الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ توجيهية لتأمين
شبكات الواي-فاي العامة

عـــام

إخلاء المسؤولية / الحقوق القانونية

قامت الوكالة الوطنية للأمن السيبراني (NCSA) بإعداد ووضع هذا المنشور, بعنوان " مبادئ توجيهية لتأمين شبكات الواي-فاي العامة" - الإصدار 2.0 - ، لمساعدة مزودي خدمة الواي-فاي العامة والمستخدمين على فهم المخاطر المرتبطة بها والتخفيف من حدتها. وهي مسؤولة عن مراجعة هذه الوثيقة والمحافظة عليها. وعلى الوكالة بصفتها مصدر ومالك, بغض النظر عن طريقة نسخ أي نسخة سواء أكانت كلية أو جزئية من هذه الوثيقة؛ بما يخص «إرشادات الأمن السيبراني لشبكات خدمة الواي-فاي العامة».

وفي حالة طلب أي نسخ بخصوص هذه الوثيقة بقصد التسويق التجاري, يلزم الحصول على إذن كتابي من الوكالة الوطنية للأمن السيبراني. ولها أحقية في تقييم مدى فعالية وإمكانية تطبيق جميع النسخ المطورة فيما يخص الأغراض التجارية.

ولا يجوز تفسير الإذن الصادر عن الوكالة الوطنية للأمن السيبراني على أنه تأييد للنسخ المطورة ولا يجوز للمطور بأي حال من الأحوال الإعلان عن ذلك أو إساءة تفسيره بأي شكل من أشكال في وسائل الإعلام أو المناقشات الشخصية / الاجتماعية.

مراقبة الوثائق

تفاصيل الوثيقة	
رقم هوية الوثيقة	IAG-NGE-GPWN
الإصدار	إصدار 2.0
التصنيف والنوع	عام
الخلاصة	لمساعدة مزودي خدمة الواي-فاي العامة والمستخدمين على فهم المخاطر المرتبطة بها والتخفيف من حدتها.

المراجعة / الموافقة

القسم / المهمة	تمت المراجعة / الموافقة	الإصدار	التاريخ
شؤون الحوكمة والضمان السيبرانى الوطني		2.0	

سجل النسخ المنقحة

الإصدار	المؤلف:	وصف المراجعة	التاريخ
1.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	أبريل 2018
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	يناير 2023
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور + تعديلات تصحيحية طفيفة	ديسمبر 2023

التفويض القانوني

يحدد القرار الأميري رقم (1) لسنة 2021 فيما يخص إنشاء الوكالة الوطنية للأمن السيبراني، صلاحياتها (المشار إليها فيما يلي باسم "الوكالة الوطنية للأمن السيبراني"). وتتمتع الوكالة الوطنية للأمن السيبراني بسلطة الإشراف على أمن البنية التحتية الوطنية الحيوية وتنظيمها وحمايتها من خلال اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد تم إعداد هذه الوثيقة مع الأخذ في الاعتبار بالقوانين المعمول بها في دولة قطر. وفي حالة نشوء تعارض بين هذه الوثيقة (أحكام أو بنود محددة) وقوانين دولة قطر، تسود قوانين دولة قطر. وبذلك، يعتبر أي مصطلح من هذا القبيل (أحكام أو بنود محددة) محذوفًا من هذه الوثيقة، دون المساس بالأحكام المتبقية من هذه الوثيقة. ويلزم في هذه الحالة إجراء تعديلات لضمان الامتثال للقوانين السارية ذات الصلة بدولة قطر.

جدول المحتويات

1 المقدمة

1.1 السياق

تتوفر شبكات الواي-فاي العامة في قطر على نطاق واسع ومتاحة بسهولة داخل دولة قطر في المطارات والحدائق والمطاعم والمقاهي والمكتبات والفنادق. وتكون "نقاط الاتصال" منتشرة على نطاق واسع، ويرغب الأشخاص في الاتصال بها دون تردد.

والغرض منها أن تكون خدمة عامة، أو قيمة مضافة لعملائها، فهي لا تأتي دون نصيبها من المخاطر. وقد لا نكون قادرين مبدئيًا بشكل دائم القول بصيغة مؤكدة من هو مزود خدمة الواي-فاي، أو من هم المستخدمون؟ ونظرًا لأنها عادةً خدمة مجانية، فمعظم الشركات بشكل عام لا تضع الكثير من الضوابط لتأمين الخدمة.

وعلى الرغم من أنه يبدو من غير الضار تسجيل الدخول والتحقق من حسابك على وسائل التواصل الاجتماعي أو تصفح بعض المقالات الإخبارية، إلا أن الأنشطة اليومية التي تتطلب تسجيل الدخول - مثل قراءة البريد الإلكتروني أو التحقق من حسابك المصرفي قد تكون محفوفة بالمخاطر على شبكة الواي-فاي العامة.

2 الغرض والنطاق والاستخدام

2.1 الغرض

تهدف هذه الوثيقة إلى مساعدة الأفراد أو المؤسسات على فهم المخاطر المرتبطة باستخدام أو توفير شبكة الواي-فاي متاحة للجمهور وكذلك تقنيات للتخفيف من مثل هذه الهجمات..

2.2 النطاق

أي فرد \ مؤسسة يمتلك أو يوفر أو يستخدم شبكة لاسلكية متاحة للجمهور في دولة قطر.

أي مؤسسة توفر شبكة الواي-فاي للضيف ويوفر خدمات الإنترنت للمتعاونين والموظفين المؤقتين وما إلى غير ذلك.

2.3 الاستخدام

ستساعد الإرشادات الواردة في هذه الوثيقة المؤسسات على توفير خدمات واي-فاي عامة آمنة لعملائها و / أو البائعين و / أو الجمهور. كما تساعد أيضًا الأفراد على استخدام خدمات واي-فاي العامة بأمان.

3 التعريفات الرئيسية

المؤسسات/المؤسسة	تشير إلى المؤسسات و الشركات الحكومية و غير الحكومية بدولة قطر.
الفرد/الافراد	تشير إلى اي شخص/مجموعة من الاشخاص يتصل, يدير أو يمتلك شبكة انترنت لاسلكية للعموم.

4 الإرشادات

4.1 فهم المخاطر

الميزات مثل الانفتاح وسهولة الاتصال التي تجعل نقاط اتصال الواي-فاي المجانية مرغوبة للمستهلكين، وتجعلها أيضًا مرغوبة للمتسللين. وهناك عدد هائل من المخاطر المصاحبة لشبكات الواي-فاي العامة. في حين أن أصحاب الأعمال قد يعتقدون أنهم يقدمون خدمة قيمة لعملائهم، فمن المحتمل أن يكون الأمان على هذه الشبكات منخفضًا جدًا أو غير موجود.

كلما قل مستوى الأمان الذي تتمتع به نقطة اتصال الواي-فاي، أصبح من الأسهل على المهاجم الاتصال والتنصت على المستخدمين وتوزيع البرامج الضارة وسرقة المعلومات الحساسة. وتكون تقنيات مثل التطفل والتجسس والتصيد الاحتيالي وهجوم الوسيط في التشفير وأمن الحاسوب شائعة في مثل هذه السيناريوهات.

ويمكن أن تؤدي الهجمات إلى الاحتيال على المستهلكين، على سبيل المثال عن طريق سرقة معلومات بيانات بطاقة الائتمان. ويمكن أن تؤدي أيضًا إلى تسريب بيانات المستهلك الخاصة والصور والمحادثات إلى مجرمي الإنترنت لإعادة بيعها أو إعادة استخدامها في أعمال ضارة.

وهناك تهديد من وضع نقاط اتصال الواي-فاي المخترقة في الأماكن العامة لخداع الجمهور الساذج لاستخدام الخدمات وبالتالي فقدان معلوماتهم الحساسة التي قد يتم التجسس عليها من قبل مزود الخدمة الضارة.

وفي كثير من الأحيان، تفتقر هذه الخدمات إلى التحكم في الوصول، أي لا توجد طريقة لمعرفة من استخدم هذه الخدمات. وقد يكون هذا عائقًا كبيرًا في حالة وقوع حادث إلكتروني حيث قد لا تكون هناك طريقة لتحديد الإجراء المناسب لأي شخص.

4.2 مالك / مزود الخدمة شبكة الواي-فاي

يلزم أن يكون تشغيل الخدمات والوصول إلى أي معلومات خاصة بالعميل أو تخزينها أو معالجتها أو نقلها من خلال جميع الأجهزة والشبكات اللاسلكية المستخدمة، بطريقة آمنة ووفقًا لمعيار تأمين المعلومات الوطنية (NIAS) بدولة قطر.

تسمح هذه الإعدادات بتقليل:

1. التهديدات السيبرانية من الإنترنت للعملاء.
2. التهديدات السيبرانية التي قد يبدأها العملاء عن قصد أو عن غير قصد إلى أطراف أخرى عبر الإنترنت.
3. التهديدات السيبرانية التي قد يبدأها العملاء عن قصد أو عن غير قصد إلى عملاء آخرين على شبكة الواي-فاي العامة.

4.2.1 الحوكمة

1. تعريف مالك الخدمة فيما يخص هذه الخدمة. ويلزم أن يكون مالك الخدمة مسؤولاً عن تشغيل وتأمين الخدمة لتصبح في مستوى مقبول.
2. إجراء تقييم للمخاطر وتحديدها فيما يخص تشغيل هذه الخدمة. فضلاً عن تنفيذ خطة لتخفيف المخاطر المحددة وإدارتها لتصبح في مستوى مقبول.
3. يلزم على مالك الخدمة تحديد الاستخدام التشغيلي المقبول والإجراءات الأمنية للخدمة.

4. يلزم توثيق المستندات الفنية المتعلقة بالخدمة مثل وثائق تصميم الشبكة والتصميم الوظيفي وتخطيطات الشبكة وتفاصيل عنوان IP وما إلى غير ذلك؛ وتأمينها وإتاحة الوصول إليها على أساس الحاجة إلى المعرفة فقط.
5. صيانة وتوثيق مستند المخزون لجميع الأجهزة المطلوبة لتقديم هذه الخدمة.
6. صيانة وإدارة تقارير النشاط والإحصاءات وتقارير الاستخدام لمستخدمي الشبكات اللاسلكية.
7. اتفاقية أمن المعلومات: تطوير اتفاقية المستخدم الخاصة بأمن المعلومات.
8. سياسة أمن المعلومات: تحديد سياسة الخصوصية لمستخدمي الواي-فاي.

4.2.2 التحكم في الوصول

1. يلزم قبل توفير أي وصول إلى الانترنت تحديد المستخدمين والمصادقة عليهم والتصريح لهم للوصول إلى الخدمات اللاسلكية بما في ذلك الخدمات المجانية.
2. يلزم أن تكون الخدمة قادرة على تحديد المستخدمين والمصادقة عليهم بطريقة مقبولة. مثال: مصادقة ثنائية باستخدام جهاز محمول.
3. تقديم / عرض سياسة الاستخدام العادل (AUP) للمستخدم عند الوصول إلى المدخل المقيد. ويجب على المستخدم قراءة وقبول شروط الاستخدام قبل الوصول إلى أي موقع ويب.

4.2.3 جمع البيانات ومشاركتها

1. يجب أن تتضمن سياسة الاستخدام العادل أيضًا إخلاء المسؤولية القانونية وشروط سياسة الخصوصية والموافقة على استخدام أي معلومات تعريف شخصية (PII) قد يتم طلبها أو جمعها من المستخدم أثناء عملية تسجيل الدخول إلى النظام أو استخدام خدمات الإنترنت. (راجع ملحق سياسة الاستخدام العادل)
2. يجب استخدام أي بيانات يتم جمعها من المستخدمين ومشاركتها فقط وفقًا للوثائق القانونية الحالية مثل قانون حماية خصوصية البيانات الشخصية.
3. لا ينبغي مشاركة البيانات الشخصية مع أي طرف خارجي إلا عندما يكون ذلك مطلوبًا ومسموحًا به بموجب قانون حماية خصوصية البيانات الشخصية (المادة 18).

4.2.4 تصلب الأمن:

4. عند تصميم الشبكة الخاصة بك، افصل شبكة عملك / شركتك عن شبكة الواي-فاي العامة. ومن الأفضل الفصل ماديًا، ولكن الفصل المنطقي مع الضوابط القوية يمكن أن ينجح أيضًا إذا كان يوفر التخفيف اللازم من المخاطر.
5. يجب وضع تدابير أمان مناسبة للشبكة مثل تقسيم المناطق والتكوين المناسب لحلول إدارة التهديدات الموحدة (مثل جدران الحماية وغيرها)، وفقًا لأفضل الممارسات العالمية (مثل معيار تأمين المعلومات الوطنية وNIST 800-41 وNIST 800-53 وISO 27001 وغيرها).
6. استخدم معرف مجموعة خدمات مختلفة أثناء تحديد أسماء الشبكة اللاسلكية. تجنب استخدام أسماء مشابهة مثل "ABC_Corp" و "ABC_Public" أو "ABC_Guest"
7. استخدم بروتوكولات أمان لاسلكية قوية مثل نظام الوصول المحمي للشبكات اللاسلكية الطراز الثاني وأمن طبقة نقل بروتوكول المصادقة القابل للامتداد. وتجنب استخدام بروتوكولات الخصوصية المكافئة للشبكات السلكية وبروتوكول التطبيقات اللاسلكية.
8. قم بمسح / تعطيل كلمات المرور الافتراضية على مبدّلات وموجهات الشبكة ونقاط الوصول اللاسلكية وأي أجهزة أخرى. بالإضافة إلى تكوين كلمات مرور قوية بما يتماشى مع أفضل الممارسات. فعلى سبيل المثال، حد أدنى للطول 12 حرفًا بدون متطلبات تعقيد أو طول كلمة المرور ثمانية أحرف تحتوي

على واحد على الأقل من كل حرف صغير (a-z)، حرف كبير (A-Z)، رقم (0-9)، علامة ترقيم / حرف خاص.

9. قم بتكوين نقاط الوصول والموجهات وفقًا لأفضل الممارسات العامة / البائع. وكذلك القيام بالتشفير (إذا كان متاحًا)، وعادة ما يتم تعطيله افتراضيًا.
10. قم بتغيير كلمات المرور بشكل دوري.
11. الاحتفاظ بسجلات وصول الخاصة بالمستخدمين. يجب أن تحتفظ سجلات الوصول بسمات مثل اسم المستخدم (إن أمكن) ورقم الهاتف المحمول المرتبط (المستخدم للمصادقة) وعنوان IP المخصص والتاريخ والوقت وما إلى غير ذلك، والتي قد تحدد هوية المستخدم.
12. تمكين استخدام سجلات الأمان على جميع الأجهزة. راجع "إرشادات إدارة الحوادث - إجراءات المتطلبات الأساسية" للحصول على الدعم والإرشاد
13. الاحتفاظ بسجلات الأمان لمدة لا تقل عن 120 يومًا.
14. اتخاذ التدابير المناسبة لضمان اكتشاف والاستجابة ومنع نقاط الوصول المخترقة وتكنولوجيا الاستنشاق على شبكة الواي-فاي العامة. كما يوصى بشدة باستخدام نظام منع الاختراق / نظام كشف الاختراق اللاسلكية حيث تتوفر شبكة الواي-فاي العامة أو تتواجد مع شبكة المؤسسة.
15. استخدم آليات التبادل الديناميكي والشبكة الخاصة الافتراضية الآمنة لنقل معلومات التعريف الشخصية أو معلومات الدفع لتوفير قدر كافٍ من التشفير والتحكم في الوصول من طرف إلى طرف.
16. قم بتصحيح البنية التحتية اللاسلكية وتحديثها بانتظام.

4.2.5 الأمن المادي:

1. يجب اتخاذ تدابير مناسبة لتأمين نقاط الوصول فعليًا من الوصول المادي غير المصرح به أو الضرر المادي العام
2. تأكد من تأمين جهاز التوجيه اللاسلكي أو نقاط الوصول من مستخدمي شبكة الواي-فاي العام/ الضيف؛ إذ أنه من المستحسن أن تكون غير مرئية أو مثبتة في مناطق يسهل الوصول إليها مثل الأماكن المرتفعة (الأعمدة) أو تحت السقف المستعار الزائف.
3. إذا كانت هناك منافذ لشبكة Ethernet على الجدران، فتأكد من أنها ليست في متناول الزوار وأنها مؤمنة بشكل كاف. وإذا لم يتم استخدامها، فقم بفصلها عن الشبكة.
4. إذا كان الجهاز مفقودًا / مسروقًا، فقم بتعديل معرف مجموعة الخدمات المختلفة (اسم الواي-فاي) وكلمات المرور.

4.2.6 الإبلاغ عن الحوادث والتعامل معها.

1. جهة الاتصال في حالات الطوارئ:
   (أ) أنشئ قائمة جهات اتصال للوصول إلى الموظفين (الفرق الداخلية ومُورِّدي الدعم) أثناء وقوع أي حادث. راجع القسم 4-8 من إدارة الحوادث في معيار تأمين المعلومات الوطنية.
   (ب) إنشاء اتصال مع الوكالة الوطنية للأمن السيبراني ووكالات تطبيق القانون ومزود خدمة الإنترنت الخاص بك.
1. تسجيل أي حادث يتعلق بأمن المعلومات (خرق أو نشاط يتعلق بالجرائم السيبرانية) داخليًا وكذلك المتعلق بالوكالة الوطنية للأمن السيبراني ووكالات تطبيق القانون (وزارة الداخلية).
2. إبلاغ الوكالة الوطنية للأمن السيبراني عن الحوادث بالاتصال على الخط الساخن 16555 أو إرسال بريد إلكتروني إلى ncsoc@ncsa.gov.qa

4.3 مستخدمي شبكات الواي-فاي العامة

4.3.1 العادات الأمنية السليمة

1. لا تستخدم الأجهزة القديمة وغير المحدثة التي قد تكون ضعيفة ولم يتم تحديثها بشكل كافٍ للاتصال بشبكات الواي-فاي العامة.
2. لا تترك الجهاز متصل بشبكة الواي-فاي أو البلوتوث عند عدم استخدامه.
3. لا تترك شبكة الواي-فاي على خاصية الاتصال التلقائي بالشبكات
4. تجنب استخدام شبكة واي-فاي مفتوحة غير محمية بكلمة مرور.
5. لا تشارك اسم المستخدم / كلمة المرور أو جهازك المحمول لتلقي رموز الأمان الخاصة بالوصول إلى شبكات الواي-فاي العامة مع أي شخص بما في ذلك الأصدقاء.
6. لا تدخل إلى مواقع الويب التي تحتفظ بمعلوماتك الحساسة، مثل الواقع المتعلقة بالخدمات المالية أو الرعاية الصحية أثناء الاتصال بشبكة الواي-فاي العامة. وفي حالة الحاجة إلى الدخول:
   (أ) يفضل استخدام خدمة 3G / 4G / 5G الخاصة بمشغل شبكة الجوال بدلاً من نقاط اتصال شبكة الواي-فاي العامة.
   (ب) لا تقم بتسجيل الدخول إلى أي حساب من خلال تطبيق جوال، ولكن انتقل إلى موقع الويب بدلاً من ذلك وتحقق من أنه يستخدم HTTPS (بروتوكول نقل النص الفائق الآمن) قبل تسجيل الدخول.
   (ج) اتصل من خلال شبكة خاصة افتراضية VPN.
   (د) تسجيل الخروج من الحسابات عند الانتهاء من استخدامها.
7. أثناء إجراء الاتصال أو الاتصال بالفعل بشبكة الواي-فاي العامة:
   (أ) حاول التحقق مما إذا كان اتصالاً لاسلكيًا شرعيًا. تحقق من معرف مجموعة الخدمات قبل الاتصال، حيث قد يقوم المستخدمون المخادعين بإعداد نقطة وصول مخترقة لاسلكية خادعة عن قصد بأسماء مثل المقاهي الشهيرة أو الفنادق أو الأماكن التي توفر خدمة الواي فاي المجانية.
   (ب) تعطيل مشاركة الملفات على الكمبيوتر المحلي.
   (ج) يوصى باستخدام أجهزتك الشخصية مثل الهواتف المحمولة والأجهزة اللوحية أثناء الوصول إلى أي مواقع ويب تقوم بتخزين أو طلب إدخال أي معلومات حساسة وقد يكون من المفيد الوصول إلى مثل هذه المواقع الحساسة عبر شبكة هاتفك المحمول، بدلاً من اتصال بشبكة الواي-فاي العام.
   (د) تجنب استخدام المحطات الطرفية العامة / المشتركة للوصول إلى أي مواقع ويب تتطلب إدخال أي معلومات حساسة.
   (ه) أثناء استخدام المحطات الطرفية العامة / المشتركة، تأكد من تسجيل الخروج من كل بوابة قمت بتسجيل الدخول إليها. إحذف محفوظات الاستعراض واحذف ذاكرة الويب المؤقتة قبل مغادرة المحطة.

5 الامتثال والإنفاذ

5.1 الامتثال والإنفاذ

تم نشر هذه المبادئ التوجيهية لمساعدة المؤسسات على فهم أفضل حول المخاطر التي تتعرض لها خدمة الواي فاي العامة والمخاطر المرتبطة باستخدامها.

المبادئ التوجيهية تكمل معيار تأمين المعلومات الوطنية وسياسة تصنيف البيانات الوطنية.

6 ملحق (سياسة الاستخدام العادل)

فيما يلي قائمة بالمناطق التي سيتم تغطيتها في سياسة الاستخدام العادل فيما يخص شبكات الواي-فاي العامة أو الخاصة بالضيف، ويُطلب من مستخدمي الواي-فاي القراءة والموافقة من أجل الاتصال بالإنترنت عبر شبكتك:

1. عدم استخدام الخدمة للأنشطة التي تنتهك خصوصية الآخرين على سبيل المثال إرسال بريد عشوائي والتعدي على الخصوصية بإرسال رسائل غير مرغوب فيها أو رسائل تجارية.
2. عدم الانخراط في أي نشاط ينتهك حقوق الملكية الفكرية للآخرين، بما في ذلك براءات الاختراع وحقوق النشر والعلامات التجارية وما إلى غير ذلك.
3. الوصول إلى حسابات أو معدات أو شبكات بشكل غير قانوني أو بدون تصريح تابع لطرف آخر أو محاولة اختراق الإجراءات الأمنية لنظام آخر (مثل مسح المنفذ والمسح الخفي وما إلى ذلك).
4. استخدام الخدمة بما يخالف قوانين وأنظمة دولة قطر.
5. الدخول إلى المواقع المحظورة أو غير القانونية (مثل المقامرة عبر الإنترنت والمواقع الإباحية).
6. الرجوع إلى عمليات النطاق الترددي العالي مثل عمليات نقل الملفات الكبيرة
7. استخدام الخدمة لنقل، أو نشر، أو تحميل، أو إتاحة لغة أو مواد تشهيرية أو مزعجة أو مسيئة أو تهديدية تشجع على الأذى الجسدي أو تدمير الممتلكات.
8. الإشارة إلى توزيع الملفات الضارة (مثل فيروسات الإنترنت وأحصنة طروادة)

7 المرفقات

7.1 الاختصارات

APT تهديد مستمر متقدم

DDoS هجمات حجب الخدمة الموزعة

ISP مزود خدمة الإنترنت

NCSA الوكالة الوطنية للأمن السيبراني

7.2 المراجع

لا توجد مراجع

7.3 قائمة الأشكال

لا يوجد رسومات توضيحية

7.4 الإبلاغ عن الحوادث إلى الوكالة الوطنية للأمن السيبراني

يمكن للمؤسسات التي تواجه هجوم حجب الخدمة الموزعة إبلاغ الوكالة الوطنية للأمن السيبراني عن الحادث بإحدى الطرق التالية:

الاتصال بالخط الساخن الخاص بالوكالة الوطنية للأمن السيبراني على رقم 16555 (خدمة على مدار الساعة طوال أيام الأسبوع)

إرسال بريد الإلكتروني على البريد الالكتروني الخاص بالوكالة الوطنية للأمن السيبراني ncsoc@ncsa.gov.qa

قد تجد المؤسسات أيضًا الإرشادات التالية مفيدة في الاستعداد لمواجهة أي هجوم / حادث.

إرشادات لإدارة الحوادث - الإجراءات المطلوبة مسبقًا