

كيف
تنشئ كلمة
مرور قوية



إشارات Esharat

للأطفال



6 نصائح للبقاء آمناً على شبكات الواي فاي العامة

أصبح من أسلوب حياتنا العصري عندما نخرج من منزلنا أن نبحث عن إشارة واي فاي عام والاتصال بها، سواء كنا داخل مركز تجاري أو في المقهى أو المطعم، أو عندما نستقل القطار أو حتى لو كنا على شاطئ البحر؛ لكن يجب أن نتذكر جيداً أن شبكات الواي فاي العامة مستهدفة بكثرة من قبل قرصنة الإنترنت، لذلك يجب أن تكون حذراً عند استخدامها. فالاتصال بالشبكة الخاطئة سيعرض كافة معلوماتك الشخصية للسرقة، لذلك انتبه جيداً عند استخدام شبكات الواي فاي العامة.

فيما يلي أهم 6 نصائح تساعدك في حماية خصوصيتك أثناء استخدام شبكات الواي فاي العامة:

احتفظ بمعلوماتك الشخصية لنفسك

لا تدخل أي كلمات مرور أو تفاصيل بنكية أو أرقام بطاقة هويتك إلى شبكات الواي فاي العامة. قد يبدو هذا أمراً بديهياً، إلا أن الكثيرين يتجاهلون ذلك ويقومون بالإفصاح عن بياناتهم الشخصية.

تجنب مشاركة بياناتك الخاصة

أوقف خاصية "مشاركة الملفات" على هاتفك قبل الاتصال بشبكة واي فاي عامة. صحيح أن المشاركة أمر إيجابي في حياتنا الاجتماعية، لكن في العالم الافتراضي المشاركة على شبكات الواي فاي العامة قد تعرض خصوصيتك وبياناتك للخطر.

اتصل بشبكة آمنة دائماً

من الأفضل أن تبحث عن شبكة واي فاي تتطلب تسجيل الدخول إليها أولاً. عادةً ما تكون هذه الشبكات محمية مما يعني أنها آمنة، أما إذا وجدت شبكة مفتوحة لا تحتاج إلى إدخال كلمات مرور فعليك التعامل معها بحذر. وعلى الرغم من أن الفنادق والمطاعم توفر شبكات غير محمية إلا أن الدخول إليها يتطلب استخدام كلمة مرور محددة. وإن لم تتطلب هذه الشبكات ذلك، فاحذر من استخدامها.

تحقق بنفسك من شبكة الواي فاي

تجنب ضبط إعدادات هاتفك على الاتصال التلقائي بأقرب شبكة واي فاي، وإلا ستعرض معلوماتك الشخصية للتجسس بكل سهولة؛ بل تحقق بنفسك من كافة الشبكات المتوفرة على هاتفك ثم اختر شبكة الإنترنت الأكثر أمناً.

لا تستخف بأهمية التحديثات

من الضروري أن تحدّث البرامج على جهازك وقتما كانت التحديثات الأخيرة متاحة. فهناك شركات مثل "أبل" تطرح تحديثات لبرامج أجهزتها حتى تستطيع حمايتها من أحدث برامج الاختراق التي تم اكتشافها. وتذكر أنك ستكون معرضاً للاختراق دائماً إن لم تقوم بتحديث أجهزتك.

اختر شبكة الواي فاي بدقة وحذر

عندما تحاول الاتصال بشبكة واي فاي عامة ستجد قائمة طويلة من الشبكات الظاهرة على جهازك، وستجد أيضاً بعض الشبكات المتطابقة في الاسم، وهذا يشير إلى أن هذه الشبكات تقع تحت سيطرة أحد القرصنة. لذلك احرص دائماً على اختيار الشبكة الأصلية التي تحظى بالحماية، وإذا عجزت عن تحديدها يمكنك أن تسأل أحد الموظفين في المكان.

كيف تنشئ كلمة مرور قوية

كلمة المرور القوية مهمة جداً لحماية حساباتك من الخطر والحفاظ على أمنها وتجنب أي نوع من التجسس أو اختراق لأجهزتك. وقاعدة إنشاء كلمة مرور قوية تكون في صياغة كلمة طويلة يسهل تذكرها وفي نفس الوقت يصعب تخمينها. إليك بعض النصائح المهمة لمساعدتك في إنشاء كلمة مرور منيعة وقوية.

اختر أحرفاً وأرقاماً متنوعة

لا تستخدم الحروف فقط عند إنشاء كلمة المرور، فكلمة المرور القوية لا تكتمل سوى بمزج الحروف والأرقام معاً لصياغة كلمة معقدة مثل (b41{}E\$h4r@tD) وغيرها من الصيغ الأخرى.

تجنب استخدام بياناتك الشخصية

تجنب استخدام المعلومات الشخصية مثل اسمك وتاريخ ميلادك أو هواياتك المفضلة وغيرها.. إن كلمات المرور التي تحتوي على معلومات شخصية كهذه يسهل اختراقها باستخدام برامج قرصنة تعتمد على قواعد بيانات أو قاموس خاص.

اجعل كلمة المرور متفردة

تجنب استخدام كلمة المرور نفسها في جميع الحسابات والأجهزة الخاصة بك، بل احرص على إنشاء كلمة مرور مختلفة لكل حساب وجهاز لديك حتى تتجنب اختراقها جميعاً بسهولة.

كن مبتكراً

استخدم لوحة مفاتيح جهاز الكمبيوتر الخاص بك لإنشاء كلمات مرور من خلال "التوصيل بين النقاط". فمثلاً إذا قمت بتوصيل الأحرف والأرقام "567ygvpn" على لوحة المفاتيح ستجد أنها تشكل حرف Z. كما يمكنك إنشاء كلمات مرور يسهل تذكرها من خلال استخدام رموز الوجوه المفضلة لديك مثل (:، =، (، 8) وغيرها من الأشكال.

اختر كلمة مرور طويلة

كلما كانت كلمة المرور أطول، كانت محاولة اختراقها أصعب على الآخرين. أما إذا اخترت كلمة قصيرة وسهلة فإنك بذلك تساعد المخترقين على الوصول بكل سهولة إلى حساباتك. لذلك يجب أن تتكون كلمة المرور الخاصة بك من 8 حروف وأرقام على الأقل.

00

00

امغامرات
شيلد هان

تدور أحداث هذه القصة
في غرفة نوم أحد الأطفال
بمنزل في دولة الإمارات
العربية المتحدة..

آه! هذا مزعج للغاية.

إنني أَلعب مباراة كرة القدم
لكنني أخسر باستمرار..
تعبت من الخسارة!

لم كل هذه
الضجة يا جمال؟

سوف أقوم بتنزيل بعض
رموز الغش لكي أفوز
وأغلب الجميع!

أريد أن أفوز.. هذا
كل ما يهمني يا أسماء!

ولكن ألا تعرف
أن الغش أمر سيء جداً؟

لا أنصحك بزيارة
هذا الموقع لا يبدو
آمناً على الإطلاق.

انظري إلى
هذا الموقع الإلكتروني
الرائع الذي وجدته:

www.cheatersalwaysprosper.hacked

لا تقلقي، جميع مواقع
الإنترنت آمنة! لو لم
يكن هذا الموقع آمناً لكان
قد تم إغلاقه على الفور.

انظري، هناك بعض
رموز الغش التي ستجعلني
أفوز في كل مرة أَلعب!

تمهل يا جمال! أنت على وشك
ارتكاب خطأ جسيم جداً!

"شيلدمان!"

أيها الصغيران، لا يمكنكما
تنزيل أي ملف من موقع مجهول من
دون اتخاذ الاحتياطات اللازمة!

فقد تكون هذه المواقع
ضارة جداً وقد تحتوي على
فيروسات خبيثة قادرة على
تدمير جهاز الحاسوب!

لا أريد أن يحدث
مثل هذا الأمر لي أبداً!

ولكن كيف يمكننا
أن نعرف أنه موقع سيء؟

لن أقوم بتنزيل
هذه الرموز إذا!

أحسنت يا جمال! وتذكر، إذا أردت
أن تكون ماهراً في شيء ما، فعليك
أن تكرر المحاولة دائماً ولا تستسلم أبداً!
وكما قالت لك أختك، الغش لا ينفع أبداً..
تصفح الإنترنت بحذر وتحقق من كل
شيء قبل التنزيل والتحميل!

إلى اللقاء يا "شيلدمان"،
أنت بطلي المفضل!

عندما ترغب في تنزيل أي ملف، خصوصاً إذا كان
من مصادر غير موثوقة لا تعرفها، فعليك أن تقوم بمسح
الملف أولاً حتى تتأكد أنه آمن وخالٍ من الفيروسات؛ وبعدها
يمكنك اللعب على جهازك من دون أي مخاطر!

سؤال جيد يا أسماء.. سأخبركما ببعض
النصائح التي عليكم تذكرها جيداً قبل أن
تقوما بتنزيل أي ملف جديد على الجهاز!

يجب أن ننسخ الرابط ونقوم بمسحه
على الإنترنت للتحقق من عدم احتوائه
على فيروسات، وهذا كفيلاً بإخبارنا
إذا كان الملف آمناً للتحميل أم لا.

شكراً لك يا "شيلدمان"!
لم أكن أعرف كل ذلك، لذلك
سأقوم بمسح الملف الآن!

انظر! المسح يظهر أنه
يحتوي على فيروس!

علينا أن نتحقق أيضاً من الموقع
الإلكتروني؛ يجب أن نقوم بتنزيل
الملفات من المواقع المعروفة
والموثوقة فقط والتي تبدو ذات
تصميم احترافي.

يجب أن نتحقق أولاً من الملف الذي
نريد تنزيله.. لو كان غير قانوني كالأغاني
أو الأفلام أو رموز الغش، فقد
يكون مجرد خدعة وسيصيب أجهزتنا
بفيروس خبيث، لذلك علينا تجنب
تنزيل أي ملفات بشكل غير قانوني!

ابحث عن 10
كلمات ضائعة
تتعلق بأجهزة
الكمبيوتر وعالم
الإنترنت.

ح	ض	ش	ب	ر	م	ج	ي	ا	ت	ص	ف
ي	ا	و	ط	هـ	ق	ف	ل	ى	ا	أ	ث
ة	ظ	س	ط	ب	ض	ك	ن	هـ	ر	غ	ك
ع	ة	ك	و	م	ا	ن	ض	ة	ع	ت	ل
ب	ذ	ظ	ن	ب	ت	و	ء	ب	ي	س	م
ا	ص	م	ق	خ	ة	م	ر	خ	و	م	ة
ط	ح	ئ	س	ت	ط	ف	ة	ل	ا	خ	ا
ل	ؤ	ر	ا	د	خ	ش	ا	ش	ة	ب	ل
ا	ج	ك	ص	م	ث	ع	ن	ذ	هـ	ع	س
ذ	ب	ق	ت	ا	س	و	ر	ي	ف	ن	ر
ش	ؤ	ي	م	ط	ز	هـ	و	ش	ت	ف	ى
هـ	ن	ا	ل	ا	ن	ت	ر	ن	ت	ذ	م

الطابعة
فأرة
الإنترنت
حاسوب
شاشة
برمجيات
كلمة السر
فيروسات
روابط
شبكات

ما هي برأيك كلمة السر الأقوى؟ اختر واحدة فقط.

