1.2 ARB عربي

دليل

التوعية السيرانية

لضيوف الرحمن

الشريك الاستراتيجي

أوقاف
الهيئة العامة للأوقاف
GENERAL AUTHORITY FOR AWQAF

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	اُرْدُوْ URD
Español SPN	Русский язык RUS
Bahasa Malaysia MAY	සිංහල භාෂාව SIN
አማርኛ AMH	فارسی PER
o'zbek UZB	हिंदी HIN

محتوى دليل التوعية السيبرانية

اضغط على العنوان للوصول إلى الصفحة المطلوبة

أمـن التطبيقـات

تثبيت التحديثات للأجهزة

رمـز الوصـول لمـرة واحدة OTP

فقــدان الهـاتـــف وأهـميـــة عـمـــل النسـخ الاحتيـاطي

مواقـع وتطبيقات تـهمّـك

أرقـام تهمّك

أهمية الوعي بالأمن السيبراني في موسم الحج والعمرة

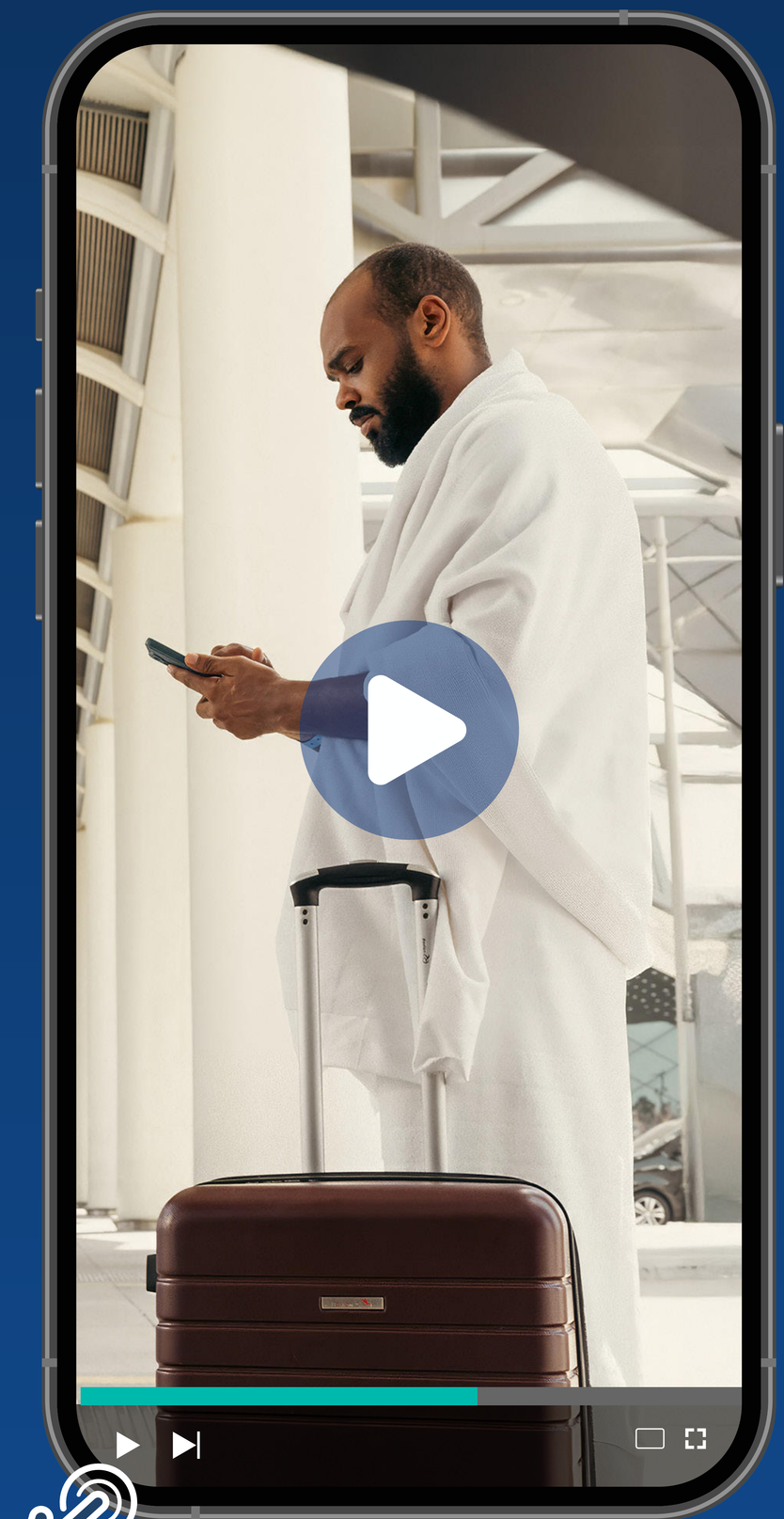
يستخدم المهاجمون حيل متجددة لشن الهجمات السيبرانية

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 خطوط الدفاع للحد من المخاطر السيبرانية المتجددة التي يشهدها الفضاء السيبراني.

يُعدّ الوعي السيبراني من أوائل خطوط الدفاع للحد من التهديدات المتجددة في الفضاء السيبراني



اضغط للوصول إلى الفيديو

أساليب الهندسة الاجتماعية والتصيد وكيفية تجنبها

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

لدفعهم على الإفصاح عن معلومات حساسة أو لحثّهم على القيام بإجراءات خاطئة تعرّض أمنهم السيبراني للخطر.

ومن الأساليب التي قد يستخدمها المهاجم لشنّ 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

يعتبر 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 التصيّد:

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.

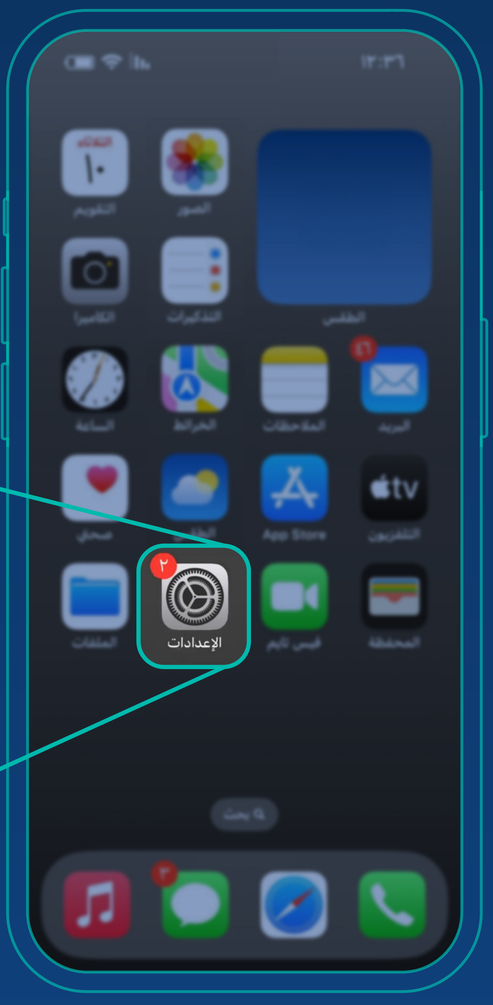
تعيين رمز الدخول وإعداد السمات الحيوية

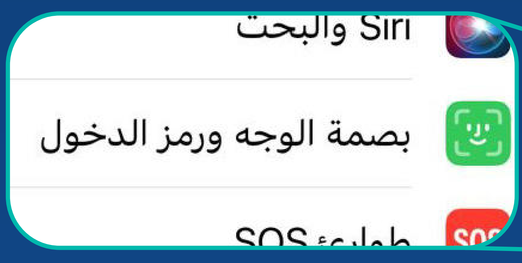
يُعد أمراً بالغ الأهمية ويُسهم في:

1. التحقق من هوية المستخدم.
2. الحماية من الوصول غير المصرح به.
3. حماية البيانات الحساسة.

تعيين رمز الدخول
وإعداد السمات الحيوية

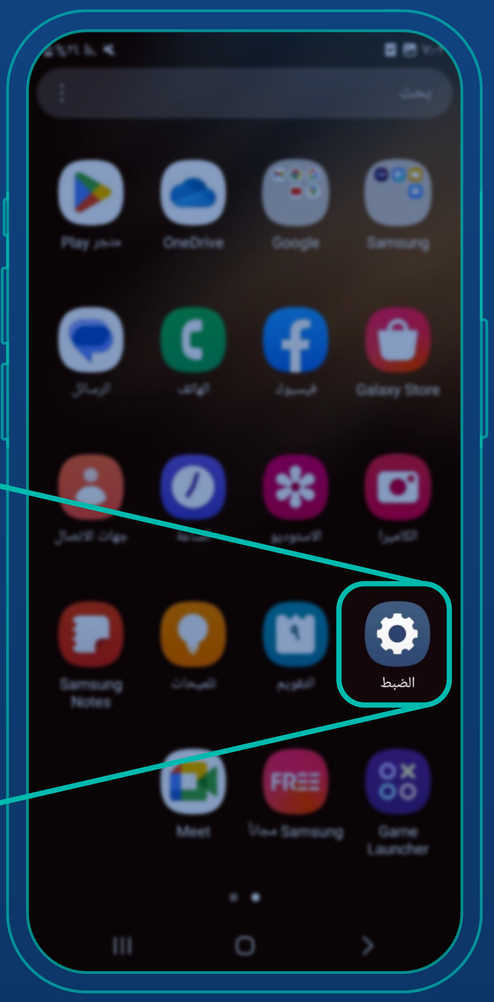
iOS

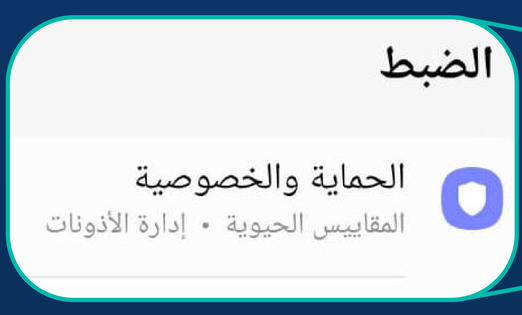


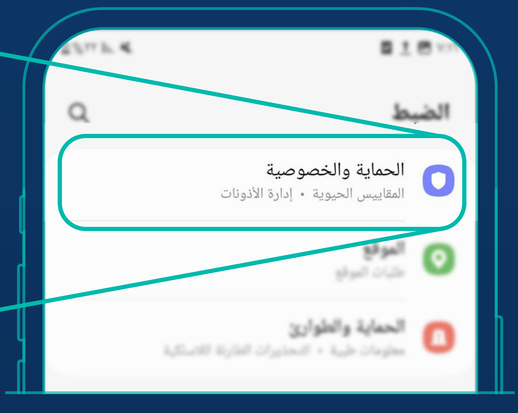


تعيين رمز الدخول
وإعداد السمات الحيوية

Android

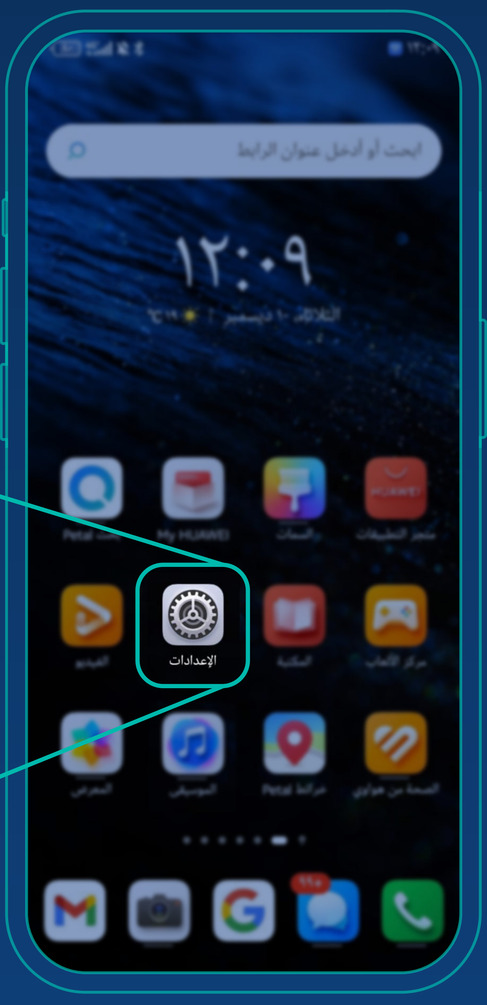


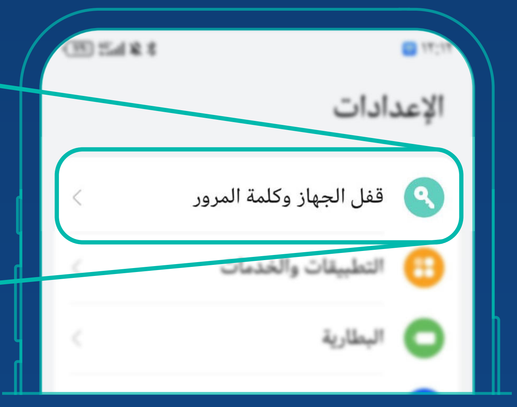


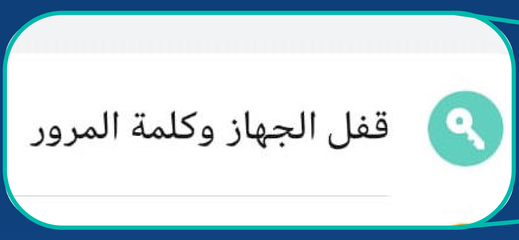


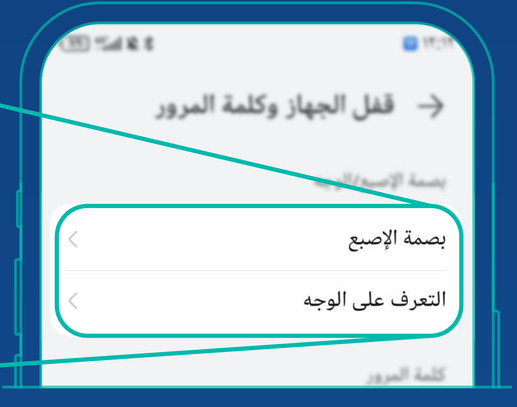
تعيين رمز الدخول
وإعداد السمات الحيوية

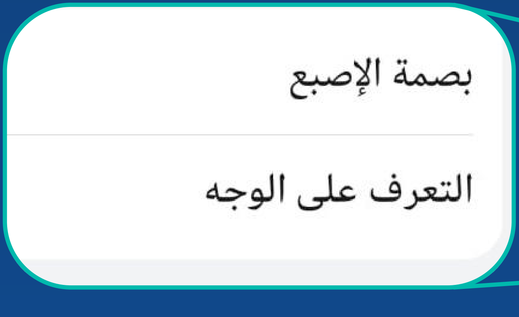
HUAWEI











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

يعمـل المهاجمون على إنشـاء المواقع المزيّفة لتحقيق عدد من الغايات..منها:

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

تذكّـر

قد تكـون المواقـع المزيفة مطابقة في مظهرها للمواقع الحقيقية، لذلك احـرص علـى التـأكد مـن صحّـة الرابـط الخـاص بالموقع الذي ترغب بزيارته.

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

لتصفّح آمن لشبكة الإنترنت.. احرص على:

1. تحديث المتصفح بشكل مستمر.

2. مراجعة إعدادات الأمان والخصوصية الخاصة بالمتصفّح.

3. الابتعاد عن زيارة المواقع المشبوهة وغير الموثوقة.

أمن التطبيقات

للإسـهام فـي تأميـن التطبيقـات والحد من المخاطر السيبرانية التي قد تنتج عند تحميلها أو استخدامها.. احرص على:

تحميل
التطبيقات من المصادر المعروفة.

تقنين
الصلاحيات الممنوحة للتطبيقات إلى الحد الأدنى.

تفعيل
خاصية التحديث التلقائي لكافة التطبيقات.

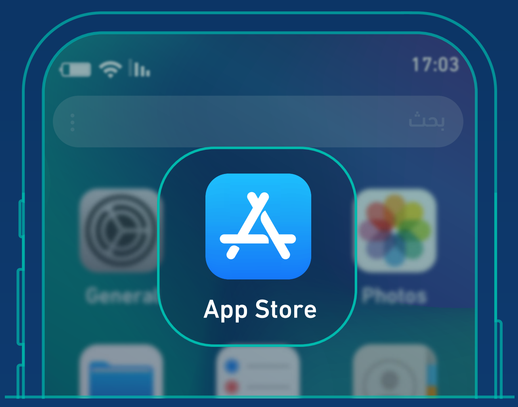
تجنّب
تثبيت التطبيقات من خارج المتاجر الخاصة بالأجهزة.

استخدم المواقع والتطبيقات الموثوقة فقط.

أمن التطبيقات

حمّـــل التطبيقـــات

من المتاجر الخاصة بالأجهـزة

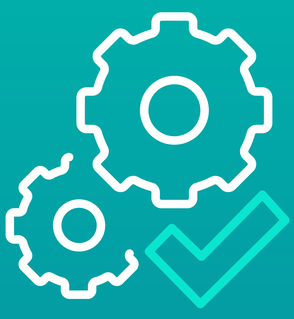


وعنـد الرغبة بتحميـل أحـد التطبيقات.. احرص على:

- التحقق من موثوقية مطور التطبيق.
- الاطـلاع علـى تقييـم التطبيـق 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.

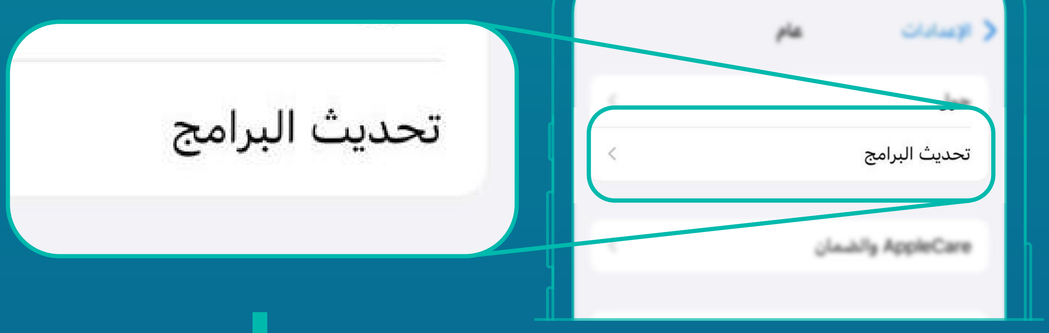
يرفع مستوى الأمان.

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

لتحقيق أقصى فائدة منها،
قم بتفعيل خاصيّة التحديث التلقائي لكي تضمن التثبيت المباشر للتحديثات عند ظهورها.

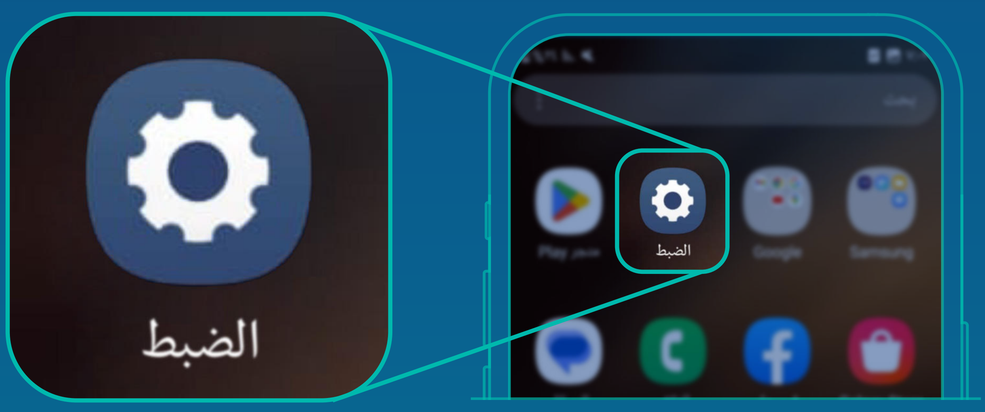
تثبيـت التحديثـات

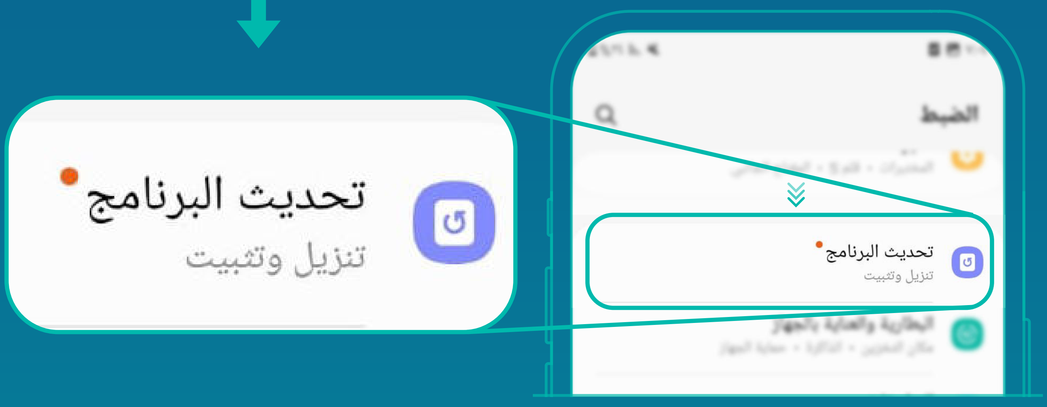
لأجهـزة iOS



تثبيـت التحديثـات

لأجهـزة Android



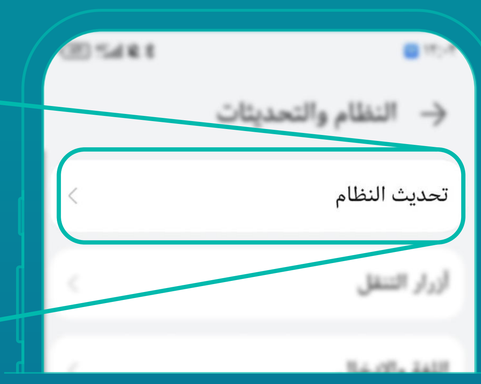


تثبيـت التحديثـات

لأجهـزة Huawei

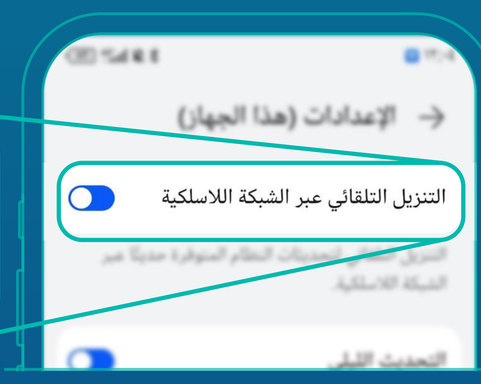
النظام والتحديثات

تحديث النظام



التحقق من وجود تحديثات

التنزيل التلقائي عبر الشبكة اللاسلكية



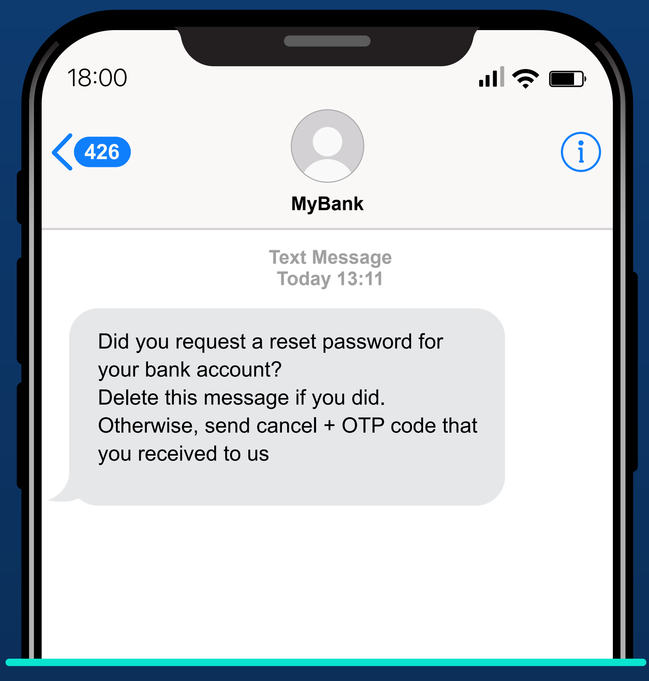
رمز الوصول لمرة واحدة

OTP

رمز الوصول لمرة واحدة يُستخدم لغرض التحقّق 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.



تذكّر

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

فقدان الهاتف

وأهمية عمل النسخ الاحتياطي Backup

فقـدان الهاتـف المحمول قد يعرضـك لعدد من المخاطر السـيبرانية منها الوصول غير المشروع لجهازك وبياناتك وحساباتك.. لذلك احرص على:

- اسـتعمال وسـيلة للمصادقة على الهوية لمنع الوصول غير المشروع إلى الجهاز.
- تفعيـل خاصية تحديـد الموقـع الجغرافي لمعرفة موقع الجهاز في حال تم فقدانه.
- التأكـد مـن قدرتـك علـى حـذف 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.

تأكّد مـن إجـراء نسخ احتيـاطي لبياناتك المهمة.

مواقع وتطبيقات تهمّك

اضغط على العنوان للوصول إلى الصفحة المطلوبة

نُسُك

Download on the App Store

WWW

EXPLORE IT ON AppGallery

GET IT ON Google Play

قطار الحرمين السريع
HARAMAIN HIGH SPEED RAILWAY

GET IT ON Google Play

Download on the App Store

WWW

أرقام تهمّك

911

للحالات الطارئة والخدمات الأمنية

937

للاستشارات والاستفسارات الطبية

92002814

مركز اتصال وزارة الحج والعمرة
للإجابة عن استفسارات ضيوف الرحمن

1966

للاستفسارات الخاصة بالمسجد الحرام
والمسجد النبوي الشريف

بإمكانك 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

تـــقبّل الله
أعمالكم وسعيكم
ودمتم آمنين

للمزيد من المعلومات
التوعوية
تابعونا على حسابنا
في تويتر

Haj.gov.sa | @HajMinistry

وزارة الحـج والـعمـرة
MINISTRY OF HAJJ AND UMRAH