



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

اتصال آمن دائماً وفي كل مكان



قف. فكر. آمن.

استخدام

اتصال غير آمن

يشبه إجراء

محادثة خاصة

في غرفة مزدحمة.
افتراض أن هناك من



ncscbh

ncsc_bh

www.ncsc.gov.bh

فعل الشبكة الافتراضية الخاصة (VPN)

أداتك للاتصال الآمن

يُشفّر بياناتك

يحمي كل ما ترسله أو تستقبله، سواء
كانت معلومات شخصية أو مهنية.



يُخفي موقعك الجغرافي

يقلل من تتبع المواقع والإعلانات أو من
مجرمي الإنترنت.



يحميك عند الاتصال بشبكات الواي
فاي العامة

يحافظ على أمان جهازك وبيانات
مؤسستك عند الاتصال بشبكات غير
موثوقة.



وصول آمن لمنصات العمل

توفير اتصال آمن بأنظمة العمل أثناء
السفر أو العمل عن بُعد.



تنبيه مهم



احرص دائماً على تفعيل
الشبكة الافتراضية الخاصة
(VPN) عند استخدام
الشبكات العامة أو
المشتركة، لأنها خطوة
أساسية لحماية
بيانات العمل.



استخدم نقطة الاتصال الشخصية

فهي أكثر أمانًا من شبكات الواي فاي العامة!

اتصال مشفر

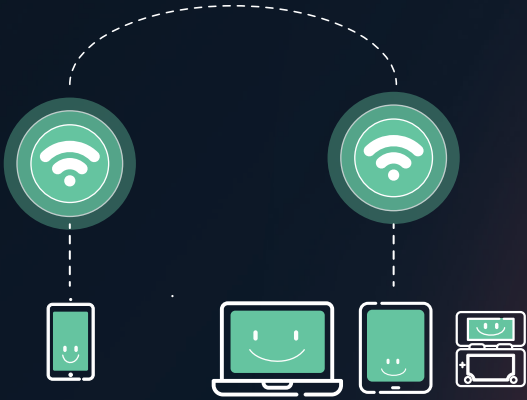
تعتبر بيانات هاتفك المحمول أكثر أمانًا وأقل عرضة للاختراق مقارنة بشبكات الواي فاي التي لا تتطلب كلمة مرور.

لا يسمح للغرباء بالاتصال

على عكس شبكات الواي فاي العامة، أنت من يحدد من يمكنه الاتصال بشبكته.

أمان أثناء التنقل

مثالي أثناء السفر، أو في الأماكن العامة، أو في حالات الطوارئ.



تنبيه مهم

في حال عدم توفر واي فاي آمن، استخدم نقطة الاتصال الخاصة بجهازك، ولا تنس تفعيل كلمة مرور قوية.

تجنب الاتصال بشبكات الواي فاي (Wi-Fi) العامة غير الآمنة

شبكات الواي فاي العامة = أبواب مفتوحة للمخترقين!

يمكن للمخترقين اعتراض أي بيانات ترسلها (مثل كلمات المرور، رسائل البريد الإلكتروني، أرقام بطاقات الائتمان).

قد تبدو بعض المواقع الوهمية آمنة، حتى لو كانت تستخدم بروتوكول HTTPS.

يمكن للمخترقين توجيهك إلى مواقع تصيد احتيالية، مثل صفحات تسجيل الدخول أو البنوك المزيفة.



تنبيه مهم

قُم بإيقاف ميزة "الاتصال التلقائي بشبكات الواي فاي العامة" لتجنب الاتصال بشبكات غير آمنة دون إذنك.

HTTPS

قفل الأمان الذي يحميك

يشير حرف الـ "S" في بروتوكول HTTPS على أن الاتصال "آمن"، ويشير الرمز  في شريط المتصفح إلى أن بياناتك مشفرة أثناء الإرسال.

هذا يعني أن الموقع يستخدم شهادة أمان صالحة، ويُعد أكثر أمانًا. ولكن:



كن حذرًا

يمكن للمخترقين إنشاء مواقع وهمية تبدو موثوقة.

تحقق دائمًا

من عنوان الموقع (URL)، وكن حذرًا من الروابط غير المألوفة.

 <https://example.com> 

 <http://example.com> 