الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

الأمن السبراني .. يُسافر معك



© LibyaCERT

www.nissa.gov.ly
www.facebook.com/nissa.libya

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

أُسست الهيئة الوطنية لأمن وسلامة المعلومات بموجب قرار مجلس الوزراء رقم (28) لسنة 2013 ميلادي، والذي ينص على أن هدف الهيئة هو توفير السياسات والمعايير الاستراتيجية اللازمة من أجل تأمين وسلامة البيانات الرقمية ووسائل وشبكات الاتصال، وكذلك توفير خدمات المصادقة الإلكترونية والتشفير إلى جانب وضع وتنفيذ آليات الاستجابة الفورية للحوادث المتعلقة بشؤون تكنولوجيا المعلومات والاتصالات، وكذلك الاهتمام بشؤون حوكمة الإنترنت ومجالاتها بالإضافة لدورها كمنسق رئيسي لجميع شؤون أمن وسلامة المعلومات والاتصالات على المستوى المحلي والدولي.
يمكنكم الحصول على المزيد من المعلومات عن الهيئة من خلال زيارة موقعها على شبكة الإنترنت: www.nissa.gov.ly

معلومات الاتصال:
العنوان: مبنى البريد – شارع الزاوية – طرابلس – ليبيا.
صندوق بريـــد: 83388
هـــــاتف: 218213614127 +
فـــــاكس: 218213614277 +
البريد الإلكتروني: info@nissa.gov.ly

نصائح الأمن السبراني للمسافرين

قد يعتقد البعض أن الأمن **السبراني*** أمر متعلق فقط بالتواجد في المنزل أو المكتب أو الفصل الدراسي . . والواقع أنه من المهم أن نتحلى بالسلوك الآمن عند استخدام التقنية أينما سافرنا . . فكلما سافرنا واتصلنا بالانترنت عبر رحلاتنا . . كلما زادت المخاطر والتهديدات السبرانية التي تواجهنا . . لا أحد في مأمن من أن يكون ضحية لجريمة إلكترونية سواءً في المنزل أو في السفر . . ولكن اتباع النصائح البسيطة التالية يبقيك أكثر أمناً.

*"الفضاء **السبراني** هو فضاء التواصل من خلال الربط بين مجموعة من العناصر كأجهزة الكمبيوتر وأنظمة الشبكات والبرمجيات وحوسبة المعلومات ونقل وتخزين البيانات والأهم من ذلك كله مستخدم كل هذه العناصر.. الإنسان".

قبل أن تذهب

قم بتحديث برمجيات هاتفك الذكي

تعامل مع هاتفك الذكي كما تتعامل مع حاسوبك في العمل أو في المنزل، قم بتحديث برمجيات أنظمة التشغيل والتطبيقات وبرامج مكافحة الفيروسات بشكلٍ دائمٍ وخصوصاً قبل السفر، الأمر الذي سيُحسّن من قدرته الدفاعية ضد البرمجيات الخبيثة.

احذف سجل النشاطات السابقة

امسح محفوظات متصفحات الانترنت وغيرها من المعلومات المخزّنة الناتجة عن استخدامك للجهاز، والتي يمكن أن يُساء استخدامها ، كما يفضل أن تحذف التطبيقات والبرامج الغير ضرورية.

أمن جهازك برمز مرور

تعوّد على أن تؤمن جهازك باستخدم رمز دخول وكلمات مرور صعبة التخمين عندما لا تستعمله . . حتى ولو غبت عنه لدقائق قليلة . . فتلك الدقائق تعتبر وقتاً كافياً ليسرق فيها شخص ما معلوماتك أو يتلفها.

انسخ معلوماتك احتياطياً

انسخ من باب الاحتياط جهات الاتصال الخاصة بك، وصورك ومقاطعك المرئية وغيرها من بيانات جهازك إلى جهاز آخر أو إلى خدمة سحابية.

عندما تصل وجهتك

أوقف الاتصال التلقائي

عطّل إمكانية الاتصال بالشبكات اللاسلكية (wifi) وتقنية البلوتوث التلقائي، فبعض الأجهزة تبحث وتتصل بشكل آلي بالشبكات المتاحة، والبلوتوث يمكّن الجهاز من الاتصال تلقائياً بالأجهزة الأخرى كسماعة الرأس أو أنظمة الترفيه بالسيارات، قم بتعطيل تلك الميزات لكي لا تتصل إلا إذا أردت ذلك.

فكّر قبل أن تتصل بالشبكة

قبل أن تتصل بأي نقطة توصيل لاسلكية في المطار أو الفندق أو المقهى، تأكّد من اسم الشبكة ومن أنها فعلاً تخص ذلك المكان، تأكّد كذلك من دقة إجراءات تسجيل الدخول من موظفي تلك الأماكن . . ولا تقم بإجراء أي أنشطة تحوي معلومات حساسة . . كالتسوق عبر الانترنت أو الأعمال المصرفية عبر شبكة لاسلكية عامة، واستخدم فقط المواقع التي تبدأ بـ "https://" لإجراء تلك الأنشطة . . وعادةً ما يكون استخدام اتصال شبكة الجوّال أكثر أمانًا من استخدام شبكة لاسلكية عامة.

فكّر قبل النقر

توخى الحذر عند التحميل من / أو النقر على أي روابط غير معروفة، وخاصة تلك التي تصل عبر تطبيقات المراسلة الفورية والبريد الإلكتروني، قم بحذف الرسائل المشبوهة أو تلك التي تأتيك من مصادر مجهولة، راجع واقرأ بتمعن تفاصيل وصلاحيات أي تطبيق قبل تثبيته.

احمِ جهازك

لمنع السرقة أو الوصول الغير مصرح به أو فقدان بياناتك الحساسة لا تترك جهازك دون رقابة مطلقاً – بما في ذلك أجهزة التخزين الخارجية USB – في مكان عام . . حافظ على أجهزتك مؤمنة في سيارات الأجرة وفي المطارات وفي الطائرات وحتى في غرفة الفندق.

قم بالحد من إمكانية تتبع موقعك

من الشائع جدًا للمسافرين مشاركة أماكن تواجدهم عبر مواقع التواصل الاجتماعي أثناء تنقلهم في الخارج، إلا أن هذا النوع من المشاركة "المفرطة" قد تخلق تهديدًا لك، لذا فالحد من المعلومات التي تنشرها عبر الإنترنت حول أماكن تواجدك تقلّل احتمالات تعرضك وممتلكاتك الشخصية للتهديد.

تهديدات شائعة عند السفر

شبكات لاسلكية غير آمنة

رغم أن الشبكات اللاسلكية العامة توفر لك سهولة الاتصال بالإنترنت من أي مكان تقريبًا، إلا أنها قد تكون غير آمنة، فتلك الشبكات يمكنها كذلك أن تسمح لمجرمي الإنترنت بالوصول إلى جهازك المتصل بها. وخاصة لتزايد انتشارها في أماكن أخرى غير تلك التي اعتدنا عليها.

أجهزة الكمبيوتر العامة

توفّر مراكز رجال الأعمال والمكتبات ومقاهي الانترنت أجهزة كمبيوتر يمكن لأي شخص استخدامها، ولكن لا يمكن لك كمسافر الوثوق في أنها آمنة. فالمشرفون عليها قد لا يقومون بتحديث أنظمة التشغيل أو برامج مكافحة الفيروسات في تلك الأجهزة بشكل مستمر. ومن المحتمل أن تكون مصابة ببرمجيات خبيثة . . وأحد الأمثلة على ذلك استخدام برمجية يمكن للمجرمين من خلالها تلقي معلومات شخصية عن المستخدمين مثل الاسم وأرقام بطاقات الائتمان وتواريخ الميلاد وكلمات المرور . . كما عليك تجنب شحن جهازك بوصلات شحن غير آمنة كتلك الموجودة في غرف الفنادق.

التعرض لسرقة الجهاز

غالبًا ما يتم استهداف المسافرين من قبل اللصوص، بحثاً عن فرص لسرقة أجهزة الكمبيوتر المحمولة أو الهواتف الذكية المتروكة دون رقيب، إذا كنت تحضر مؤتمرًا أو معرضاً تجارياً، كُن حذراً بشكل خاص، فهذه الأنشطة تقدم للصوص فرصاً متنوعة لسرقة الأجهزة التي يحتمل أن تحتوي على معلومات حساسة.