ما هي السلامة الرقمية ولماذا يجب علينا الاهتمام بها؟

- الأمان الرقمي او السيبراني هو الخطوات اللي نقوم بها لحماية هويتنا وممتلكاتنا الرقمية. وهو حماية الأنظمة المتصلة بالإنترنت، عبر مجموعة من التقنيات والعمليات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به. يتضمن هذا الشيء حماية البيانات مثل ملفاتنا الخاصة، صورنا، معلوماتنا الشخصية، مراسلاتنا الخاصة، او معلومات خاصة بالمؤسسة التي نعمل لديها او اسرار خاصة بالعمل، جميع هذه الأمور وكثير غيرها يجب حمايتها من الهجوم أو التلف أو الوصول غير المصرح به.

- يوجد أنواع مختلفة من تهديدات الأمن السيبراني، مثل الفيروسات والبرامج الضارة وهجمات برامج الفدية والتصيد الاحتيالي... يمكن استخدام هذه التهديدات لسرقة معلومات حساسة، أو تعطيل البنية التحتية الخاصة بشركة او حتى مدينة او دولة معينة، أو تشفير كامل الملفات على جهاز معين او مجموعة من الاجهزة واستخدامهم كرهينة لإجبار الأشخاص او المؤسسات على دفع فدية وهذا الشي معروف بـ Ransomware.
- لمكافحة هذه التهديدات، تستخدم المنظمات والأفراد مجموعة من تدابير الأمن السيبراني، مثل جدران الحماية Firewall وبرامج مكافحة الفيروسات والتشفير وامور كثيرة مختلفة. تساعد هذه الإجراءات على منع او التخفيف من حوادث الأمن السيبراني واكتشافها في وقت مبكر وتقليل الضرر.
- بالإضافة للتدابير التقنية، يتضمن الأمن السيبراني ايضاً ممارسات مثل التدريب على التعرف على التهديدات المحتملة وتجنبها، بالإضافة لوضع وتطوير سياسات وإجراءات لحماية البيانات والأنظمة الحساسة.
- بشكل عام، يعد الأمن السيبراني امر مهم بعالمنا المترابط بشكل متزايد، ومن المهم أن تقوم المنظمات والأفراد بخطوات للحماية من التهديدات المحتملة.

- الامن السيبراني مؤلف من عدة طبقات، كلما قمنا بتطبيق واحدة من تدابير وممارسات الامن السيبراني كلما رفعنا مستوى الحماية على اجهزتنا وبيناتنا، ويصبح الامر أصعب على الهاكر وأكثر كلفة من الناحية المالية والوقت.

- الأمان الرقمي أصبح امر مهم جداً، لأننا أصبحنا نستخدم الكثير من الاجهزة الالكترونية وصار معظم تواصلنا عبر الانترنت، ونحن نحتفظ بكمية كبيرة من البيانات المهمة والحساسة على اجهزتنا وحساباتنا وضمن التطبيقات التي نستخدمها.

- ويصبح الأمر مهم أكثر إذا كنا نعمل على أمور قد تشكل خطورة على حياة اشخاص او خسارة مادية كبيرة. مثلاً (أبحاث لإنتاج دواء جديد لمرض مستعصي) او مواضيع حساسة مثلاً (كشف اختلاس)، او العمل مع اشخاص مستضعفين او مضطهدين مثلاً (العمال الأجانب، والمثلية الجنسية، او اللاجئين).

- يوجد ايضاً برامج تجسس متطورة وخطيرة مثل Pegasus أو FinFisher، هذه البرامج خطيرة جداً وقد تمكن الهاكر من اختراق الأجهزة والتحكم بها بشكل كامل، أي أنهم يستطيعون الوصول الى كل شيء داخل الجهاز المخترق: مثل جهات الاتصال والصور وقراءة الدردشة والاستماع للمكالمات وتشغيل الكاميرا والميكروفون...

بعض الامثلة:

- مثلاً في بعض الدول يتم إيقاف بعض الأشخاص عند نقاط التفتيش أو على الحدود ويطلبوا منهم فتح الهاتف المحمول للتحقق من بعض المعلومات.
- او مثلاً وقت نقوم بزيارة مكتب معين، ويطلبوا منا ترك الهاتف المحمول مع الموظفين عند المدخل.

- مثل آخر: السنة الماضية قامت آنسة من سوريا بإرسال هاتفها المحمول بعد أن تعطل للتصليح بأحد المتاجر في منطقة سكنها. فقام الموظف في هذا المتجر بسرقة صورها الخاصة التي تظهر بها بدون حجاب وقام بنشر هذه الصور على الانترنت. وهذا العمل تسبب بمشكلة للآنسة مع عائلتها. وبعد هذه الحادثة بأيام للأسف قام أحد اقاربها بقتلها بسبب تلك الصور.

طرق الاختراق عديدة، وكذلك وسائل الحماية متوفرة وليست صعبة. المطلوب منا نحن ان نأخذ الامر بجدية ونطبق الأمور التي سوف نناقشها اليوم. ولكن هذا الشيء غير كافي لأنه لدينا ساعة واحدة فقط وهذا غير كافي للتكلم بالتفصيل في بعض هذه الأمور. هذه الجلسة هي للفت نظركم واثارة اهتمامكم والمطلوب منكم ان تتابعوا بعد ذلك. سوف نعطيكم بعض المصادر للمتابعة ومن السهل إيجاد الكثير من المعلومات والفيديوهات عن المواضيع التي سنناقشها او طريقة استخدام بعض البرامج التي قد نذكرها.

امثلة عن طرق الاختراق:

التصيد Phishing:

قد تحدث عندما نتلقى رسالة نصية في الهاتف SMS او رسالة عبر وسائل التواصل الاجتماعي كفيسبوك، تويتر، واتساب او غيرهم، قد تتضمن هذه الرسالة رابط او مرفقات خبيثة، كما يمكن ان تكون اتصال هاتفي حيث يطلب المتصل بعض المعلومات التي قد تساعده في عملية الاختراق. او في حال فتحنا الرابط الموجود في الرسالة فقد يؤدي الى صفحة مزورة او يطلب معلومات قد تساعده في عملية الاختراق، مثلاً قد يفتح الرابط صفحة مزورة لموقع فيسبوك ففي حال أدخلت اسم المستخدم وكلمة السر سوف يتمكن المخترق من سرقة حسابي على فيسبوك. اوقد يطلب معلومات عن حسابي البنكي او معلومات عن الشركة او المنظمة التي اعمل بها ليتمكنوا من اختراقهم.

فلذلك يجب ان أكون حذر جداً عند تلقي رسالة او اتصال من اشخاص او ارقام مجهولة، خاصتاً إذا كانت هذه الرسالة تتضمن ملف او رابط والمطلوب ان أقوم بفتحهم. وعادتاً يستخدمون عامل الضرورة ويحثون الضحية على التصرف بسرعة، او يستخدمون السلطة كأن يذكر انه مدير الشركة او مدير من الفرع الرئيسي ويجب عليك ان تتصرف مباشرتاً وإن لم تفعل سوف يتم طردك من العمل او خصم مبلغ من راتبك. او ان يتظاهر بانه يتواصل معكم من المصرف وانه يوجد حركة غريبة في حسابكم، وللتأكد من هويتكم عليكم الإجابة على بعض الأسئلة مثل رقم الحساب، تاريخ الميلاد، كلمة السر...

التصيد منتشر ومستخدم بكثرة من قبل الهاكرز وهو شيء خطير، قد يكون التصيد هو الهجوم بحد ذاته مثلاً لاختراق حساب معين، او قد يكون خطوة البداية لاختراق كبير، مثلاً اختراق حساب موظف لاستخدامه في اختراق المؤسسة بالكامل.

تخمين كلمات السر:

استخدام كلمات سر ضعيفة يسهل الامر على الهاكرز لتخمين ومعرفة كلمة السر. سوف نتكلم لاحقاً بالتفصيل عن كلمات السر وبرامج ادارت كلمات السر.

الفيروسات:

يجب التنبه وحماية اجهزتنا من الفيروسات. ومن الضروري استخدام برنامج مكافح الفيروسات على اجهزتنا والتأكد من أنه يقوم بتحديث قاعدة البيانات الخاصة به. وعدم استخدام البرامج المقرصنة لأنها اغلب الأوقات تتضمن فيروسات. وتحميل البرامج من موقعها الأصلي فقط.

الهندسة الاجتماعية:

الهندسة الاجتماعية مستخدمة بشكل كبير جداً من قبل الهاكرز. بكل بساطة الهندسة الاجتماعية هي الاحتيال، حيث يقوم الهاكر بالاحتيال على المستخدم لعمل شيء معين لم يكن يرغب اساساً في عمله، او جعله يفصح عن معلومات كان عليه ان يبقيها سرية. او بان يقوم الهاكر بجمع جميع المعلومات المتوفرة على الانترنت عن شخص يود اختراق اجهزته او حساباته، ويستخدم هذه المعلومات للتقرب وبناء الثقة واضفاء الإحساس بوجود أشياء وهوايات مشتركة مما يسهل عملية الاحتيال على هذا الشخص.

هذه بعض الأمثلة عن التصيد:

كما تشاهدون في هذه الأمثلة، الهاكر يحاول ان يستغل تعاطف الأشخاص مع الموقوفين ويتلاعب بالكلام ليحثهم على فتح الرابط.

- لذلك يجب تجاهل هذا النوع من الرسائل وعدم فتح الروابط التي تتضمنها.
- التحقق مع الشخص المرسل إذا كان هو قد أرسل الرسالة.
- التحقق من عنوان المرسل.
- التحقق من الروابط.
- التحقق من الأخطاء الاملائية في نص الرسالة.
- عادتاً رسائل التصيد تستخدم تحية عامة وليس شخصية.

سوف أقوم بإرسال رابط لموقع من شركة غوغل للتدرب على كيفية اكتشاف هجمات التصيد.

https://phishingquiz.withgoogle.com/

سوف أعرض عليكم رسالة تصيد وعليكم اكتشاف علامات التصيد في هذا البريد الالكتروني. الرجاء كتابة الإجابات في الدردشة.

- العنوان هو .com وليس .org
- استخدام عامل الطوارئ، السلطة وضرورة السرعة في الإجابة.
- يجب علينا التحقق من الرابط عبر تمرير المؤشر فوق الرابط دون الضغط عليه.

- يوجد أخطاء املائية.
- لم يستخدموا اسم المرسل في توقيع الرسالة.

هذه امثلة إضافية عن صفحات مزورة. كما تلاحظون يجب دائماً التحقق من الرابط، وعادتاً إذا كان موقع فيسبوك مثلاً فتوح لدي في المتصفح وبعد فتح الرابط ظهرة صفحة فيسبوك جديدة وتطلب مني تسجيل الدخول فهذا يعني بأن هذه الصفحة مزورة.

سوف نتكلم الان عن كلمات السر:

من الضروري استخدام كلمات سر جيدة طويلة ومعقدة لحماية حساباتنا. كلمات السّر يجب أن تكون:

- طويلة: مؤلفة من 14 حرف على الأقل.
- معقدة: أي أن تتضمن ارقام واحرف صغيرة وكبيرة ونقاط والحروف الخاصة مثل ؟!/
- عشوائية: أي لا نستخدم نمط معين لتأليف كلمات السر، مثلاً: marhabagmail marhabatwitter
- غير شخصية: يجب الا استخدم اسمي، تاريخ ميلادي، رقم هاتفي.
- يجب أن تكون سهلة الحفظ: لكي لا نخسر الوصول الى حساباتنا.
- سرية: لا نشاركها مع أحد.
- لا نكتبها على ورقة ولا في ملفات على الكمبيوتر.
- فريدة: يجب ان نستخدم كلمة سر خاصة بكل حساب.

هذه امثلة عن مدة الوقت الذي يستغرقه الهاكر لتخمين كلمة السر، ولماذا من المهم أن تكون طويلة ومعقدة: مثلاً: إذا استخدمنا كلمة سر مؤلفة من ارقام فقط يستطيع الهاكر تخمينها في بضع دقائق او ساعات. وكلما زاد عدد الاحرف والأرقام والرموز كلما صعب على الهاكر تخمين كلمة السر.

ما هي عبارة السر Passphrase ولماذا ننصح بها:

عبارة السر هي طريقة سهلة لتأليف كلمات سر طويلة وسهلة الحفظ. يجب أن تكون مؤلفة من 4 الى 5 كلمات عشوائية، او نستخدم عبارة تتضمن شيء غير منطقي.

مثلاً: No 1 want to break free!

فهذه عبارة سر طويلة تتضمن أحرف وأرقام وشيء غير منطقي وسهلة الحفظ.

1Banana2birds100friends!

هذه أربع كلمات عشوائية تتضمن أحرف وأرقام طويلة وسهلة الحفظ ايضاً.

من المستحسن استخدام كلمات سر بهذا الشكل، لأنها تعتبر آمنة، طويلة بشكل كافٍ، معقدة، وسهلة الحفظ.

- ما هو HTTPS وبماذا يختلف عن HTTP:

HTTPS هو النسخة الآمنة والاتصال مشفر مع الموقع الذي استخدمه. لذلك يجب دائماً التأكد قبل ادخال اسم المستخدم وكلمة السر بأن الموقع يستخدم HTTPS. لأن ذلك يعني أن الاتصال مشفر وإذا كان هناك من يراقب الانترنت لن يستطيع قراءة بياناتي.

- يجب عدم فتح حساباتي على أجهزة غريبة، فقط على جهازي الخاص. لأنه لا يمكنني معرفة ما إذا كان هذا الجهاز مخترق او عليه برامج تجسس.
- فهم طريقة استعادة كلمة السر:

عادتاً معظم المواقع تقدم طريقة لإعادة ضبط كلمة السر في حال نسيناها، ولكن معظم هذه الطرق تتضمن أسئلة قد تكون الإجابة عنها سهلة للهاكر او تتوفر معلومات عنها على الإنترنت. مثلاً تاريخ ميلادي، المدرسة التي تعلمت بها، اسم الحيوان الأليف وغيره... لذلك يجب أن ننتبه أي أسئلة وأي إجابات نختار كي لا يكون من السهل على الهاكر استخدام هذه الطريقة.

برامج إدارة وحفظ كلمات السر:

نحن ننصح باستخدام برنامج KeePassXC لأنه برنامج جيد، سهل الاستخدام، مفتوح المصدر، يحفظ كلمات السر في خزنة مشفرة مما يوفر امان جيد.

يمكنكم تحميل البرنامج من هذا الرابط www.keepassxc.org هو متوفر لنظام تشغيل ويندوز، ماك ولينكس.

عند استخدام البرنامج لأول مرة سوف يطلب منكم انشاء حاوية لحفظ كلمات السر داخلها. وسيطلب منكم كلمة سر لتشفير هذه الحاوية. كلمة السر هذه يجب أن تكون جيدة طويلة ويجب ألا ننساها ابداً، في حال فقدان كلمة السر لن يعود باستطاعتكم الوصول الى كلمات السر خاصة بكم، كل ما عليكم من الان هو حفظ كلمة سر واحدة فقط.

يمكنكم حفظ عدد غير محدود من البيانات داخل البرنامج. عند ادخال البيانات يمكنكم ادخال اسم المستخدم وكلمة السر ورابط الموقع الخاص بهذا الحساب، وملاحظات خاصة بهذا الحساب.

للدخول على الحساب نفتح دائماً الرابط الذي ادخلناه، بهذه الطريقة نضمن بأن الرابط آمن ونحمي أنفسنا من التصيد.

التحقق بخطوتين:

في حال تمكن الهاكر من معرفة اسم المستخدم وكلمة السر الخاصة بأحد حساباتنا فسيستطيع الدخول الى حسابنا. لكي نحمي حساباتنا بشكل أفضل معظم المواقع توفر طبقة حماية ثانية تسمى التحقق بخطوتين، عند تفعيل هذه الخدمة نضيف طبقة حماية جديدة على الحساب، فعند تسجيل الدخول من جهاز جديد لم استخدمه من قبل، بعد ادخال اسم المستخدم وكلمة السر سيطلب مني كود معين للسماح بالدخول للحساب. أي انني سأكون بحاجة لشيء ثالث لكي أتمكن من الدخول للحساب. هذا الشيء يمكن أن يكون كود يولد

ضمن تطبيق على الهاتف، او رسالة نصية تصلنا على هاتفنا، او اكواد احتياطية نستطيع الحصول عليها من داخل حسابنا، او مفتاح خاص بالتحقق بخطوتين... الكود صالح للاستخدام مرة واحدة فقط، والكود الذي نحصل عليه من التطبيق على الهاتف تولد ضمن التطبيق من دون الحاجة الى الانترنت وهو صالح لمدة دقيقة فقط. ويطلب مني التحقق بخطوتين مرة واحدة من المتصفح، عند تسجيل الدخول مرة جديدة من الجهاز نسفه وعلى نفس المتصفح فلن يطلب مني ذلك، في بعض الأحيان على اختيار ذلك عند تسجيل الدخول.

نستطيع تفعيل التحقق بخطوتين من خلال اعدادات الحساب، عند تفعيلها سيعطيني الخيار لاختار أي نوع من التحقق بخطوتين أفضل، نحن لا ننصح باستخدام الرسائل النصية لأنها غير آمنة كفاية. يجب عدم مشاركة الاكواد مع أحد وفي حال وصلتني رسالة او اتصال يطلب مني مشاركة الكود يجب تجاهل هذا الطلب.

من المستحسن تفعيل أكثر من طريقة للتحقق بخطوتين، مثلاً التطبيق على الهاتف والكود الاحتياطي، ام المفتاح مع التطبيق على الهاتف او الكود الاحتياطي...

الفيروسات:

يوجد العديد من أنواع البرامج الخبيثة اكثرها انتشاراً: Virus فيروس، Ransomware فيروس الفدية، Worm دودة، Trojan حصان طروادة، Keylogger مسجل نقرات المفاتيح، RAT أداة التحكم عن بعد، Rootkit الجذور الخفية، والعديد غيرهم.

جميع هذه الملفات الخبيثة خطيرة، ولكن اخطرها هو أداة التحكم عن بعد، إذ أنها تعطي الهاكر تحكم كامل بجهاز الضحية، فيستطيع استخدام الجهاز كأنه بحوزته، ويمكنه قراءة كل شيء وسرقة ملفات، تشغيل الكاميرا والميكروفون...

يجب أن نكون حزرين عند استخدام اجهزتنا والحفاظ عليها خالية من البرامج الخبيثة. ويجب علينا استخدام برنامج مكافح فيروسات لمساعدتنا على اكتشاف البرامج الخبيثة وازالتها. في حال ليس باستطاعتنا شراء برنامج مكافح فيروسات يمكننا استخدام النسخة المجانية فهي متوفرة من معظم شركات مكافح الفيروسات على أن يكون من شركة معروفة.

تصاب اجهزتنا بالبرمجيات الخبيثة عند تنصيب برامج غير اصلية واستخدام الباتش او الكراك لتفعيل البرامج المقرصنة، عند استخدام فلاشه مصابة ببرامج خبيثة، عند فتح ملحقات تتضمن برامج خبيثة، او فتح روابط خبيثة... ويجب عدم السماح لاحد باستخدام جهازنا. ومن الضروري دائماً تحديث نظام التشغيل والبرامج المستخدمة.

الهجمات المتقدمة:

الهجمات المتقدمة هي الهجمات التي تستخدم ثغرات غير معروفة من المطورين Zero day exploit. ويستخدم فيها برامج خبيثة متطورة مثل بيغازوس Pegasus وفينفيشر Finfisher وغيرهم، التي تمكنهم

من السيطرة على الجهاز بشكل كامل. هذه الهجمات مكلفة جداً وخطيرة وليس من السهل الحماية منها. وعادتاً يستهدف بها اشخاص محددين مسبقاً.

إذا كنتم تعتقدون انكم عرضة لهذا النوع من الهجوم عليكم اخذ اقصى درجات الحيطة والحذر. وتطبيق جميع النقاط التي ذكرناها سابقاً. كما ننصح باستخدام هاتفين واحد خاص للمكالمات الحساسة وعدم مشاركة رقمه مع احد، والطلب من الأشخاص الذين تتواصلون معهم عدم تسجيل الرقم لديهم. وتنصيب فقط التطبيقات التي نحتاجها فقط.

التواصل الآمن:

عند اختيار تطبيق للتواصل يجب أن نبحث عن التطبيقات التي تستخدم التشفير من طرف الى طرف End to End Encryption وأن يكون متوفر بشكل افتراضي أي انني لست بحاجة لتغيير أي شيء في الاعدادات لتفعيل التشفير. في هذا النوع من التشفير يتم التشفير على جهازي ويتم فك التشفير على جهاز الشخص الآخر، ولا تستطيع الشركة او أي شخص آخر قراءة الرسائل او التنصت على المحادثة.

نحن ننصح باستخدام تطبيق سيغنال، لأنه سهل الاستخدام وآمن جداً، يوفر التشفير من طرف الى طرف، وهو مفتوح المصدر، وقد تم التحقق من الكود البرمجية الخاصة به، وهو لا يخزن المحادثات، ويخزن المعلومات الوصفية لمدة قصيرة فقط، ويوفر خاصية المسح التلقائي للرسائل من طرفي جهة الاتصال.

تطبيق وير Wire هو تطبيق آخر جيد ننصح باستخدامه، لإنشاء حساب أنتم بحاجة لبريد الكتروني وهذا أمر جيد لأنه ليس عليكم مشاركة رقم هاتفكم مع جميع جهات الاتصل. ولديه تقريباً جميع مميزات تطبيق سيغنال.

واتساب جيد ويؤمن تشفير من طرف الى طرف ولكنه مملوك من قبل شركة فيسبوك، وهم يسجلون معلومات وصفية عديدة.

تطبيق مسنجر وتلغرام عليكم الدخول الى الاعدادات لتفعيل التشفير. ولا ننصح باستخدام هذا النوع من التطبيقات للمحادثات الآمنة لأنه قد ينسى الشخص تفعيل التشفير وقد لا يعرف بعض الأشخاص كيفية تفعيل التشفير.

التشفير من طرف الى طرف:

هو عندما اكتب رسالة او اجري اتصال يتم التشفير على جهازي ومن ثم يتم ارسال البيانات مشفرة الى الطرف الثاني. وتمر البيانات مشفرة عبر مخدمات الشركة المالكة للتطبيق ويتم فك التشفير على هاتف المتلقي وعندها يستطيع قراءة او سماع الرسالة. بهذه الطريقة لا يستطيع أحد آخر غير طرفي الاتصال من قراءة او الاستماع للمحادثة، واي شخص آخر بين طرفي الاتصال يراقب الانترنت سوف يرى فقط معلومات مشفرة تمر ولن يستطيع التنصت.

ما هو وضع التأمين في الأندرويد Lockdown Mode:

هذه الخاصية متوفرة في العديد من الهواتف التي تستخدم نظام تشغيل اندرويد 9 والاصدارات اللاحقة له.

لتفعيل هذه الخاصية نقوم بالضغط على زر تشغيل الهاتف لثواني فتظهر لدينا عدة خيارات من بينها خيار وضع التأمين. إذا لم يكن هذا الخيار متوفر قد يتوجب عليكم تفعيله من الإعدادات.

بعد تفعيل خاصية وضع التأمين لن تعود تظهر الإشعارات على الشاشة. ولن يعود بالإمكان فتح الهاتف إلا باستخدام كلمة السر او الرمز او النمط وسيتم تعطيل إمكانية فتح الهاتف بواسطة البصمة والوجه والطرق الأخرى.

وعند تفعيل خاصية وضع التأمين فهي تعمل حتى يتم فتح الجهاز بعد ذلك يعود الجهاز للعمل بشكل عادي. إذا كنت ارغب في إعادة تفعيل وضع التأمين فعلي إعادة تفعيله من جديد.

ما هو وضع التأمين في الايفون Lockdown Mode:

خصائص هذه الميزة تختلف كلياً في هاتف ايفون عن هاتف اندرويد.

وضع التأمين لدى شركة أبل متوفر لأجهزة ايفون التي تعمل بنظام تشغيل IOs 16 وأجهزة الايباد التي تعمل بنظام تشغيل iPad OS 16 وعلى أجهزة كمبيوتر أبل التي تعمل بنظام تشغيل Ventura.

عند تفعيل خاصية وضع التأمين على أجهزة ماك سوف يتم حصر دردشة تطبيق iMessage على ارسال وتلقي الرسائل النصية والصور فقط، لن يعود بالإمكان اجراء مكالمات صوتية او فيديو او ارسال وتلقي أي نوع آخر من المرفقات.

سيتمكن فقط الأشخاص الموجودون في جهات الاتصال لديكم من التواصل معكم عبر FaceTime وiMessage. ولن يتم استقبال اتصالات عبر هذا التطبيق من ارقام مجهولة.

وسوف يتم حظر بعض الميزات في متصفح سفاري، لتعزيز الحماية، مما قد يؤدي الى توقف عمل بعض المواقع كالمعتاد او بشكل كامل.

وإذا كان هاتفكم مقفلاً، فلن يتفاعل مع الأجهزة الأخرى إذا تم توصيله عبر كابل.

روابط لمصادر إضافية:

- (NDI | CyberSecurity Handbook (cyberhandbook.org
- NDI's Practical Cybersecurity for Organizations Online Course
- Surveillance Self-Defense
- Security Planner