FORGEMARK LABS

الأمن الرقمي للناس

دليل الأمان الرقمي للعائلة

دليل مجاني وعملي لكل بيت: الهاتف،
وواتساب، والبريد، والبنك، والواي فاي.

Forgemark Labs — مجاني

forgemarklabs.com

أُعدّ نص هذا الدرس بمساعدة أدوات الذكاء الاصطناعي، وراجعه وتحقق من معلوماته فريق Forgemark Labs، وهو المسؤول عن محتواه. الغلاف بأشكال العلامة فقط. المحتوى للتوعية العامة، وليس نصيحة قانونية أو مالية أو مهنية.

قبل أن تبدأ: اطمئن

أغلب ما يحدث للناس العاديين ليس «اختراقًا عبقريًا»، بل حيلة بسيطة تعتمد على الاستعجال والثقة. والخبر الجيد أن خمس عادات صغيرة تمنع معظم هذه الحيل.

لن تحتاج إلى برامج غالية ولا إلى خبرة تقنية. كل ما في هذا الدليل مجاني، ويمكن تنفيذه في جلسة واحدة لا تتجاوز ساعة للعائلة كلها.

طريقة الاستعمال: اقرأ القسم، ثم نفّذ خطوته فورًا، ثم ضع علامة في قائمة التحقق في آخر الدليل.

المصادر: الخطوات الأساسية نفسها توصي بها CISA في حملة Secure Our World [1] والمركز الوطني البريطاني للأمن السيبراني NCSC [2][3][4][5][6].

1. القاعدة الذهبية: الرموز لك وحدك

حين يصلك رمز من أرقام (مثل رمز تفعيل واتساب، أو رمز البنك، أو رمز الدخول إلى بريدك)، فهذا الرمز يعني: «صاحب هذا الهاتف موافق».

لا تعطِ أي رمز لأي شخص. لا لصديق، ولا لموظف، ولا لمن يقول إنه من «الدعم الفني».

- واتساب ينصح بعدم مشاركة رمز التسجيل ولا الرقم السري أو كلمة السر للتحقق بخطوتين مع أحد. [7]
- البنوك لا تطلب منك الرقم السري للبطاقة ولا رمز التحقق (OTP)، لا بالهاتف ولا على مواقع التواصل. (البنك المركزي المصري: حملة «معًا نكافح الاحتيال») [8] [9]
- إذا وصلك رمز لم تطلبه، فلا تعطه لأحد. [10]

جملة تحفظها العائلة: «من يطلب الرمز، فهو المحتال».

2. كلمات المرور: أقل حفظًا، وأمان أكثر

المشكلة

استعمال كلمة سر واحدة في كل مكان. إذا تسرّبت من موقع واحد، يمكن تجربتها على بريدك وحساباتك الأخرى. [2] [3]

الحل في ثلاث نقاط

1. **كلمة سر طويلة للبريد:** اجمع ثلاث كلمات عشوائية لا رابط بينها. [2] لا تستعمل تاريخ الميلاد ولا أسماء أفراد العائلة ولا أرقامًا متتالية. [2]
2. **كلمة مختلفة لكل حساب مهم:** البريد، والبنك، وواتساب (رقمه السري أو كلمة سره)، وفيسبوك وإنستغرام.

3. **مدير كلمات المرور:** خزنة مشفّرة تحفظ كلماتك وتملؤها عنك، فلا تحفظ إلا كلمة واحدة قوية. [3]
   - على Android وChrome: مدير كلمات مرور Google المدمج. [11]
   - على iPhone: تطبيق «كلمات السر» (Passwords) المدمج في iOS 18 وما بعده؛ وفي النسخ الأقدم من: الإعدادات ← كلمات السر. [12]

لماذا البريد أولًا؟

لأن «نسيت كلمة السر» في أغلب المواقع ترسل رابط الاستعادة إلى بريدك. من يملك بريدك يستطيع تغيير كلمات السر الأخرى. [13]

لا تكتب كلمات السر في ملاحظة على الهاتف ولا ترسلها في محادثة. إن كنت تفضّل الورق، فاحفظ الورقة في مكان آمن في البيت، لا في المحفظة. وبعض البنوك تمنع تدوين كلمة سرها، فراجع شروط بنكك. [2] [3]

3. التحقق بخطوتين: القفل الثاني

ما هو؟ بعد كلمة السر يطلب الحساب دليلًا ثانيًا: رمزًا يصل إلى هاتفك، أو ضغطة تأكيد، أو مفتاح مرور. [4] [14]

لماذا يهم؟ حتى لو عرف شخص كلمة سرك، يصعب عليه كثيرًا الدخول دون الخطوة الثانية. [1] [4]

أين تفعّله؟ (بالترتيب)

الحساب	المسار التقريبي	المصدر
بريد Gmail / حساب Google	من حساب Google، افتح «الأمان» (أو «الأمان وتسجيل الدخول»)، وابحث عن «التحقق بخطوتين»، ثم «تفعيل»	[14]
واتساب	الإعدادات ← الحساب ← التحقق بخطوتين ← تفعيل	[15]
حساب Apple	غالبًا مفعّل افتراضيًا؛ تأكّد من: الإعدادات ← اسمك، ثم ابحث عن قسم تسجيل الدخول والأمان	[16]
فيسبوك وإنستغرام	مركز الحسابات (أو «حساب Meta» في بعض الحسابات) ← كلمة السر والأمان ← المصادقة الثنائية	[17]

نصيحة: احفظ «الرموز الاحتياطية» التي يعطيك إياها الحساب في مكان آمن، لتدخل بها إذا ضاع هاتفك، ولا تعطها لأحد. [14]

نصيحة من Google: الرموز التي تصل برسالة SMS أضعف من غيرها أمام الهجمات على رقم الهاتف؛ فإن أمكن، استعمل تنبيه Google أو مفتاح المرور. [14]

مراجعة سريعة لحساب Google: صفحة «فحص الأمان» تعرض الأجهزة المتصلة وإعدادات الأمان في دقائق. [18]

4. واتساب: قفل الحساب في عشر دقائق

الحيل الشائعة (لتعرفها، لا لتخاف منها)

- **«أرسلتُ لك رمزًا بالخطأ»:** رسالة من حساب صديق قد يكون مسروقًا، تطلب رمزًا وصلك. [19] [7]
- **«معك فريق الدعم، حسابك سيُغلق»:** واتساب لا يطلب رمزك. [7]
- **روابط «صوّت لي» ورموز QR غريبة:** قد تنتهي بربط جهاز غريب بحسابك. ربط الأجهزة يكون من داخل تطبيق واتساب فقط، لا من رابط. [20]: النمط من مصادر ثانوية)
- **«أنا في مشكلة، حوّل لي مالًا»:** من حساب قريب مسروق، وقد يصحبها صوت مقلّد بالذكاء الاصطناعي. [21]

خطوات القفل

1. **فعّل التحقق بخطوتين:** الإعدادات ← الحساب ← التحقق بخطوتين ← تفعيل. اختر رقمًا سريًا أو كلمة سر (حسب إصدار التطبيق)، وأضف بريدك. وإن ظهر في «الحساب» خيار «مفاتيح المرور»، ففعّله أيضًا. [15]
2. **راجع الأجهزة المرتبطة:** الإعدادات ← الأجهزة المرتبطة. أخرج أي جهاز لا تعرفه. [20]
3. **الخصوصية:** من إعدادات الخصوصية، ابحث عن خيار المجموعات واختر من يضيفك إليها. وفي المكالمات، ابحث عن خيار كتم المتصلين غير المعروفين. [22]
4. **التحديث من المتجر الرسمي فقط،** ولا تستعمل نسخًا معدّلة من التطبيق. [5] [23]

إذا سُرق الحساب

1. سجّل برقمك من جديد بالرمز الذي يصلك؛ هذا يُخرج الشخص الآخر. [19]
2. إن طُلب رقم سري أو كلمة سر لا تعرفها، فاتبع تعليمات واتساب على الشاشة؛ قد تلزمك مدة انتظار تصل إلى سبعة أيام. [19]
3. أخبر أصدقاءك من وسيلة أخرى ألا يصدّقوا أي طلب مال أو رموز.

5. مكالمات ورسائل «البنك» المزيّفة (مصر والخليج)

كيف تبدو؟

- مكالمة: «معك خدمة العملاء. بطاقتك ستُوقف. أعطني الرمز الذي وصلك لنلغي العملية».
- رسالة: «حسابك مُعلّق. حدّث بياناتك من هذا الرابط».
- رسالة شحنة: «طردك متوقف. ادفع رسومًا بسيطة من الرابط». (مثال شائع)

العلامات

- **الاستعجال والتهديد:** «الآن، وإلا». [24] [25]
- **طلب بيانات سرية:** الرقم السري، أو رمز التحقق، أو بيانات البطاقة كاملة. [9]
- **رابط في رسالة غير متوقعة.** [24] [25]

- معرفة المتصل باسمك أو بجزء من رقم بطاقتك **لا تثبت** أنه من البنك؛ فقد تكون بعض بياناتك منشورة أو مسرّبة. [24] [10]

ماذا تفعل؟

1. **أغلق المكالمة بهدوء.** لا حاجة إلى نقاش.
2. **اتصل أنت بالبنك على الرقم المطبوع خلف بطاقتك،** أو افتح تطبيق البنك الرسمي بنفسك. [9] [25]
3. **لا تضغط روابط الرسائل.** اكتب عنوان البنك بنفسك أو استعمل التطبيق. [24] [25]
4. **إن أعطيت شيئًا بالفعل:** اتصل بالبنك فورًا لإيقاف البطاقة. السرعة تفرق. [9]

ملاحظة لمصر والخليج: النصيحة نفسها تكرّرها البنوك والجهات الرقابية. البنك المركزي المصري: حملة «معًا نكافح الاحتيال» [8]. في الخليج: راجع موقع البنك المركزي في بلدك.

5ب. خمسة أسئلة تكشف أغلب الرسائل المزيّفة

قبل أن تضغط أو ترد أو تحوّل، اسأل نفسك:

1. **هل كنت أنتظر هذه الرسالة؟** رسالة غير متوقعة عن جائزة أو شحنة أو حساب موقوف تستحق الشك. [24] [25]
2. **هل فيها استعجال أو تهديد؟** «خلال ساعة»، «وإلا سيُغلق حسابك». الجهات الحقيقية لا تبني طلبها على الذعر. [24] [25]
3. **هل تطلب رمزًا أو رقمًا سريًا أو بيانات بطاقة؟** إن كان الجواب نعم، فتوقّف. [7] [9]
4. **هل فيها رابط أو ملف؟** لا تفتحه. اذهب إلى الموقع أو التطبيق الرسمي بنفسك. [24] [25]
5. **هل أستطيع التأكد من طريق آخر؟** اتصل بالشخص أو الجهة على رقم تعرفه أنت، لا على الرقم الموجود في الرسالة. [25] [9]

إن كان جواب سؤال واحد مقلقًا، فالأفضل أن تنتظر وتتأكد. التأخير دقائق لا يضرّ، أما الاستعجال فهو ما يريده المحتال.

وإن ضغطت رابطًا بالخطأ؟ لا تذعر. لا تُدخل أي بيانات في الصفحة، وأغلقها. وإن كنت أدخلت كلمة سر، فغيّرها فورًا من التطبيق أو الموقع الرسمي، وفعّل التحقق بخطوتين. وإن أدخلت بيانات بطاقة، فاتصل بالبنك. [24] [9]

6. تحديث الهاتف والنسخ الاحتياطي

لماذا التحديث؟ كثير من التحديثات تصلح ثغرات أمنية. وبعد الإعلان عن الثغرة قد يحاول المحتالون استغلالها، فالتحديث السريع أكثر أمانًا. [5] [1]

الجهاز	المسار	المصدر
iPhone	الإعدادات ← عام ← تحديث البرنامج	[26]

الجهاز	المسار	المصدر
Android	الإعدادات ← ابحث عن «تحديث» (في هواتف Google: النظام ← تحديثات البرامج؛ ويختلف المكان حسب الشركة المصنّعة)	[27]
التطبيقات	Google Play أو App Store، مع تفعيل التحديث التلقائي	[23]، [5]

- **فعّل التحديث التلقائي** إن أمكن. [5]
- **الهاتف الذي توقّف عنه الدعم** يصبح أقل أمانًا مع الوقت؛ فكّر في بديل حين تستطيع. [5]
- **النسخ الاحتياطي:** فعّل النسخ الاحتياطي لصورك وجهات الاتصال ومحادثات واتساب، وخذ نسخة قبل أي تحديث كبير. [6] [26]

6ب. قفل الهاتف نفسه

- **قفل الشاشة برمز أو بصمة أو وجه،** وتجنّب الرموز السهلة مثل 1234 و0000 وسنة الميلاد. [2] [1]
- **أخفِ محتوى الإشعارات عن شاشة القفل،** فلا يقرأ الرموز من يمسك الهاتف. من إعدادات الإشعارات في هاتفك، ابحث عن معاينة الإشعارات على شاشة القفل. (دليل مستخدم iPhone: تغيير إعدادات الإشعارات؛ المسار في Android يختلف حسب الشركة)
- **فعّل ميزة العثور على الهاتف:** «Find Hub» على Android (اسمها القديم «العثور على جهازي»)، أو «تحديد الموقع» (Find My) على iPhone. تساعدك على العثور على الهاتف المفقود وقفله عن بُعد. تأكّد اليوم أنها مفعّلة. [28]

7. الواي فاي: في المقهى وفي البيت

الواي فاي العام

- **اطمئن قليلًا:** أغلب المواقع والتطبيقات اليوم تشفّر الاتصال، فالشبكات العامة أكثر أمانًا من قبل. [29]
- **تأكّد من اسم الشبكة** من العاملين؛ قد توجد شبكة مزيّفة باسم مشابه. [30]
- **لا تتجاهل تحذيرات المتصفح.** (احتياط عام)
- **صفحة دخول تطلب كلمة سر بريدك أو بطاقتك؟** أغلقها. (استنتاج من [25])
- **للأمور المالية،** استعمل بيانات هاتفك بدل الشبكة العامة. [30]
- **أوقف الاتصال التلقائي** بالشبكات التي لا تعرفها. (احتياط عام)

واي فاي البيت (الراوتر)

- **غيّر كلمة سر صفحة إدارة الراوتر الافتراضية** (ليست كلمة سر الواي فاي نفسها). [31]
- **استعمل تشفير WPA3، أو WPA2 إن كان الراوتر لا يدعم WPA3،** وكلمة سر واي فاي طويلة. [31]

- **حدّث برنامج الراوتر** حين يتوفر تحديث من الشركة المصنّعة أو مزوّد الخدمة. [31]
- إن لم تكن متأكدًا، اطلب المساعدة من مزوّد خدمة الإنترنت. لا تغيّر إعدادًا لا تعرفه.

8. الأطفال وكبار السن

- **تحدّثوا قبل أن يحدث شيء:** اشرحوا القاعدة الذهبية (الرموز لنا وحدنا) لكل فرد، خاصة الوالدين الكبار.
- **كلمة سر العائلة:** اتفقوا على كلمة لا يعرفها غيركم، تُسأل عند أي اتصال أو رسالة صوتية تطلب مالًا بشكل عاجل. [21]
- **«اسألني قبل أن ترسل»:** اتفاق بسيط في العائلة: أي طلب رمز أو مال أو تثبيت تطبيق غريب، يُسأل عنه شخص آخر أولًا.
- **التطبيقات من المتجر الرسمي فقط.** [23]
- **ساعدوهم بأيديكم:** فعّلوا التحقق بخطوتين على هواتف الوالدين معهم، لا عنهم، حتى يعرفوا الرقم السري أو كلمة السر.

9. خطة الطوارئ (احتفظ بها)

إذا شككت أن حسابًا أو بطاقة تعرّضا للخطر:

1. **البطاقة أو المال:** اتصل بالبنك فورًا على الرقم المطبوع خلف البطاقة. [9]
2. **واتساب:** سجّل برقمك من جديد، ثم فعّل التحقق بخطوتين. [19] [15]
3. **البريد:** غيّر كلمة السر من جهاز تثق به، وراجع الأجهزة المتصلة في «فحص الأمان». [18] [14]
4. **أخبر من حولك** من وسيلة أخرى ألا يصدّقوا رسائل باسمك.
5. **أبلغ الجهة الرسمية المختصة بالجرائم الإلكترونية في بلدك.** في مصر: الخط الساخن 108 (مكافحة جرائم المعلومات، وزارة الداخلية)، أو مكتب المباحث المختص في مديرية الأمن بمحافظتك. احتفظ بالرسائل والصور ولا تحذفها. في الخليج: منصة الشرطة الرسمية في بلدك (مثل eCrime في دبي، و«كلنا أمن» في السعودية). [32] [33]

رقم بنكي (من خلف البطاقة)	
بريد الاستعادة	
من أتصل به في العائلة	

(لا تكتب في هذه الورقة أي كلمة سر أو رقم سري.)

قائمة التحقق للعائلة

ضع علامة ✓ عند كل خطوة. كرّر المراجعة كل ثلاثة أشهر.

لكل فرد

- [ ] أعرف القاعدة الذهبية: لا أعطي أي رمز لأي شخص.
- [ ] كلمة سر بريدي طويلة، ولا أستعملها في أي مكان آخر.
- [ ] فعّلت التحقق بخطوتين على البريد.
- [ ] فعّلت التحقق بخطوتين على واتساب، وأضفت بريدي.
- [ ] راجعت «الأجهزة المرتبطة» في واتساب، ولا يوجد جهاز غريب.
- [ ] فعّلت التحقق بخطوتين على فيسبوك وإنستغرام (إن كنت أستعملهما).
- [ ] أستعمل مدير كلمات مرور (مدمج في الهاتف أو غيره).
- [ ] نظام هاتفي محدّث، والتحديث التلقائي مفعّل.
- [ ] التطبيقات من المتجر الرسمي فقط، وتحديثها تلقائي.
- [ ] النسخ الاحتياطي للصور وجهات الاتصال وواتساب مفعّل.
- [ ] أعرف أن البنك لا يطلب رقمي السري، وأن الاتصال يكون بالرقم المطبوع خلف بطاقتي.
- [ ] هاتفي مقفل برمز أو بصمة أو وجه، والرمز ليس سهلًا مثل 1234.
- [ ] محتوى الإشعارات مخفي عن شاشة القفل.
- [ ] ميزة العثور على الهاتف مفعّلة (Find My أو Find Hub).
- [ ] حفظت «الرموز الاحتياطية» لحسابي في مكان آمن.
- [ ] راجعت خصوصية واتساب: من يضيفني إلى المجموعات، وكتم المتصلين غير المعروفين.
- [ ] تأكّدت أن التحقق بخطوتين مفعّل على حساب Apple (إن كان عندي iPhone).
- [ ] أوقفت الاتصال التلقائي بالشبكات التي لا أعرفها.

للعائلة

- [ ] اتفقنا على «كلمة سر العائلة».
- [ ] اتفقنا على «اسألني قبل أن ترسل».
- [ ] ساعدنا الوالدين الكبار على تنفيذ القائمة.
- [ ] ورقة خطة الطوارئ مكتملة ومحفوظة (دون كلمات سر).

للبيت

- [ ] كلمة سر صفحة إدارة الراوتر ليست الافتراضية.
- [ ] الواي فاي يستعمل WPA3 (أو WPA2 إن لم يتوفر) بكلمة سر طويلة.
- [ ] برنامج الراوتر محدّث.

المصادر

المعلومات في هذا الدليل مأخوذة من الإرشادات العامة لجهات رسمية:

CISA (الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية): Secure Our World، وHome Network Security.

NCSC (المركز الوطني البريطاني للأمن السيبراني): نصائح البقاء آمنًا على الإنترنت، والتصيّد الاحتيالي.

FTC (لجنة التجارة الفدرالية الأمريكية): التصيّد الاحتيالي، والواي فاي العام.

صفحات المساعدة الرسمية: WhatsApp، وGoogle، وApple، وMeta.

Take Five to Stop Fraud (حملة القطاع المصرفي البريطاني).

البنك المركزي المصري (حملة «معًا نكافح الاحتيال»)، ووزارة الداخلية المصرية (الخط الساخن 108).

المركز الكندي للأمن السيبراني (Get Cyber Safe)، ووكالة الأمن القومي الأمريكية NSA: الواي فاي العام.

مكتب التحقيقات الفدرالي FBI (IC3): كلمة سر العائلة.

الروابط الكاملة في نهاية الملف المنشور. هذا الدليل للتوعية العامة، ولا يغني عن التواصل مع بنكك أو مزوّد الخدمة في حالتك الخاصة.

الروابط الكاملة

[1] CISA: Secure Our World
https://www.cisa.gov/secure-our-world

[2] NCSC (UK): Use three random words
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

[3] NCSC (UK): Password managers
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

[4] NCSC (UK): Turn on 2-step verification
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

[5] NCSC (UK): Install the latest software and app updates
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

[6] NCSC (UK): Always back up your most important data
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

[7] WhatsApp Security page + Singapore CSA advisory AD-2020-007
https://www.whatsapp.com/security
https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2020-007/

[8] Central Bank of Egypt campaign «معاً نكافح الاحتيال», via the Egyptian Banking Institute (Masrafeyoun), 25 Sep 2025
https://masrafeyoun.ebi.gov.eg/?p=14200

[9] Take Five to Stop Fraud (UK Finance): About
https://takefive-stopfraud.org.uk/about/take-five

[10] FTC consumer alert, June 2024: Got a call about fraud activity on your bank account?
https://consumer.ftc.gov/consumer-alerts/2024/06/got-call-about-fraud-activity-your-bank-account-it-could-be-scammer

[11] Google Help: Save, manage & protect your passwords
https://support.google.com/accounts/answer/6208650
https://passwords.google.com

[12] Apple Support: Use the Passwords app
https://support.apple.com/120758

[13] NCSC (UK): Use a strong and separate password for your email
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

[14] Google Account Help: Turn on 2-Step Verification (Arabic version: «إعدادات الأمان وتسجيل الدخول»)
https://support.google.com/accounts/answer/185839

[15] WhatsApp FAQ: How to manage two-step verification settings + WhatsApp blog, 25 Aug 2026 (passkeys; 6-digit PIN being upgraded to a password, gradual rollout)
https://faq.whatsapp.com/1920866721452534
https://blog.whatsapp.com/one-billion-people-are-now-protected-with-passkeys-on-whatsapp-plus-more-account-security-features

[16] Apple Support: Two-factor authentication for Apple Account
https://support.apple.com/en-us/102660

[17] Meta Help: Two-factor authentication
https://www.facebook.com/help/148233965247823

[18] Google Security Checkup
https://myaccount.google.com/security-checkup

[19] WhatsApp FAQ: How to recover a compromised account
https://faq.whatsapp.com/1131652977717250

[20] WhatsApp FAQ: How to unlink a device
https://whatsapp.com/faq/en/web/28080003

[21] FBI IC3 PSA I-120324-PSA, 3 Dec 2024
https://www.ic3.gov/PSA/2024/PSA241203

[22] WhatsApp blog: New privacy features: Silence unknown callers and Privacy Checkup (June 2023)
https://blog.whatsapp.com/new-privacy-features-silence-unknown-callers-and-privacy-checkup

[23] Google Play Help: Update apps
https://support.google.com/googleplay/answer/113412

[24] NCSC (UK): Phishing scams
https://www.ncsc.gov.uk/collection/phishing-scams

[25] FTC (US): How to recognize and avoid phishing scams
https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[26] Apple Support: Update iPhone or iPad
https://support.apple.com/en-us/118575

[27] Android Help: Check & update your Android version
https://support.google.com/android/answer/7680439

[28] Google Find Hub + Apple Find My
https://support.google.com/android/answer/6160491
https://support.apple.com/102648

[29] FTC (US): Are public Wi-Fi networks safe?
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[30] Canadian Centre for Cyber Security (Get Cyber Safe): Public Wi-Fi
https://www.getcybersafe.gc.ca/en/secure-your-connections/public-wi-fi

[31] CISA: Home Network Security (archived page)
https://www.cisa.gov/news-events/news/home-network-security

[32] Egypt Ministry of Interior: emergency numbers (108 = «مكافحة جرائم المعلومات»)
https://moi.gov.eg

[33] Gulf reporting: UAE u.ae "Report cybercrimes online" (Dubai Police eCrime, Abu Dhabi Police Aman, My Safe Society); Saudi «كلنا أمن»
https://u.ae

© 2026 Forgemark Labs

أُعدّ نص هذا الدرس بمساعدة أدوات الذكاء الاصطناعي، وراجعه وتحقق من معلوماته فريق Forgemark Labs، وهو المسؤول عن محتواه. الغلاف بأشكال العلامة فقط. المحتوى للتوعية العامة، وليس نصيحة قانونية أو مالية أو مهنية.

الخط: Tajawal – SIL Open Font License 1.1



FORGEMARK LABS

forgemarklabs.com

مواد مجانية أخرى على الموقع: forgemarklabs.com