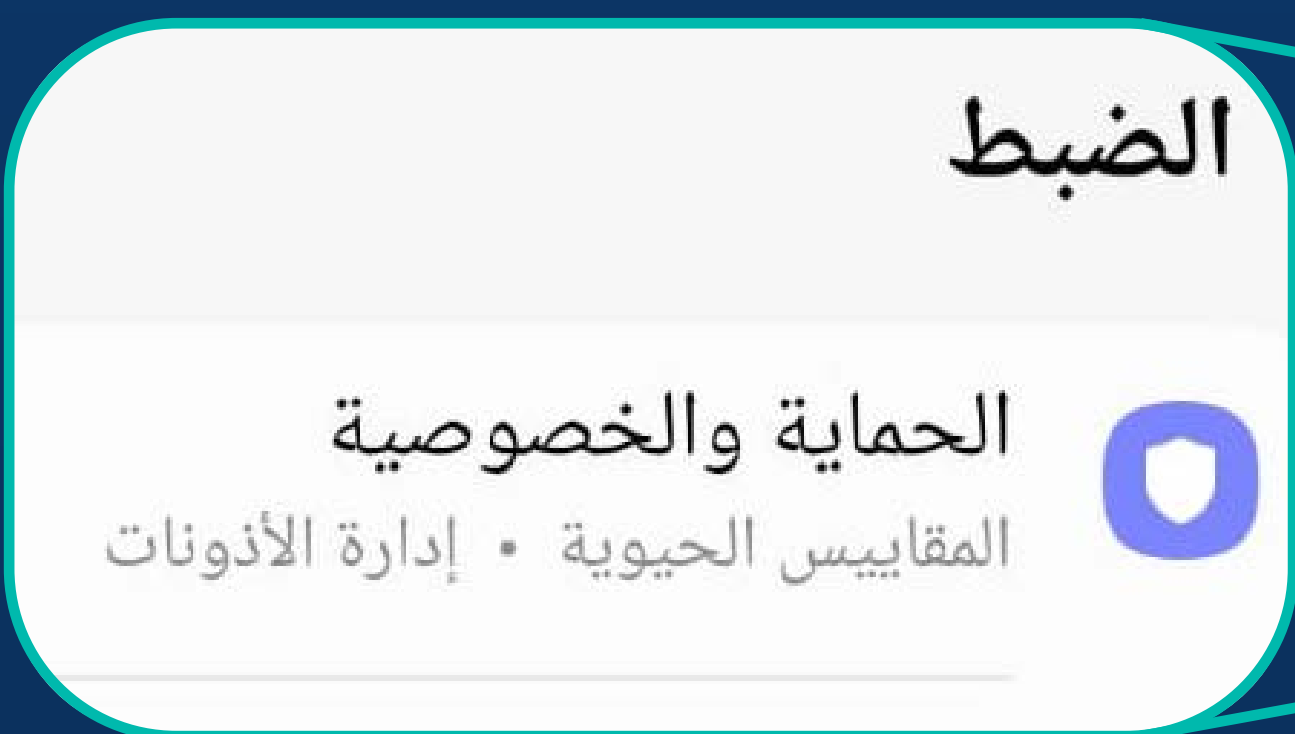
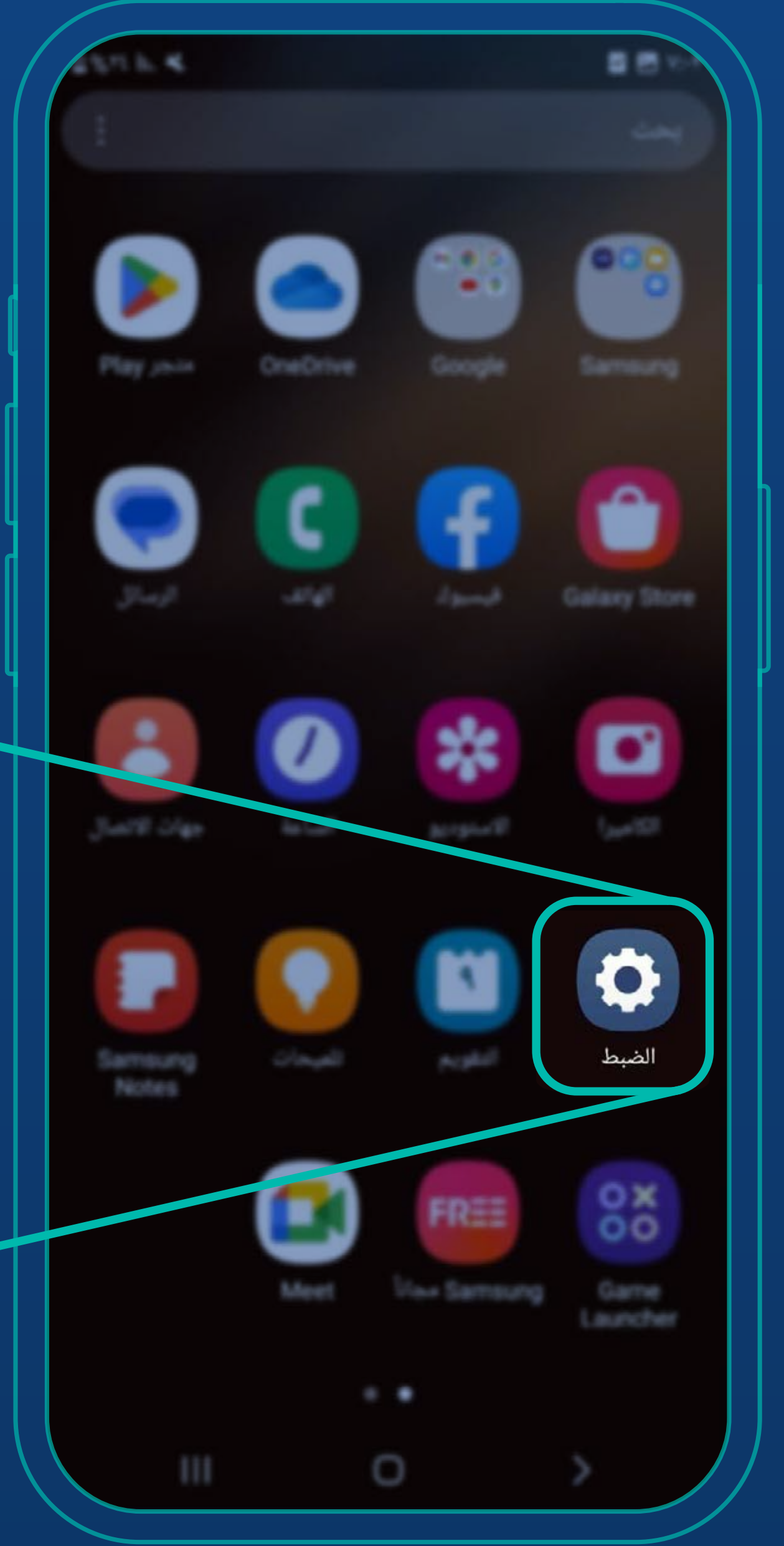
وإعداد السمات الحيوية



تعيين رمز الدخول

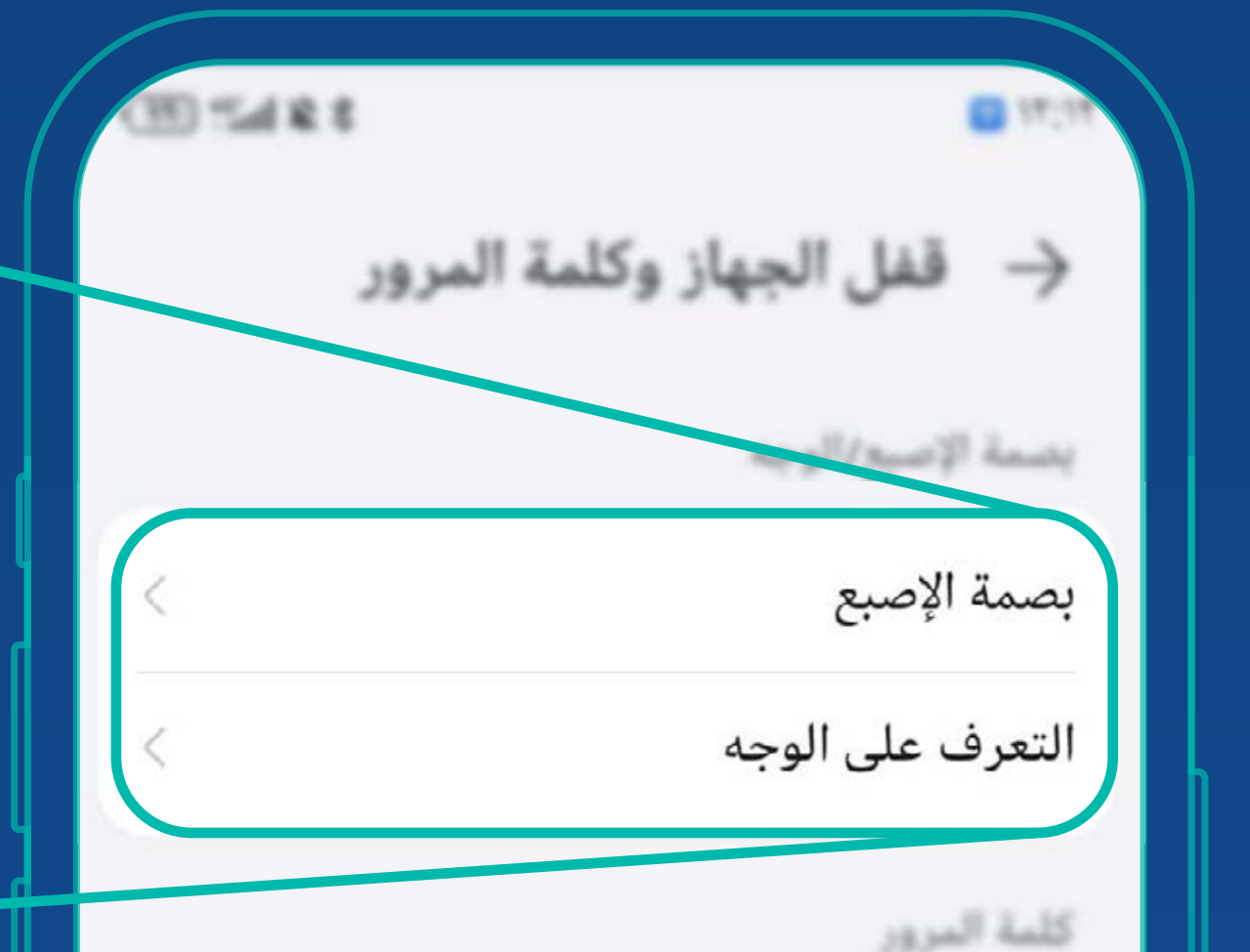
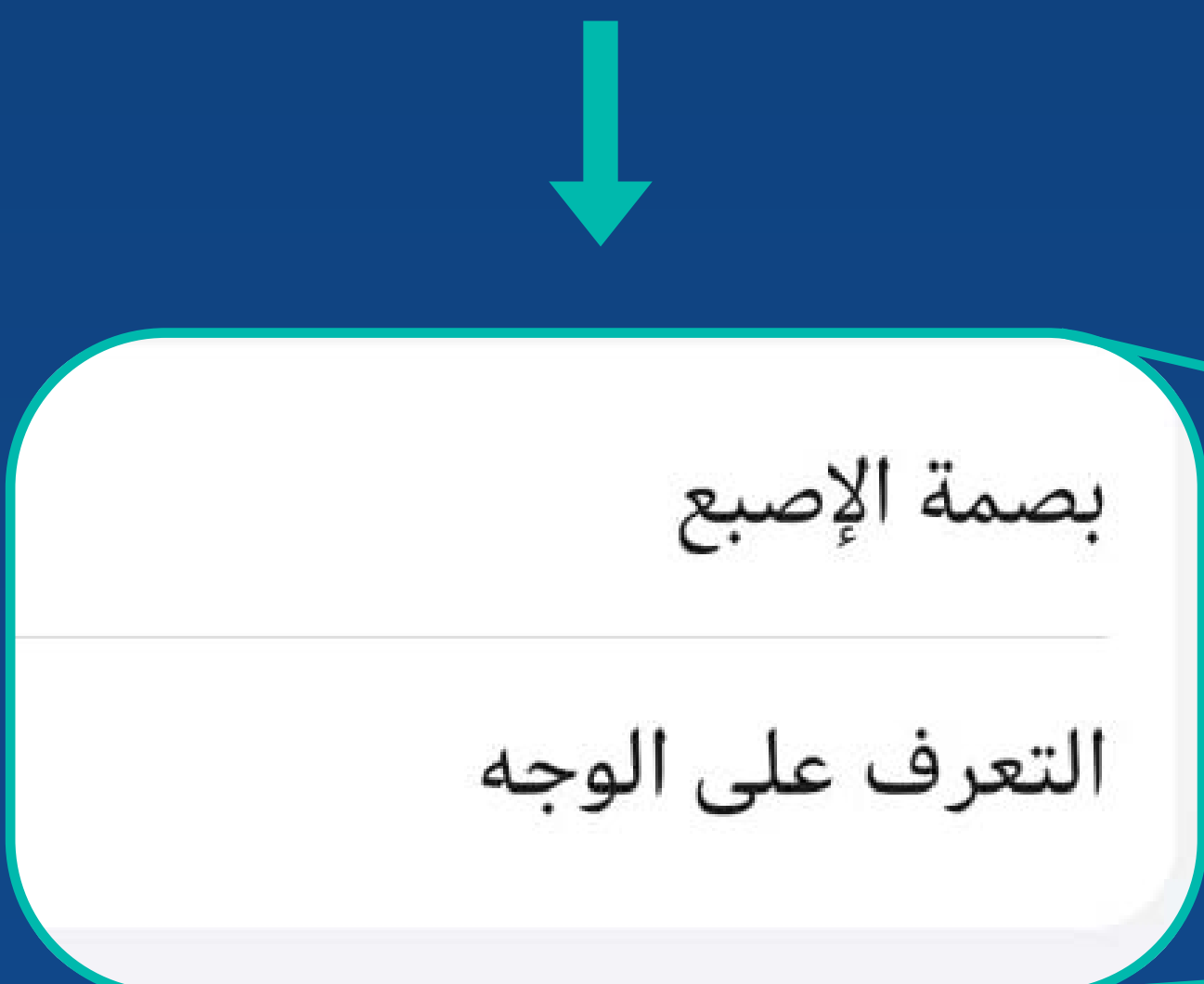
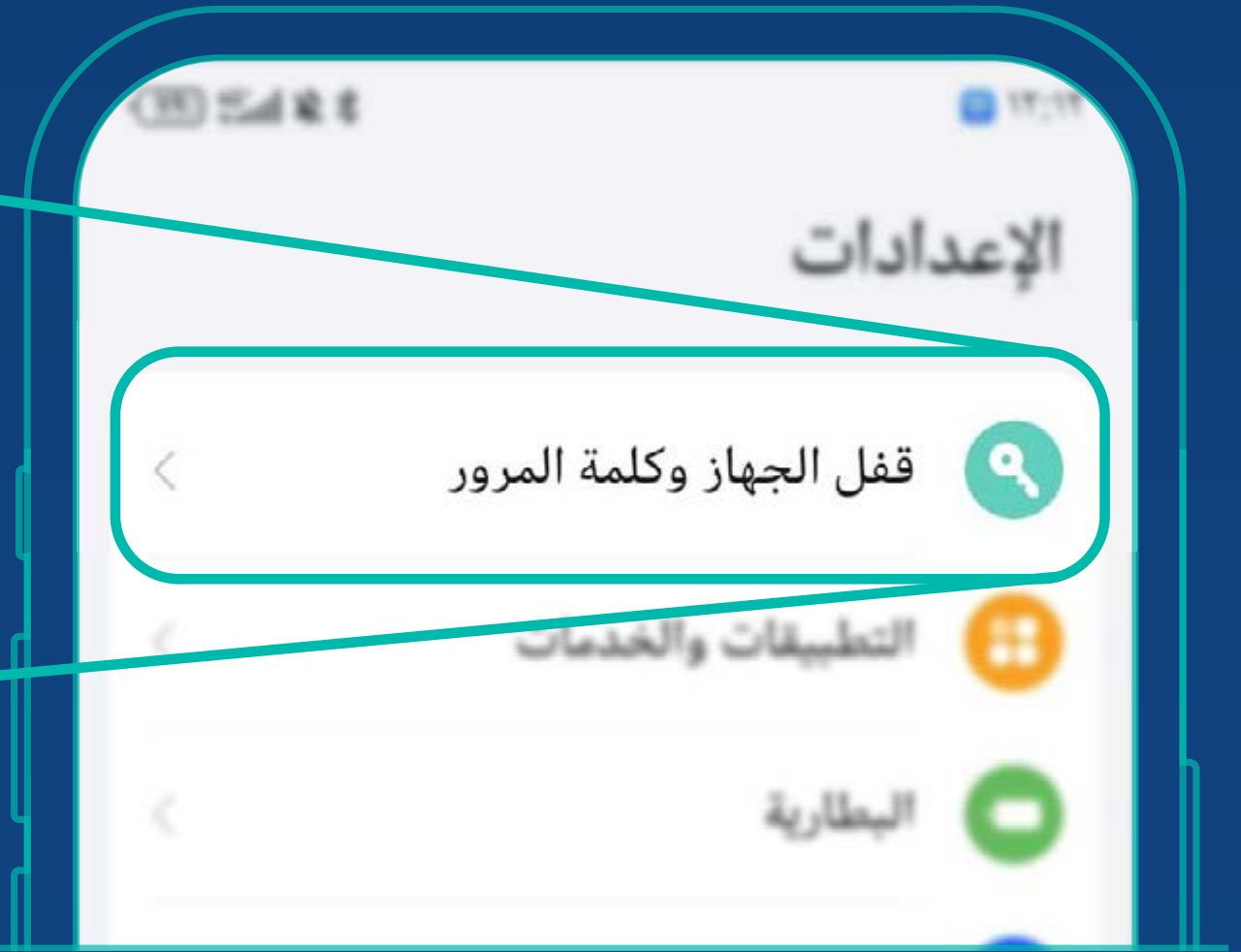
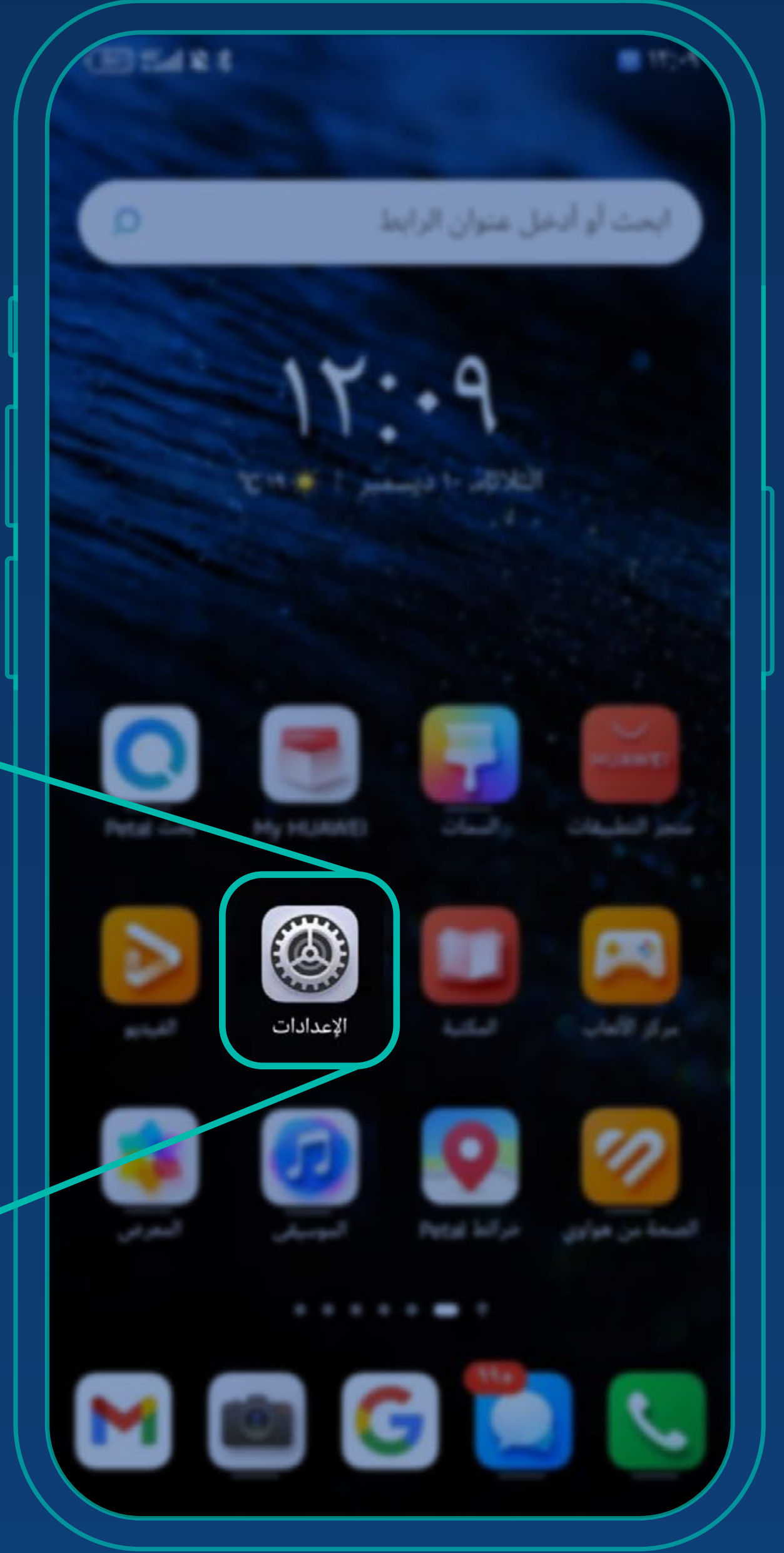
وإعداد السمات الحيوية

Android



تعيين رمز الدخول

وإعداد السمات الحيوية



التصفّح الآمن لشبكة الإنترنت

تصفّح شبكة الإنترنت

قد يعرّضك لعدد من المخاطر السيبرانية.. منها:

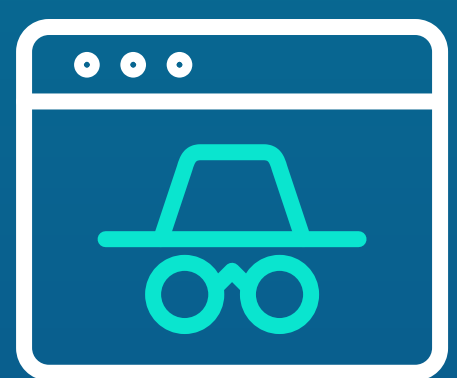
إصابة الجهاز بالبرمجيات الضارة.



سرقة البيانات الشخصية
والحساسة مثل اسم المستخدم
وكلمة المرور.



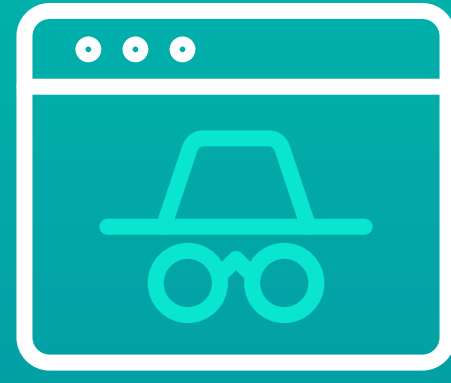
التعامل مع المواقع المزيفة.



تجنّب التجاوب مع الروابط أو
الرسائل مجهولة المصدر.



التصفّح الآمن لشبكة الإنترنت



يعمل المهاجمون على إنشاء المواقع المزيفة لتحقيق عدد من الغايات..منها:

- سرقة بيانات الدخول للحسابات.
- جمع أكبر قدر ممكن من البيانات.
- القيام بعدد من أعمال التصيد والاحتيال.

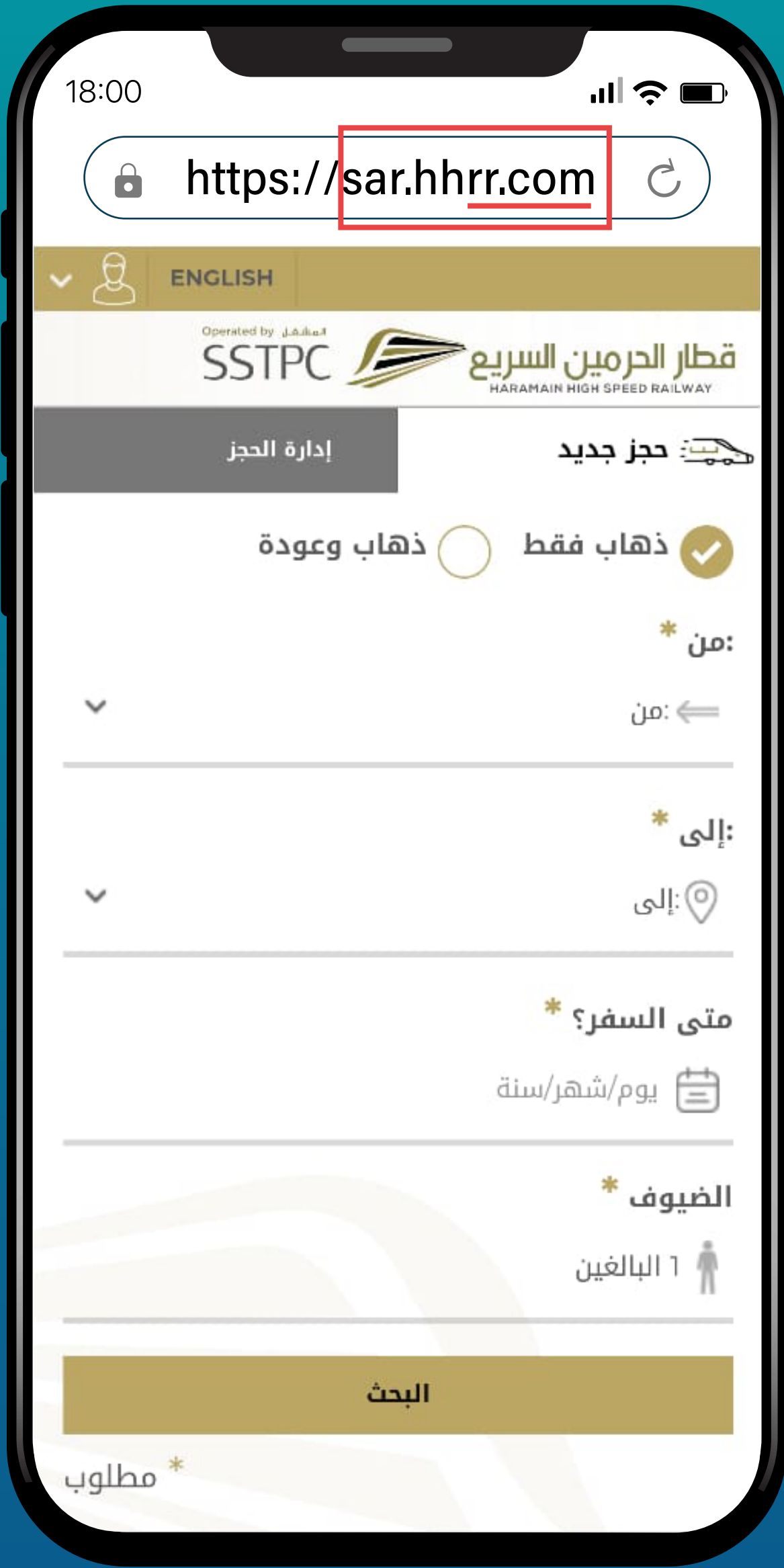
قد تكون المواقع المزيفة مطابقة في مظهرها للمواقع الحقيقية، لذلك احرص على التأكد من صحة الرابط الخاص بالموقع الذي ترغب بزيارته.



تذكّر



التصفح الآمن لشبكة الإنترنت



الموقع المزيف



الموقع الأصلي

يمكن الوصول لموقع قطار الحرمين
من خلال كتابة الرابط التالي:



<https://sar.hhr.sa>



التصفح الآمن لشبكة الإنترنت

لتصفح آمن لشبكة الإنترنت.. احرص على:



1 تحديث المتصفح بشكل مستمر.



2 مراجعة إعدادات الأمان والخصوصية الخاصة بالمتصفح.



3 الابتعاد عن زيارة المواقع المشبوهة وغير الموثوقة.



أمن التطبيقات

للإسهام في تأمين التطبيقات والحد من المخاطر السيبرانية التي قد تنتج عند تحميلها أو استخدامها.. احرص على:



تقنين

الصلاحيات الممنوحة للتطبيقات إلى الحد الأدنى.



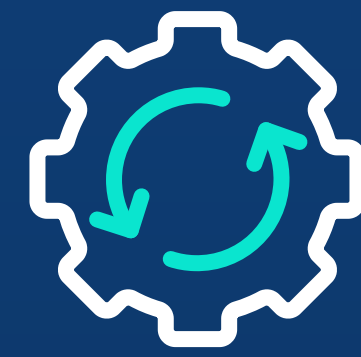
تحميل

التطبيقات من المصادر المعروفة.



تجنب

تثبيت التطبيقات من خارج المتاجر الخاصة بالأجهزة.



تفعيل

خاصية التحديث التلقائي لكافة التطبيقات.

استخدم المواقع والتطبيقات الموثوقة فقط.



أمن التطبيقات



حمّل التطبيقات
من المتاجر الخاصة بالأجهزة



وعند الرغبة بتحميل أحد التطبيقات..
احرص على:

التحقق من موثوقية مطور التطبيق.



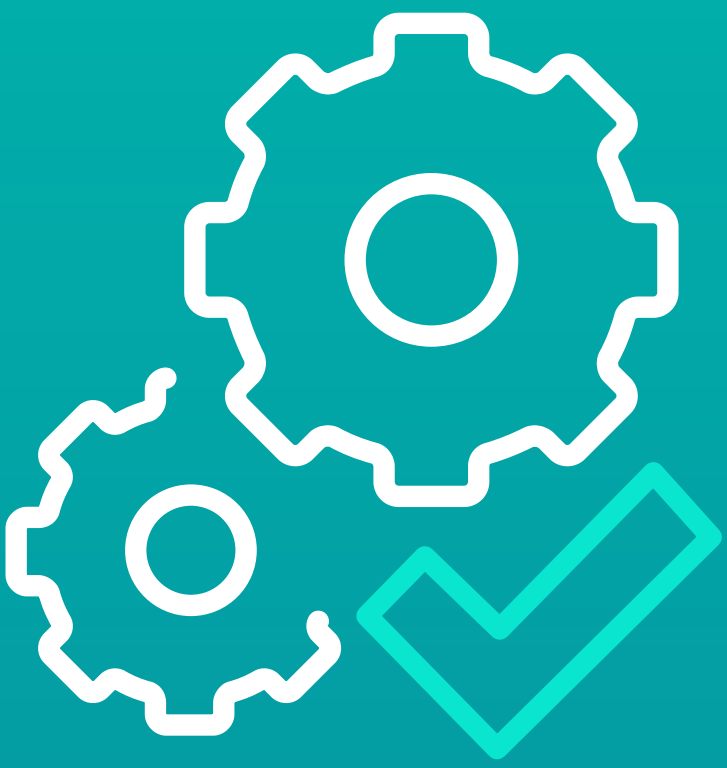
الاطلاع على تقييم التطبيق
ومراجعات المستخدمين.



تثبيت التحديثات

للأجهزة والتطبيقات

تثبيت التحديثات.. إجراء استباقي يبقيك بأمان



تُعد التحديثات الأمنية إحدى الوسائل المستخدمة لإغلاق الثغرات التي تفتح مجالاً للمهاجمين.

وتثبيتها:

يمنع الاستغلال والاستخدام غير المشروع.



يرفع مستوى الأمان.



تذكّر، تحميل التحديثات من مصادرها الموثوقة فقط، وتجنب تحميلها من مصادر غير موثوقة.

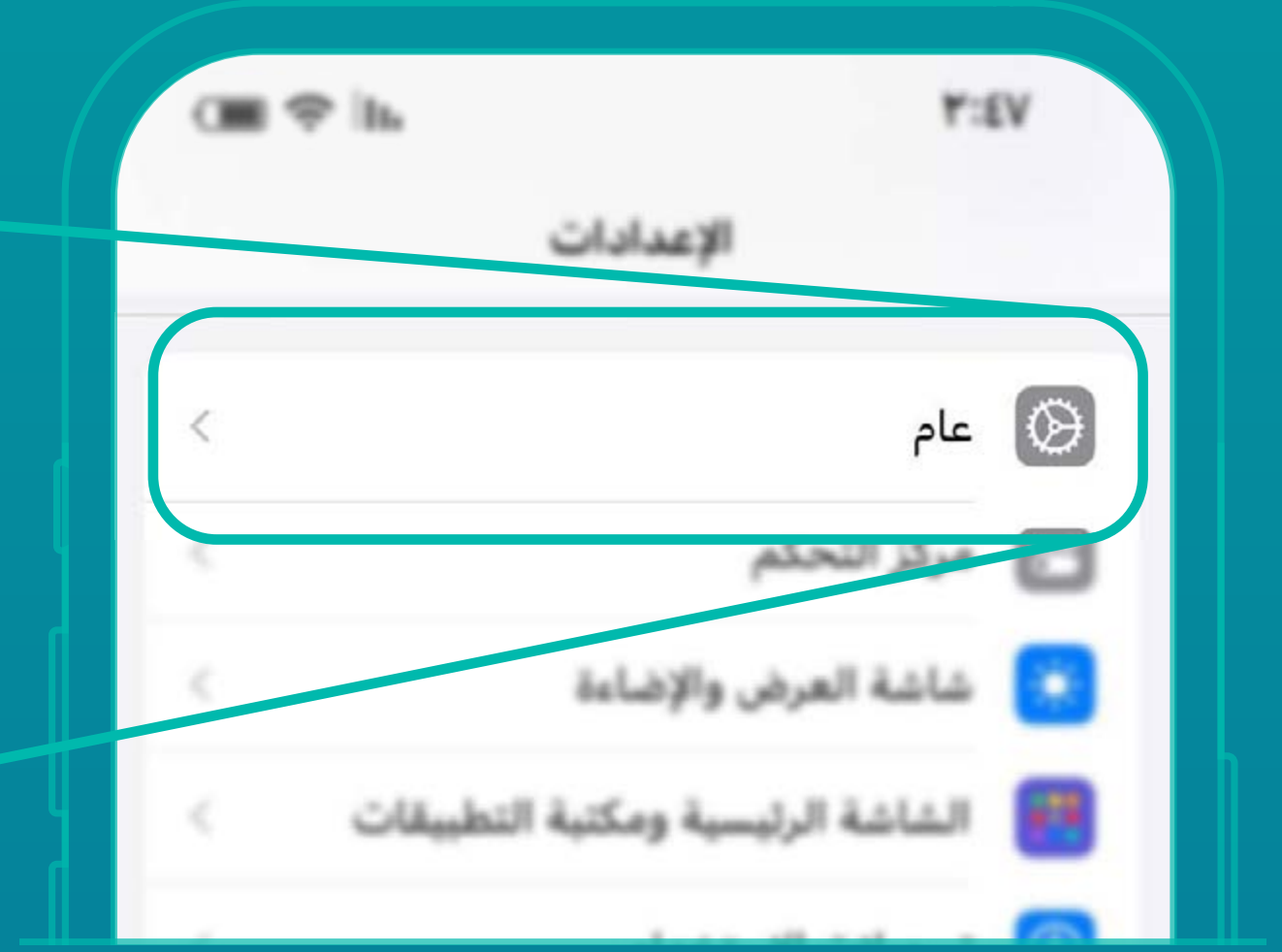
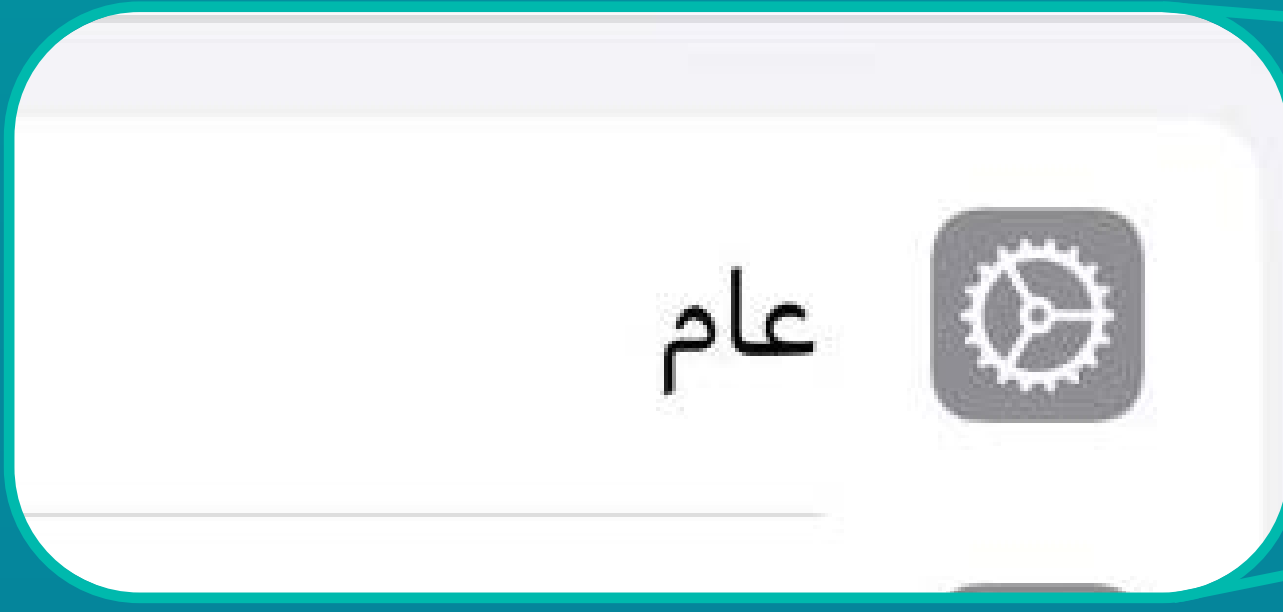
لتحقيق أقصى فائدة منها،

قم بتفعيل خاصية التحديث التلقائي لكي تضمن التثبيت المباشر للتحديثات عند ظهورها.



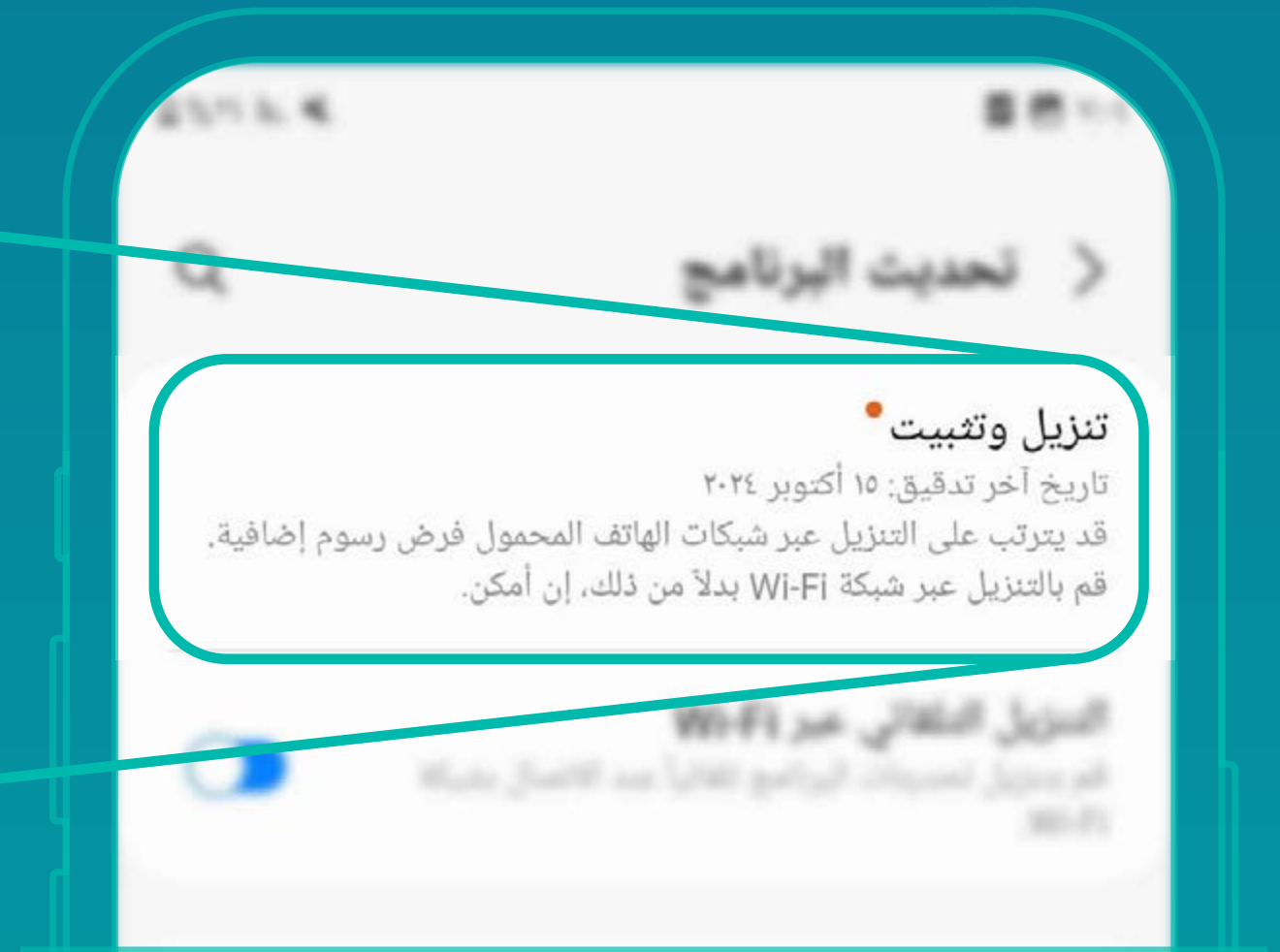
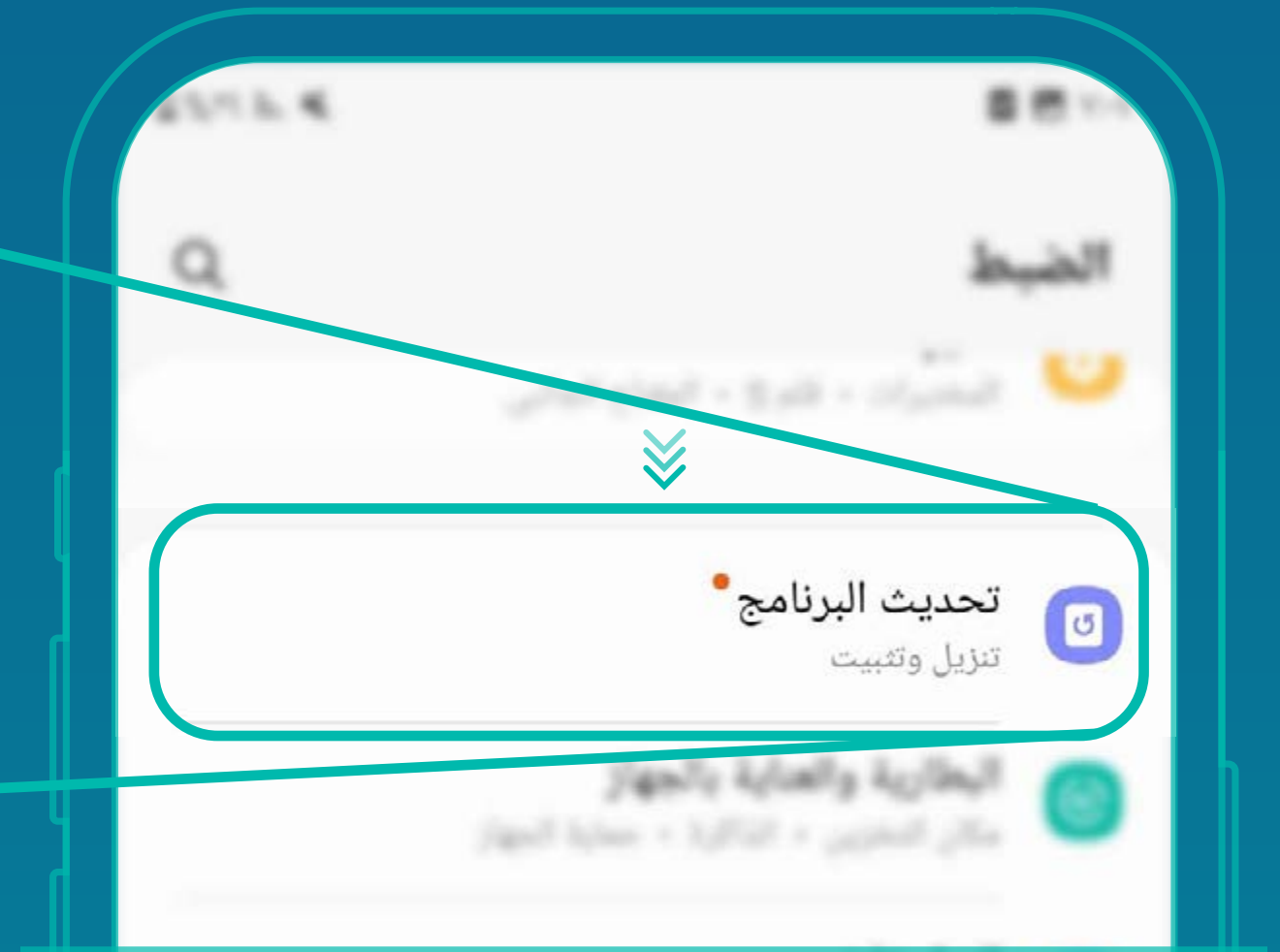
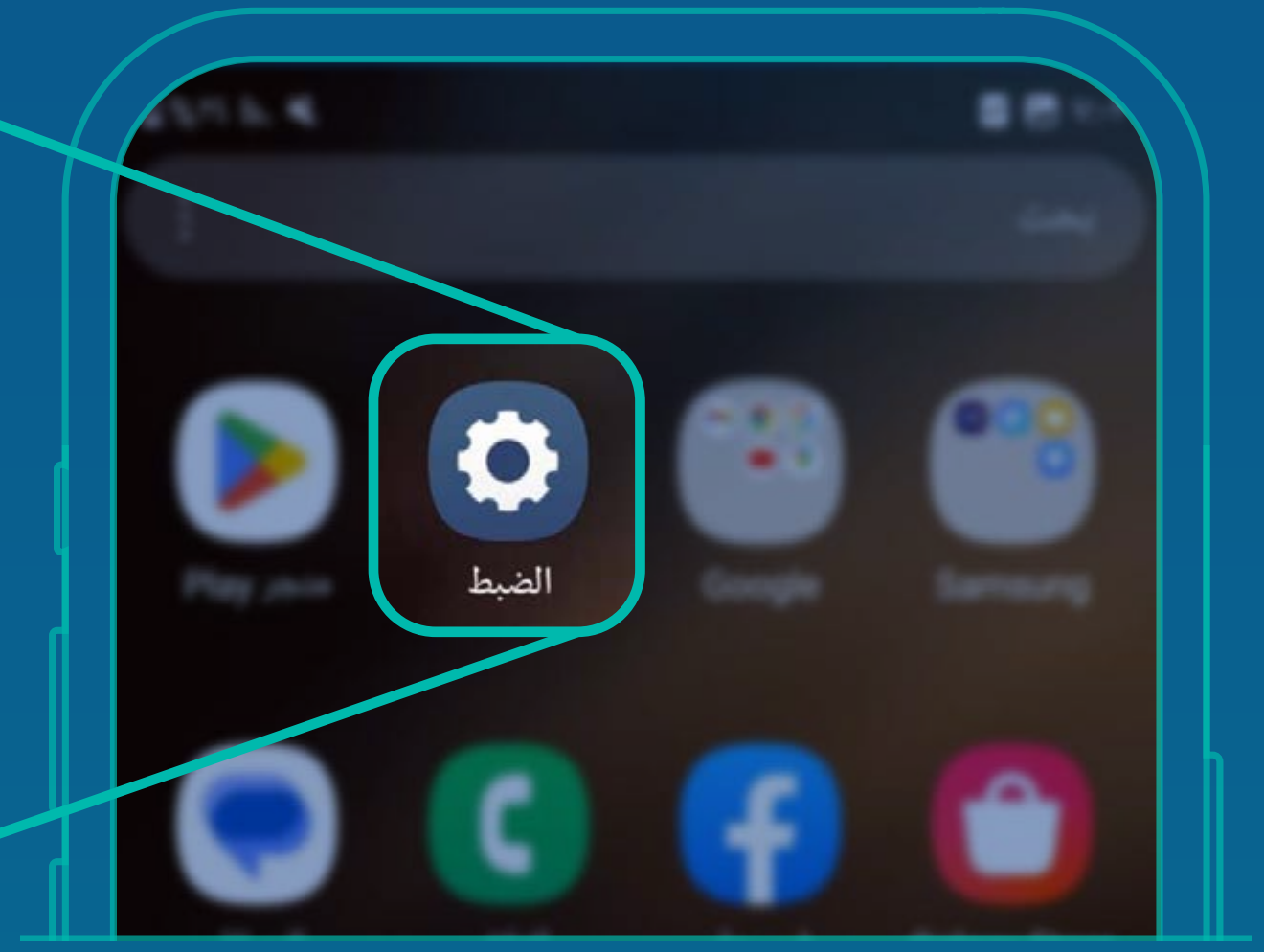
تثبيت التحديثات

لأجهزة iOS



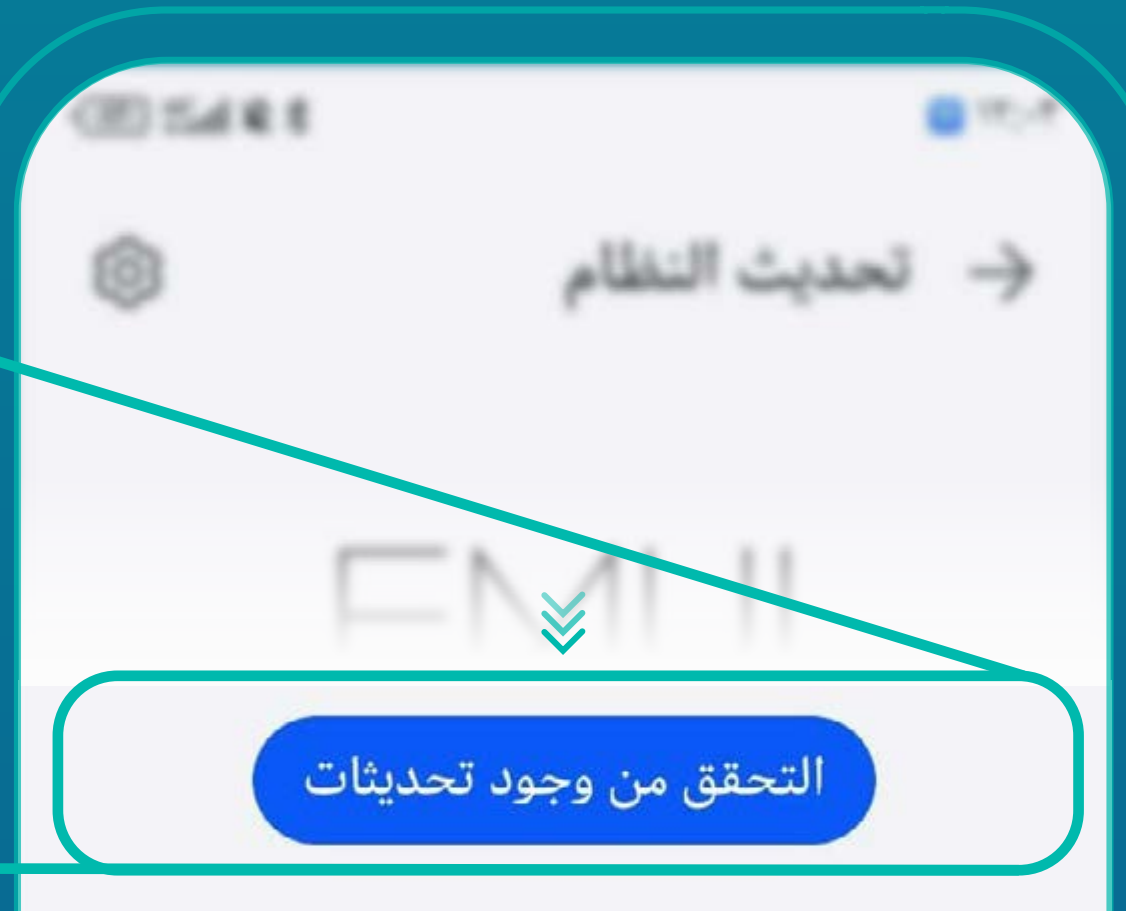
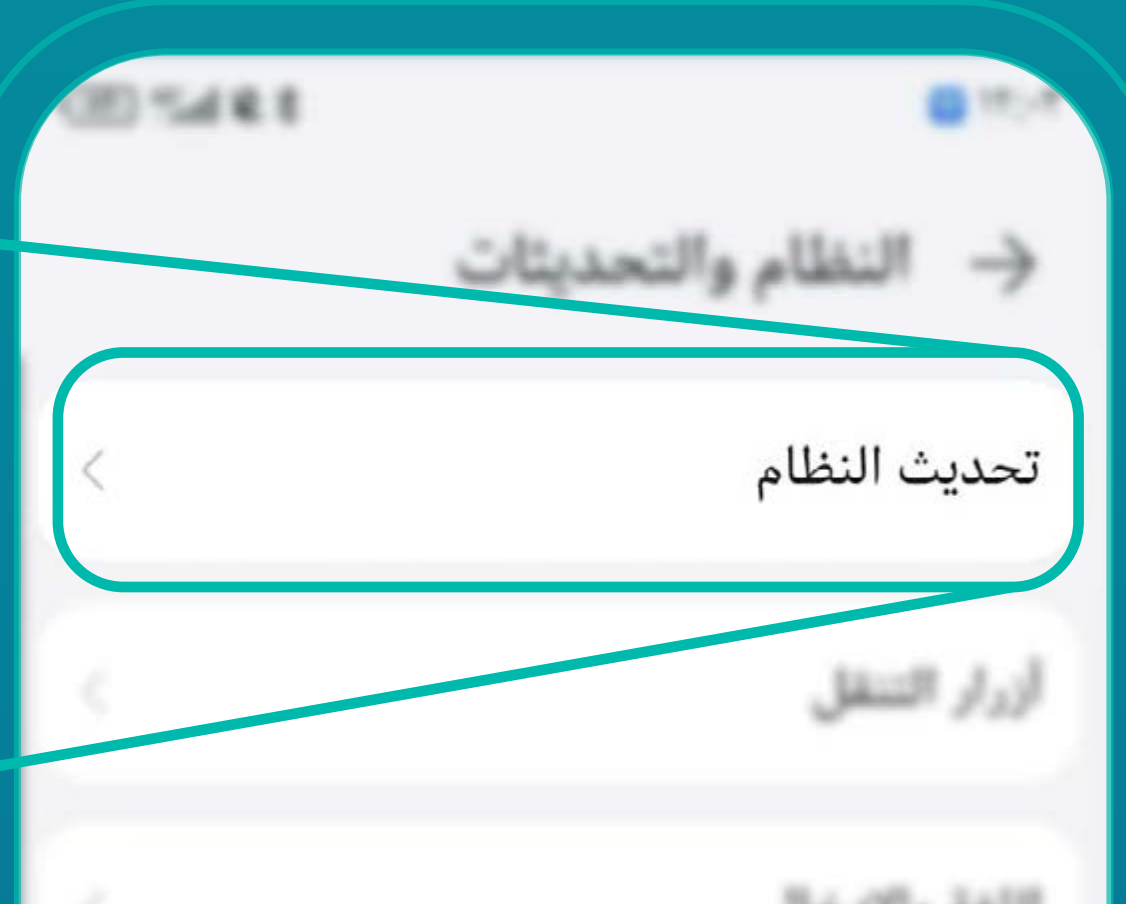
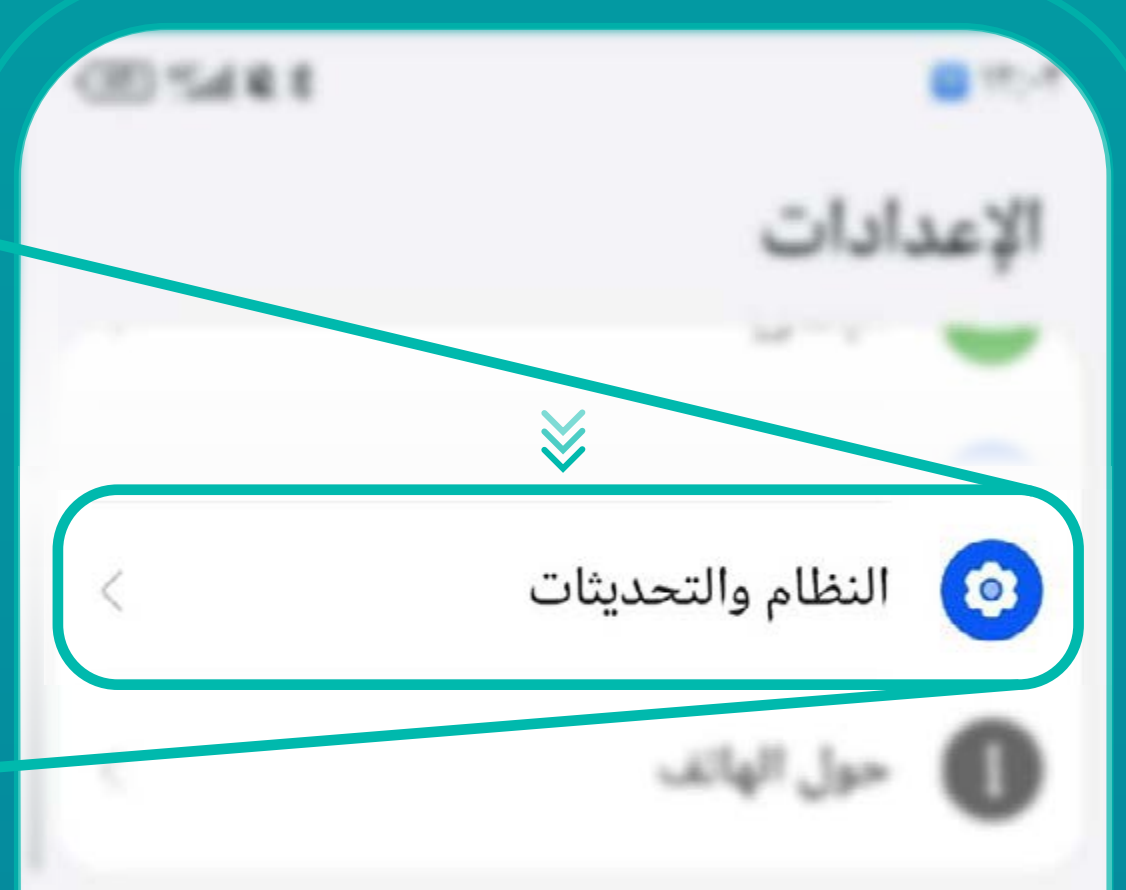
تثبيت التحديثات

لأجهزة Android



تثبيت التحديثات

لأجهزة Huawei



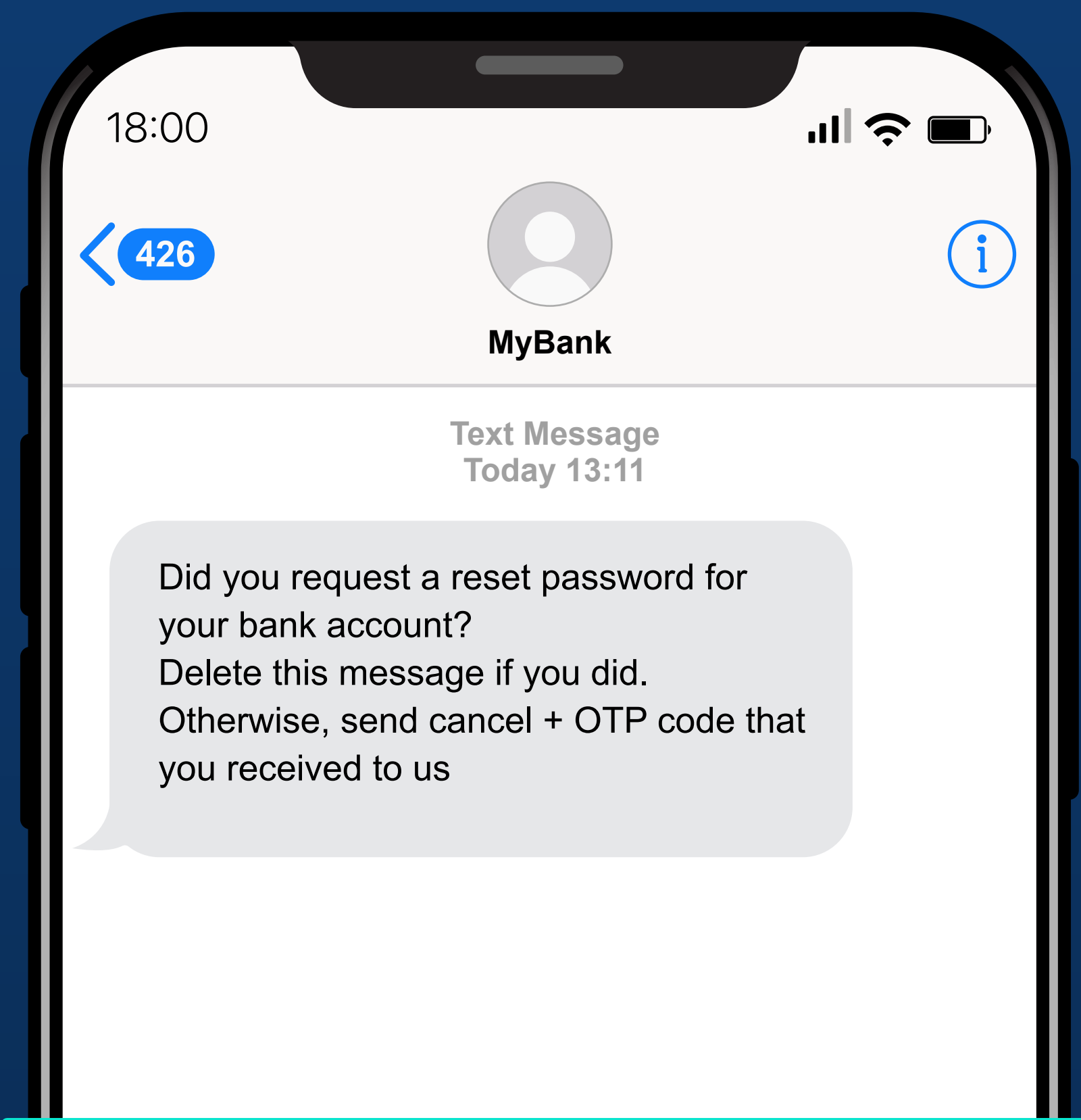
رمز الوصول لمرة واحدة

OTP

رمز الوصول لمرة واحدة يُستخدم لغرض التحقق من هوية المستخدم أو لإتمام عملية معينة عبر الإنترنت، ويحاول المهاجمون الحصول عليه للوصول غير المشروع للحسابات أو لإتمام عمليات عبر الإنترنت.

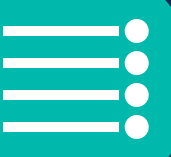
**وللتعامل الآمن مع رموز الوصول لمرة واحدة..
احرص على:**

- عدم مشاركة رمز الوصول لمرة واحدة.
- تجاهل الاتصالات أو الرسائل التي تطالبك بالإفصاح عن رمز الوصول لمرة واحدة.



تذكر

رمز الوصول لمرة
واحدة خاص بك
فقط، فلا تشاركه
مع الآخرين.



فقدان الهاتف

وأهمية عمل النسخ الاحتياطي

Backup

فقدان الهاتف المحمول قد يعرضك لعدد من المخاطر السيبرانية منها الوصول غير المشروع لجهازك وبياناتك وحساباتك.. لذلك احرص على:

- استعمال وسيلة للمصادقة على الهوية لمنع الوصول غير المشروع إلى الجهاز.
- تفعيل خاصية تحديد الموقع الجغرافي لمعرفة موقع الجهاز في حال تم فقدانه.
- التأكد من قدرتك على حذف البيانات المحفوظة على الجهاز عن بعد.

وتأكد من إجراء النسخ الاحتياطي بشكل دوري،

فهو يساعد على استعادة البيانات في حال فقدان الهاتف أو تعرضه للتلف.

تأكد من إجراء نسخ احتياطي لبياناتك المهمة.



مواقع وتطبيقات تهمك



اضغط على العنوان للوصول إلى الصفحة المطلوبة



Download on the
App Store



EXPLORE IT ON
AppGallery



GET IT ON
Google Play



GET IT ON
Google Play



Download on the
App Store



أرقام تهَمُّك

911

للحالات الطارئة والخدمات الأمنية

937

للاستشارات والاستفسارات الطبية

920002814

مركز اتصال وزارة الحج والعمرة
للإجابة عن استفسارات ضيوف الرحمن

1966

للاستفسارات الخاصة بالمسجد الحرام
والمسجد النبوي الشريف



يُمكنك الحصول على بقية الأدلة التوعوية من خلال زيارة موقع وزارة الحج والعمرة (من خلال الضغط هنا).

ستجد في هذه الأدلة جميع الإرشادات والتوجيهات التي تُيسِّر لك أداء المناسك بكل سهولة واطمئنان..



شركاؤنا في النجاح

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority



الشريك الاستراتيجي

أوقاف

الهيئة العامة للأوقاف
GENERAL AUTHORITY FOR AWQAF



تَقْبِلُ اللهُ أَعْمَالَكُمْ وَسَعْيَكُمْ وَدَمْتُمْ آمِنِينَ

للمزيد من المعلومات
التوعوية
تابعونا على حسابنا
في تويتر



Haj.gov.sa | [@HajMinistry](https://twitter.com/HajMinistry)

وزارة الحج والعمرة
MINISTRY OF HAJJ AND UMRAH

