دليل الحماية الشامل

جميل حسين طويله

دليل الحماية الشامل

هل تتطلع للحصول على دليل شامل لنصائح الحماية التي يمكنك بالفعل تطبيقها لحماية نفسك وأفراد عائلتك على شبكة الانترنت

في هذا الدليل الشامل سنقدم لك أكثر من مئة نصيحة حول الأمن السيبراني يمكنك من خلالها زيادة الحماية الخاصة بك على شبكة الانترنت وكل هذه النصائح هي مجانية وقابلة للتطبيق، كل ما يتطلبه الأمر منك هو قضاء بعض الوقت لقراءة هذه النصائح وأخذها على محمل الجد وتطبيقها

النصيحة رقم 1: كيف تكون واقعياً بخصوص وجودك على شبكة الانترنت

يجب أن تدرك بأنك هدف جذاب لمجرمي الانترنت بسبب أموالك وبياناتك (قوائم الأسماء وكلمات السر والمستندات ورسائل البريد الالكتروني ...) سيتم استهدافك لسرقة هذه المعلومات.

مجرمو الانترنت قد قاموا بأتمتة معظم هجماتهم وما هي إلا مسألة وقت ليصل الضرر لك لذلك لا تقل ابدأ: " لا يمكن أن يتم اختراقي" أو "لن يحدث هذا الأمر لي"

النصيحة رقم 2: التسوق الآمن عبر الانترنت

التسوق الآمن عبر الانترنت أمر مهم جداً لذلك يجب أن لا تقوم بعمليات الشراء من جهاز لا تملكه أو من خلال اتصالك عبر شبكة عامة أو شبكة غير موثوقة ويجب أن

تعرف بأنه يمكن لمجرمي الانترنت الحصول على بياناتك وسرقة معلومات بطاقة الائتمان الخاصة بك واستخدامها للقيام بعمليات شراء وسرقة أموالك لذلك اتبع النصائح التالية:

- تأكد من أن الشبكة التي تستخدمها هي شبكة آمنة
- استخدم كلمات سر قوية
- تأكد من المواقع التي تشتري منها أن تكون مواقع موثوقة
- لا تقم ابداً بحفظ تفاصيل بطاقتك في حساباتك في مواقع الشراء
- تحقق من معاملاتك المالية بشكل يومي للتأكد من عدم وجود أي تحويلات أو نشاط غريب

هل ترغب بالتوسع أكثر والحصول على نصائح أكثر حول هذا الموضوع؟ يمكنك قراءة دليل "التسوق الآمن عبر الانترنت"

النصيحة رقم 3: أنتبه من الذواكر المحمولة USB

انتبه لما تقوم بتوصيله بجهازك، يمكن أن تحوي الذواكر المحمولة على برمجيات خبيثة تصيب جهازك وتؤدي لاختراقه وسرقة معلوماتك الحساسة

النصيحة رقم 4: انتبه لطلبات الصداقة

أصدقائك على الفيسبوك هل هم أصدقاء حقيقيون أم أعداء

غالباً من يقوم مجرمو الانترنت بإنشاء حسابات مزورة على مواقع التواصل الاجتماعي لتكوين صداقة مع الضحايا والبدء بجمع المعلومات او تنفيذ الهجمات لذلك كن حذراً من طلبات الصداقة التي تقبلها ولا تثق بأي صديق على مواقع التواصل الاجتماعي إلا إذا كنت تعرفه بالحياة الواقعية ومتأكد تماماً انه صاحب هذا الحساب

النصيحة رقم 5: حماية كلمات السر في الحياة الواقعية

من ينظر من خلف كتفك أثناء ادخالك لكمة السر؟ هل تعلم أن يمكن للمارة أو زملاء العمل استراق النظر لسرقة كلمة السر الخاصة بك

لا تستخدم كلمات سر بسيطة قابلة للتخمين مثل 123456 ولا تستخدم كلمات سر تحوي على معلوماتك الشخصية كرقم موبايلك أو تاريخ ميلادك وتأكد من عدم مشاركة كلمات السر الخاصة بك مع أي شخص آخر

النصيحة رقم 6: استخدم مضاد فيروسات

ممكن أن تسأل السؤال التالي: هل مازلت بحاجة لاستخدام مضاد فيروسات

الإجابة هي نعم

اختر مضاد فيروسات قوي وقم بتحديثه بشكل دوري، مضاد الفيروسات ضروري للحماية ولكنه غير كافي لتامين الحماية الكاملة للمزيد من المعلومات عن مضادات الفيروسات يمكنك الاطلاع على دليل "كيف اختار أفضل مضاد فيروسات"

النصيحة رقم 7: فعل المصادقة الثنائية

استخدم المصادقة الثنائية في كل مكان تكون متاحة به وقم بإعدادها لتتلقى رمز المصادقة عبر رسالة SMS أو عبر تطبيق خاص لهذه العملية هذا الأمر سيؤمن لك طبقة حماية إضافية وسيمنع المهاجم من الوصول لحسابك حتى لو تمكن من الحصول على كلمة السر الخاصة بك

النصيحة رقم 8: راقب حساباتك المصرفية

تحقق دائماً من كشوفات وتقارير حسابك المصرفي وابحث عن أي نشاط مشبوه وإن وجد قم بالتواصل مع البنك الذي تتعامل معه وقم بتغيير كل كلمات السر المتعلقة بهذا الحساب وتأكد من تطبيق كل إجراءات وطرق الحماية الممكنة

نصيحة رقم 9: لا تترك جهازك مفتوح

لا تترك جهازك الحاسب المحمول او جهازك الموبايل بدون قفل أثناء غيابك ولا تجعل الوصول لأجهزتك أمر متاح وسهل وتأكد من منع ذلك من خلال استخدام كلمة سر قوية لتقييد الوصول لأجهزتك

نصيحة رقم 10: رتب أولويات حساباتك الأكثر أهمية

إليك قائمة سريعة للقيام بذلك:

- البريد الالكتروني
- الخدمات المصرفية عبر الانترنت / PayPal
- مواقع التجارة الالكترونية التي تستخدمها
- أي حساب آخر أدخلت فيه تفاصيل بطاقتك الائتمانية
- أي حساب آخر يحوي عل معلوماتك الحساسة (رقم الضمان الاجتماعي – العنوان – رقم الهاتف)

قم بتامين كل هذه الحسابات بكلمات سر قوية مع استخدام المصادقة الثنائية وأجعل الوصول لها صعباً قدر الإمكان على أي آخر غيرك

النصيحة رقم 11: نظف خزانتك

إليك هذه النصيحة والتي تنطبق على الحياة الواقعية والحياة الافتراضية على شبكة الانترنت، نظف خزانة ملابسك وتطبيقاتك

قم بحذف التطبيقات التي لا تقوم باستخدامها، هذه التطبيقات من الممكن ان تحوي على ثغرات وبهذه العملية أنت تقلل من هذه الثغرات وبالتالي تقلل من احتمالية اختراق جهازك

النصيحة رقم 12: علاج الإدمان على الانترنت

ادمانك على مواقع الانترنت يمكن أن يدفعك لاستخدام أجهزة غير أجهزتك للوصول للمواقع عبر شبكة الانترنت وهذا الأمر يعتبر من وجهة نظر الحماية أمر سيء جداً فمن الممكن أن يكون هذا الجهاز مصاب ببرمجيات خبيثة من نوع keylogger والتي تعمل على تسجيل كل حرف يتم كتابته عبر لوحة المفاتيح وهذا الأمر ممكن أن يؤدي لوصول كلماتك السر لأيدي المهاجمين لذلك وببساطة التزم بأجهزتك الخاصة قدر الإمكان

النصيحة رقم 13: تتبع خطواتك الرقمية

قم بعملية جرد لبصمتك الرقمية وهذا الأمر يتم من خلال الخطوات التالية:

- قم بإعداد قائمة بحساباتك عبر الانترنت
- قم بتعيين كلمات سر قوية لهذه الحسابات
- احذف الحسابات التي لم تعد تستخدمها

النصيحة رقم 14: اتبع بعض الشك

لا بأس أن تتبع بعض الشك أثناء اتصالك بالإنترنت للحفاظ على سلامتك الرقمية من خلال الشك بكل شيء تشاهده (الشك بالروابط التي تصلك عبر البريد الالكتروني – الشك بالرسائل التي تحوي على مرفقات وقادمة من مصادر غير معروفة – الشك في الرسائل والإعلانات التي تعدك بشيء جيد لدرجة يصعب تصديقه) لذلك يجب أن تبتعد عن كل هذه الأمور

النصيحة رقم 15: الدوافع الخفية

غالباً ما ينشئ مجرمو الانترنت حسابات وهمية على مواقع العمل والتوظيف للوصول لتفاصيل حساباتك في هذه المواقع ويقومون بجمع المعلومات حول دراستك و أماكن عملك السابقة وأسماء زملائك بالعمل والعديد من المعلومات الأخرى لذلك تأكد من ملفاتهم الشخصية قبل قبول طلبات المتابعة او الاتصال

بعض الأمور المثيرة للشك والتي يجب أن تبحث عنها:

- معلومات عامة قليلة
- عدد قليل من الاتصالات
- الصور الغير حقيقية

النصيحة رقم 16: اتمتة عمليات التحديث للبرامج

هل تعلم بأن عملية تحديث البرامج يمكن أن تمنع 85% من الهجمات لأن هذه العملية تقوم بإصلاح الثغرات ونقاط الضعف القابلة للاستغلال من قبل المهاجمين وهذا الأمر هو أحد القواعد الأساسية في الأمن السيبراني، لذا حافظ على تحديث برامجك وأنظمتك بشكل دائم بدون أي استثناء وإن لم يكن لديك الوقت للقيام بذلك يمكنك استخدام تطبيقات تؤدي لك هذه المهمة بشكل اتوماتيكي

النصيحة رقم 17: عزز كلمات السر الخاصة بك

إحدى أكثر النصائح التي تحدثنا عنها هي كلمة السر القوية، تعتبر كلمات السر من أكثر المواضع الهامة في الأمن السيبراني لذلك سنعيد هذه النصائح وبشكل سريع:

- استخدم كلمة سر قوية (طويلة ومكونة من أحرف كبيرة وصغيرة وأرقام ورموز)
- لا تقوم باستخدام نفس كلمة السر ضمن أكثر من حساب
- لا تستخدم كلمات السر البسيطة القابلة للتخمين
- يمكنك استخدام تطبيق مدير كلمات السر لحفظ كلمات السر لحساباتك المختلفة

النصيحة رقم 18: احذر من هجمات الهندسة الاجتماعية

هجمات الهندسة الاجتماعية مستخدمة على نطاق واسع من قبل المهاجمين ويمكن تعريف الهندسة الاجتماعية على أنها فن التلاعب بالعقول البشرية وتتم عندما يقوم المهاجم بخداعك لتكشف عن معلوماتك الحساسة أو السرية او لتقوم بعمل ليس بمصلحتك، يمكن أن تتم هذه الهجمات في المنزل أو في العمل

- **في المنزل:** يمكن أن تتلقى اتصال أو رسالة من شخص يدعي أنه موظف في البنك الذي تتعامل معه ويطلب منك كلمة السر الخاصة بحسابك المصرفي لذا احذر من أن يتم خداعك بمثل هذا الأسلوب
- **في العمل:** تتلقى اتصال أو رسالة من شخص يدعي أنه المقاول الذي تتعامل معه الشركة ويطلب صلاحيات للوصول لنظام الشركة

في كلا الحالتين يجب أن تكون إجابتك هي "لا" تحقق من هوية المتصل ولا ترسل أي معلومات سرية يتم طلبها منك بهذه الطريقة

النصيحة رقم 19: برامج الفدية

تعتبر برامج الفدية ransomware من أكبر التهديدات السيبرانية الموجودة في يومنا الحالي على الأفراد وعلى الشركات

برامج الفدية هي نوع من البرمجيات الخبيثة وتعمل على تشفير ملفاتك ومنعك من الوصول لها وطلب مبلغ مالي كفدية للسماح لك بإعادة الوصول لملفاتك، تحدثنا في سابقاً عن طرق وإجراءات الحماية الخاصة بهذا النوع من الهجمات وسنعيد لك بعض النصائح بشكل سريع

للحماية نفسك من برامج الفدية، اتبع الأمور التالية:

- قم بعمليات النسخ الاحتياطي بشكل دوري واحفظ النسخ بعدة أماكن آمنة
- لا تحتفظ بالمعلومات والملفات المهمة على جهاز الحاسب فقط
- لا تقم بفتح مرفقات رسائل البريد الالكتروني القادمة لك من مصادر غير معروفة
- لا تقم بالنقر على الروابط المرسلة لك عبر رسائل البريد الالكتروني والقادمة لك من مصادر غير معروفة
- حافظ على تحديث نظام التشغيل وجميع البرامج والتطبيقات
- استخدم مضاد فيروسات قوي
- استخدم برامج الحماية من الجيل الجديد الخاصة بكشف ومنع البرمجيات الخبيثة

النصيحة رقم 20: تعتقد أنه لا يمكن اختراقك

معظم الأشخاص يقولون "أنا لست بحاجة إلى برامج الحماية لأنني لا اتصفح مواقع غير آمنة" في البداية يجب أن تدرك حقيقة أن المواقع الشرعية ممكن اختراقها أو ممكن أن تحوي على إعلانات خبيثة والعديد من الهجمات ممكن ان تتم بدون أي اجراء من المستخدم (كالنقر على رابط أو تحميل ملف) وحتى لو كنت خبيراً في الأمن السيبراني فلا يزال هناك العديد من الثغرات ونقاط الضعف التي يمكن للمهاجمين استغلالها للوصول لك وهذا الأمر يعود بنا إلى الحقيقة التي يجب أن تؤمن بها وهي "لا يوجد نظام آمن بشكل مطلق" ويمكننا تشبيه هذا الأمر بقيادة السيارة حتى لو كنت محترف في القيادة فما يزال هناك خطر محتمل من قبل الأشخاص الموجودين حولك إذا كنت تعتقد أنه لا يمكن اختراقك فاسمح لي أن أقول لك بأنك مخطئ (آسف لتفجير فقاعتك)

النصيحة رقم 21: هجمات التصيد الاحتيالي

مجرمو الانترنت مبدعون جداً في أساليبهم الخبيثة لنأخذ هجمات التصيد الاحتيالي phishing attack على سبيل المثال والتي تهدف إلى الحصول على معلومات المستخدمين (اسم المستخدم وكلمة السر وتفاصيل البطاقة البنكية والمعلومات الحساسة الأخرى) عن طريق انتحال هوية كيان جدير بالثقة فمن الممكن أن يتظاهر المهاجم على أنه البنك الذي تتعامل معه ويستخدم صفحات مزورة مشابهة تماماً لصفحات الموقع الرسمي للبنك

لتحافظ على أمانك اتبع الخطوات التالية:

- تطبيق التحديثات لأنظمة التشغيل والبرامج بشكل منتظم
- استخدام كلمات سر قوية
- مراجعة كشوف الحسابات البنكية بشكل دوري
- التحقق من عناوين البريد الالكتروني للرسائل الواردة لك

النصيحة 22: هل اتصالك بموقع الويب يتم من خلال https

كيف يمكنك معرفة فيما إذا كان الموقع الذي تتعامل معه وتدخل فيه معلوماتك الحساسة هو موقع آمن؟

يمكن التحقق من ذلك من خلال النظر إلى شريط العنوان في المتصفح إذا كان العنوان يبدأ ب https بدل من http فقط فهذا يعني أن الموقع يقدم طبقة حماية من خلال تشفير البيانات المتبادلة معه وهذا الأمر يمنع عمليات التنصت على قناة الاتصال

إذا كان الموقع لا يبدأ ب https لا تقم بإدخال تفاصيل البطاقات البنكية أو رقم الضمان الاجتماعي أو أي من المعلومات الحساسة الأخرى

النصيحة رقم 23: احذر من الخدمات المجانية

العديد من الخدمات المجانية تحوي على إعلانات ونوافذ منبثقة والتي من الممكن أن لا تكون آمنة كما أن مجرمو الانترنت يعرفون ما الذي يبحث عنه المستخدم

بالضبط ويعملون على نشر نسخ مجانية للبرامج المدفوعة وهذه البرامج تكون ملغمة وتحوي على أكواد برمجية خبيثة تؤدي لاختراق جهازك وسرقة بياناتك وملفاتك أو ممكن أن تؤدي لتشفير ملفاتك ومطالبتك بدفع فدية مالية للقيام بعملية فك التشفير

النصيحة رقم 24: المبالغة بمشاركة الصور والمعلومات على مواقع التواصل الاجتماعي

أراهن بأنك تفعل ذلك ومن مننا لا يحب هذا الأمر ولكن يجب أن تدرك بأن الافراط بهذا الأمر ممكن أن يؤثر على أمنك الرقمي ويجعلك هدف لمجرمي الانترنت وقد تتعرض لهجمات سرقة الهوية عبر الانترنت عندما يكون جمع المعلومات عنك هو أمر سهل

المهاجم يستفيد من كل المعلومات التي تقوم بنشرها مثل أرقام الهواتف والأماكن التي تقوم بزيارتها وأسماء الأقارب وتاريخ الميلاد والعديد من المعلومات الأخرى ويستخدم هذه المعلومات للقيام بالأمور التالية:

- محاولة اختراق حساباتك
- التخمين على كلمات السر الخاصة بك
- إرسال رسائل للتصيد الاحتيالي

إذا كنت ترغب بالحصول على المزيد من المعلومات عن كيفية الحماية من هجمات سرقة الهوية يمكنك الاطلاع على دليل " الحماية من سرقة الهوية عبر الانترنت"

النصيحة رقم 25: تأكد من تأمين حساب البريد الالكتروني

البريد الالكتروني هو منزلك في عالم الانترنت فهو يحوي على كل جهات الاتصال الخاصة بك ويحوي على التخزين السحابي لملفاتك ومحادثاتك ومن خلاله يمكن إعادة تعيين كلمات السر للحسابات الأخرى المرتبطة به لذلك من المهم أن تولي أهمية كبيرة لحماية بريدك الالكتروني ويمكنك القيام بذلك من خلال الأمور التالية:

- معلومات الاسترداد الخاصة بالحساب
- سماحيات التطبيقات الأخرى
- كلمات السر
- إعدادات المصادقة الثنائية

النصيحة رقم 26: التقليل من البريد العشوائي spam

هل البريد العشوائي يملئ صندوق البريد الوارد لديك؟

يوجد بعض الأمور التي يمكنك القيام بها للتخلص من هذه المشكلة والحفاظ على صندوق البريد الوارد بأقل قدر من الرسائل العشوائية

- كن حذراً عندما إعطاء عنوان بريد الالكتروني الخاص بك
- قم بإلغاء الاشتراك في الخدمات والمواقع الإخبارية الغير ضرورية
- استخدم عوامل التصفية وتمييز رسائل البريد الالكتروني الغير مرغوب بها لمساعدة مزود خدمة البريد الالكتروني في حظرها بشكل أكثر فاعلية

- لا تنقر ابداً على الروابط الموجودة في رسائل البريد الالكتروني العشوائية spam
- لا تقم ابداً بتحميل وفتح المرفقات في رسائل البريد الالكتروني العشوائية spam
- قم بتعطيل التنزيل التلقائي لوسومات HTML في رسائلك
- استخدم حساب بريد الكتروني غير حسابك الأساسي للتسجيل في المواقع والخدمات الغير مهمة
- عند استخدام بريدك الالكتروني ضمن مواقع التواصل الاجتماعي تأكد من أن تكون الخصوصية الخاصة به "أنا فقط" حتى لا يتمكن أحد من رؤيته

تعتبر حملات البريد العشوائي spam من أهم عوامل نقل وإيصال الهجمات المستخدمة من قبل معظم مجرمي الانترنت لذا فإن التقليل من رسائل البريد العشوائي والرسائل الغير مرغوب بها يزيد من مستوى الحماية الخاص بك

النصيحة رقم 27: عادة أمنية جيدة

اتبع هذه العادات الأمنية الثلاثة لتكون أكثر أماناً على الانترنت:

- استخدم مضاد فيروسات على كل أجهزتك
- اقطع الاتصال بالشبكة عند عدم حاجتك لها
- لا تشارك كلمات مرورك مع أي أحد

بالإضافة للنصائح السابقة قم بتعليم عائلتك وأصدقائك عن كل ما تعرفه وقدم لهم النصائح المفيدة

النصيحة رقم 28: هل هاتفك الذكي آمن؟

يتجاهل الكثير من الأشخاص الحماية الخاصة بالهواتف الذكية ومع وجود كم كبير من البيانات على هذه الأجهزة فيجب عليك بذل كل ما بوسعك للحفاظ على حماية هاتفك الذكي

إليك بعض الخطوات الأساسية والحيوية التي يجب عليك اتباعها:

- قم بتفعيل قفل للشاشة
- استخدم التشفير لحماية المعلومات السرية الموجودة في هاتفك
- قم بإيقاف تشغيل Wi-Fi والبلوتوث عند عدم استخدامك لها
- قم بتثبيت مضاد فيروسات خاصة بالهواتف الذكية
- تحقق من السماحيات الخاصة بالتطبيقات
- لا تقم بتثبيت أي تطبيقات من المصادر الغير موثوقة
- قم بإخذ نسخة احتياطية لبياناتك بشكل دوري

النصيحة رقم 29: عزز خصوصيتك على شبكة الانترنت

الخصوصية = الحماية والأمان

الخصوصية يمكن أن تزيد من مستوى الحماية ويمكنك تحسينها من خلال استخدام شبكات خاصة افتراضية VPN والتي تعمل على حماية نشاطك وهويتك على شبكة الانترنت وننصحك باستخدام VPN عند الاتصال بالشبكات اللاسلكية العامة لأنها تساعدك على حماية على توفير طبقة حماية إضافية من خلال تشفير البيانات

المرسلة والمستقبلة والتي ستساعدك للحفاظ على أمانك الرقم وخاصة ضد هجمات رجل في المنتصف

النصيحة رقم 30: الإعلانات السيئة والخبيثة

هل تعلم أن المهاجم يمكنه حقن تعليمات برمجية خبيثة ضمن الإعلانات التي تظهر في صفحات المواقع الشرعية ويسمى هذا التكتيك باسم الإعلانات الخبيثة

تسمح الإعلانات الخبيثة بإصابة جهازك بمختلف أنواع البرمجيات الخبيثة لذلك ننصح بالقيام بالأمور التالية:

- استخدم مانع للإعلانات
- استخدم مضاد فيروسات قوي وقم بتحديثه بشكل دورية
- استخدم برامج الحماية من الجيل الجديد القادرة على كشف ومنع البرمجيات الخبيثة المتقدمة

النصيحة رقم 31: التحقق من الحسابات المزورة على مواقع التواصل الاجتماعي

إليك بعد الطرق المفيدة لاكتشاف أو للتحقق من حساب على مواقع التواصل الاجتماعي إذا كان مزيف أو حقيقي

- استخدم الموقع https://tineye.com أو قم بالبحث ضمن الصور بمحرك البحث غوغل لمعرفة فيما إذا كانت صورة الملف الشخصي لهذا الحساب هي صورة

موجودة مسبقاً وخاصة بشخص آخر وإذا كانت الحساب مزيف ستظهر لك الكثير من النتائج

النصيحة رقم 32: التطبيقات من المصادر الغير موثوقة

لكل عمل تحتاجه يوجد له تطبيق أو برنامج ولكن ما مصدر هذا التطبيق؟

لا تقم ابداً بتثبيت تطبيقات من مصادر على موثوقة على أجهزتك وخاصة إذا كان الموقع الذي ترغب بتحميل التطبيق منه يحوي على نوافذ منبثقة وإعلانات مدمجة وأكثر من زر للتحميل، عندما ترى مثل هذه الصفحات، اهرب منها على الفور

القاعدة العامة: استخدم المواقع الرسمية والمتاجر الرسمية للحصول على التطبيقات والبرامج ولا تقم بتثبيت أي تطبيق من المصادر الغير موثوقة وخاصة النسخ المجانية للتطبيقات المدفوعة أن المهاجم يعرف عما يبحث المستخدم ويستغل هذا الأمر بشكل احترافي

النصيحة رقم 33: نشر مكان وجودك على مواقع التواصل الاجتماعي

تحديد مكان وجودك check in في الأماكن ونشره على مواقع التواصل الاجتماعي، هذا الأمر من وجهة نظر الحماية لا يعتبر أمراً جيداً

عندما تسافر لقضاء العطلة وتقوم بإلتقاط صور في المطار ولحظة وصولك لمكان معين هذا الأمر يزيد من احتمال تعرضك للخطر، يسعى المجرمون للاستفادة من

هذه المعلومات ومعرفة عدم وجودك في المنزل للتسلل لمنزلك وسرقته، بالتأكيد لا ترغب أنت بحصول ذلك

النصيحة رقم 34: تأكد من التصفح الآمن من خلال دقية واحدة فقط

قم بتثبيت إضافة للمتصفح HTTPS Everywhere وهذا سيضمن أن كل عمليات الاتصال مع المواقع الرئيسية سيكون بشكل مشفر وبذلك تمنع أي شخص يحاول التنصت على قناة الاتصال من رؤية أو سرقة معلوماتك المتبادلة

النصيحة رقم 35: ابتعد عن مواقع القرصنة

بالتأكيد أنك ترغب بمشاهدة الأفلام والمسلسلات الجديدة أو ترغب بالحصول على نسخ مجانية للتطبيقات المدفوعة وتبحث عنها ضمن مواقع القرصنة التي تقوم بمشاركة هذه الملفات

كن حذراً عند التعامل مع هذه المواقع، البعض منها ممكن أن يحوي على ملفات آمنة ولكن من الممكن أن يحوي أيضاً على إعلانات خبيثة تودي لإصابة جهازك ببرمجيات خبيثة

النصيحة رقم 36: ما هو مدى الحماية المطبقة لديك

حان الوقت للقيام بعملية فحص واختبار مدى فعالية الحماية المطبقة

يستهدف مجرمو الانترنت الإضافات القديمة والمتصفحات والبرامج القديمة والتي تحوي على ثغرات لذلك قم بعملية فحص لكل الإضافات والبرامج القديمة التي لا

تستخدمها وقم بإلغاء تثبيتها وتأكد من تحديث كل البرامج والتطبيقات التي تستخدمها

النصيحة رقم 37: الجريمة الالكترونية كعمل تجاري

ربما لم تفكر في هذا الأمر مطلقاً ولكن يجب أن تدرك بأن مجرمي الانترنت يديرون عملياتهم كعمل تجاري ويتبعون الأمور التالة:

- البحث عن طرق جديدة لتحقيق الدخل من الهجمات (بيع البيانات على الانترنت المظلم وشراء أنواع جديدة من برامج الفدية التي لا يمكن فك تشفيرها والعديد من الأمور الأخرى)
- في بعض الأحيان يقوم مجرمو الانترنت بتوظيف أو استآجار هاكر شرير ليقوم بتنفيذ الهجمات المطلوبة
- الاستثمار في الحصول على البنية التحتية التي يمكن استخدامها لشن الهجمات والمحافظة على بقائهم مجهولين
- شراء مجموعات وأدوات الاستغلال والبرامج الخبيثة الجاهزة التي يمكن نشرها واستخدامها على الفور

غالباً ما يقوم مطورو البرمجيات الخبيثة ببيع شفراتهم او أكوادهم البرمجية الضارة وبالتالي فإن اقتصاد البرمجيات الخبيثة هو سوق نشط ومتطور باستمرار

النصيحة رقم 38: كيف تبدو رسائل التصيد الاحتيالي عبر البريد الالكتروني

هل تسألت يوماً ما كيف تبدو رسالة البريد الالكتروني المخادعة؟ ربما قد شاهدت واحدة منها من قبل ولكنك لا تعلم أنها كانت محاولة خبيثة لجمع بياناتك الشخصية أو محاولة لاختراقك

إليك بعض الأمور التي يجب أن تنتبه لها:

- لن تعرض لك المواقع الجادة عنوان بريدك الالكتروني في عنوان أو مضمون الرسالة
- لا تقم بالضغط على أي شيء يصلك عبر رسائل البريد الالكتروني حتى لو كانت الرسالة تبدو عاجلة او تحوي على نوع من الإلحاح

هذه الأمور تشير إلى محاولات تصيد سيئة التصميم ولكن يجب ان تدرك بأن هناك محاولات أخرى تبدو حقيقة حقاً وممكن ان تنخدع بها لذا تحقق دائماً من الروابط قبل النقر عليها ولا تقم بتحميل او فتح الملفات المرفقة

النصيحة رقم 39: تحقق منه قبل فتحه

تحقق بشكل دائم من أي رابط قبل فتحه ويمكنك القيام بذلك من خلال المواقع التالية:

- https://www.virustotal.com/
- http://global.sitesafety.trendmicro.com/

- http://zulu.zscaler.com/

والتي تساعد في اكتشاف فيما إذا كان موقع الويب يشكل خطر على أمنك أو خصوصيتك

قد تأتيك الروابط الخبيثة او الضارة عبر:

- البريد الالكتروني
- مواقع التواصل الاجتماعي
- تطبيقات المراسلة الفورية

النصيحة رقم 40: ممكن أن يكون الأمر مخادع

على شبكة الانترنت إذا كان الأمر مجاني أو يبدو أنه جيد لدرجة يصعب تصديقها فيجب أن يكون هذا الأمر مريباً جداً

الويب مليء بالآلاف من عمليات الاحتيال وبعضها بسيط وبعضها الأخر معقد جداً ولكن جميعها تهدف إلى شيء واحد وهو الحصول على اموالك وللأسف فإن هذه الحيل تعمل وتنجح بنسبة كبيرة جداً

النصيحة رقم 41: لا تستخدم حساب بصلاحيات عالية

عندما تقع ضحية لهجوم أو عملية اختراق سيكون الأمر مؤذي جداً بالنسبة لك ويجب أن تدرك بأن العديد من الهجمات تتم بشكل آلي حيث تقوم أكواد الاستغلال بفحص نظامك بحثاً عن ثغرات ونقاط ضعف لاستغلالها لذلك لا تستخدم حساب له صلاحيات

عالية وبدل ذلك أنشئ حساب بصلاحيات عادية للحد من خطورة الأمر وتقييد إمكانية المهاجم في حال تمكن من اختراق نظامك

النصيحة رقم 42: يجب أن تكون الحماية المطبقة متعددة الطبقات

لن تكون محمي بشكل مطلق أو بنسبة 100% من الهجمات السيبرانية لذا لا تقع في فخ الحيل التسويقية لمنتجات وبرامج الحماية وبغض النظر عن المقدار الذي يدعيه برنامج الحماية بأنه سيجعل نظامك آمن تذكر دائماً القاعدة الأساسية "لا يوجد نظام آمن بشكل مطلق أو غير قابل للاختراق" وهذا لا يعني أنه لا يجب عليك اتخاذ جميع إجراءات الحماية بل يجب أن تقوم باستخدام أكثر من طبقة للحماية وعندها في حال فشل إحدى الطبقات فممكن أن يتم كشف او إيقاف الهجوم من قبل الطبقات الأخرى

النصيحة رقم 43: قم بإعداد قائمة لتقييم المخاطر الأمنية

في كتاب فن الحرب الشهير قال الكاتب Sun Tzu: "يجب أن تعرف عدوك تماماً وأن تعرف نفسك"

لذا قم بالأمور التالية:

- إعداد قائمة لتقييم المعلومات والبيانات التي قمت بتخزينها على أجهزتك والتي من الممكن أن تكون صوراً او مستندات أو كلمات السر وبيانات الاعتماد الأخرى

- ما هي الحسابات التي تملكها على شبكة الانترنت وما هي المستخدمة منها وما هي الغير مستخدمة
- بعد إعداد هذه القائمة قم بتقييم قيمة البيانات التي تحتفظ بها وماذا سيحدث إذا لم يعد بإمكانك الوصول لها إن تم فقدانها أو حذفها أو تسريبها على شبكة الانترنت
- ما هي الحماية المطبقة للحفاظ على معلوماتك الحساسة وما هي الإجراءات المتبعة لمنع الوصول الغير مصرح لها
- ماذا عن الملفات والأجهزة المشتركة؟ من لديه حق الوصول لها
- ما هي حلول النسخ الاحتياطي الموجودة لديك

النصيحة رقم 44: تطور عمليات الاحتيال الشائعة لتصبح عمليات احتيال عبر الانترنت

يستخدم مجرمو الانترنت طرق مبتكرة لخداعك من خلال جذبك لأشياء مجانية لتقوم بالنقر أو فتح الروابط الخبيثة، مثال على ذلك الصفحات أو الرسائل التي تخبرك بأنك الرابح لجائزة معينة وستحصل على هاتف جديد أو بطاقة رحلة مجانية مع التأكيد في الإلحاح عليك والاستعجال من خلال تحديد المدة وكتابة أن هذا الأمر متاح فقط لمدة يوم واحد وهذه الأساليب للأسف تنجح مع المهاجمين ومعظم الأشخاص يقعون ضحية لعمليات الاحتيال من هذا النوع

النصيحة رقم 45: تحقق من سجل نشاط البريد الالكتروني

بالتأكيد لديك بريد الكتروني، هل تعلم بإنه يمكنك التحقق من سجل النشاط لحسابك وهذا الأمر يسمح لك برؤية الأجهزة والمتصفحات التي تم فتح حسابك منها مع تحديد الوقت وعنوان IP وإذا كان هناك شيء لا تعرفه أو جلسات قديمة من أجهزة لم تعد تملكها فقم بإنهائها وهذا الأمر موجود أيضاً في معظم مواقع التواصل الاجتماعي وتطبيقات المراسلة الفورية لذا قم بمراقبة مكان استخدام حسابك وقم بإنهاء كل الجلسات التي لا تعرفها وننصح بتطبيق المصادقة الثنائية لتكون حساباتك أكثر أماناً

النصيحة رقم 46: لا تنتظر حدوث الأمور السيئة

ينتظر معظم الأشخاص حدوث الأمور السيئة للقيام باتخاذ الإجراءات الأمنية

إما أنهم لا يدركون التهديدات الأمنية التي من الممكن أن يتعرضوا لها أو أنهم يعتبرون الحماية مجرد مضيعة للوقت والمال والجهد، في الحقيقة يمكن اختراق أي حساب على الانترنت وخاصة إذا كان مالك الحساب لا يتخذ أي اجراء لحماية نفسه وما هي إلا مسألة وقت ليتم ذلك وعندها سيكون هذا الدرس مكلفاً للغاية وسيتم التعلم منه ولكن بالطريقة الصعبة

تخيل الآن ماذا سيحدث إذا فقدت أحد حساباتك؟ أو البيانات الخاصة أو بيانات وملفات العمل، ماذا لم تم بيع هذه البيانات او نشرها على الانترنت، ماذا لم تم ابتزازك بها، كم سيؤثر هذا الأمر على سمعتك وطبيعة عمل

لمنع حدوث ذلك قم بتطبيق إجراءات الحماية الوقائية

النصيحة رقم 47: ممنوع النقر بشكل متهور

ربما قد قرأت عن الدراسات والأبحاث التي تتحدث عن تشتت البشر بسبب أجهزة الحاسب والموبايل وشبكة الانترنت ولذلك يجب أن تدرك بأن الأمر يتطلب نقرة واحدة فقط والتي ممكن ان تؤدي لإصابة جهازك ببرمجيات خبيثة

إليك بعض الأشياء التي لا يجب أن تنقر عليها:

- أي روابط قصيرة ليس لديك فكرة عن المكان الذي تؤدي له
- أي رسائل عبر البريد الالكتروني أو مرفقات لم تقم بطلبها
- أي تطبيقات داخل مواقع التواصل الاجتماعي (خاصة تلك التي تدعي اعرف من زار بروفايلك)

النصيحة رقم 48: توقف عن مقارنة نفسك بالأخرين

إذا كان الأشخاص من حولك لا يستخدمون المصادقة الثنائية أو إذا كانوا لا يدفعون مقابل مضاد فيروسات قوي وجدير بالثقة أو إذا كانوا لا يقومون بتحديث جميع برامجهم أو لا يقومون بعمليات نسخ احتياطي لبياناتهم فلا يجب أن تكون مثلهم ولا تسمح لهم بالتأثير عليك أو على الإجراءات التي تتخذها لحماية بياناتك ويجب أن تتعلم وتتأثر من الخبراء وليس العكس

النصيحة رقم 49: عصر عمليات الاحتيال الجديدة – أكبر وأفضل وأكثر جرأة

تطورت عمليات الاحتيالي لتصبح أكثر تعقيداً وأصبحت تأخذ أشكال مسابقات عبر مواقع التواصل الاجتماعي لربح تذاكر طيران مجانية او لربح هواتف أو العديد من الأمور الأخرى المشابهة لكشف مثل هذه الحيل إليك النصائح التالية:

- إذا كان من الجيد جداً تصديق أمر ما فمن المحتمل أن لا يكون كذلك
- لا يوجد شيء مجاني في هذا العالم
- تحقق دائماً من ثلاثة مصادر جديرة بالثقة على الأقل (موقع ويب رسمي – قناة رسمية موثقة على مواقع التواصل الاجتماعي – وسائل إعلام رسمية تتحدث عن الشركة او طريقة للاتصال المباشر بالشركة)

النصيحة رقم 50: قم بإزالة تطبيقات الموبايل الغير مستخدمة

ألق نظرة سريعة على تطبيقات الهاتف المحمول الخاصة بك وقم بالأمور التالية:

- إزالة أي تطبيقات لم تكن تستخدمها فمن الممكن أن تحوي على ثغرات أمنية تتعلق بالحماية والخصوصية
- قم بإلغاء السماحيات أو الأذونات التي تتطلب الوصول لمعلومات حساسة (لماذا يطلب تطبيق المصباح الوصول للرسائل – على سبيل المثال)
- حافظ على تحديث تطبيقاتك بشكل دائم لأن هذا الأمر يقلل من فرص أو احتمال استغلال الثغرات ونقاط الصعف الموجودة فيها

وتذكر القاعدة الأساسية في الأمن السيبراني: لا تقم ابداً بتحميل وتنصيب التطبيقات من المصادر الغير وتأكد من القيام بذلك فقط من المتاجر الرسمية

النصيحة رقم 51: لا تثق بأي أحد

لا تثق بأي أحد لا موظفيك ولا أصدقائك ولا حتى أخوتك وأفراد عائلتك

انت لا تعرف كيف ستتطور العلاقة وكيف ستكون الأمور على المدى الطويل لذا لا تقم بمشاركة كلمات السر الخاصة بك أو معلوماتك الحساسة مع أي شخص مهما كان مقرب منك

النصيحة رقم 52: حماية الهاتف الذكي

لا تترك جهاز الهاتف المحمول الخاص بك بدون قفل للشاشة وقم بتفعيل القفل التلقائي بعد 15 أو 30 ثانية ويجب أن تدرك أن استخدام رمز قفل PIN بسيط مكون من أربع أرقام لا يقدم الحماية الكافية لذلك انتقل لاستخدام كلمة سر أو ارسم نمطاً مخفياً ومن الأفضل أن تقوم بتفعيل المصادقة من خلال بصمة الأصبع

النصيحة رقم 53: لا يوجد أي نظام محمي ضد الاختراقات

يجب أن لا يكون اعتمادك فقط على مضاد الفيروسات في الحماية بعض النظر عن قوته فهو لن يحميك من جميع التهديدات الموجودة مثلاً لن يكون مضاد الفيروسات قادراً على حمايتك من موظف سابق او صديق/ صديقة سابق غاضب يريد الانتقام منك

النصيحة رقم 54: هل لديك شريط لاصق؟ قم بلصقه فوق الكاميرا الخاصة بجهازك الحاسب

ضع شريطاً لاصقاً على كاميرا الويب الموجودة في جهازك الحاسب

مدير مكتب التحقيقات الفدرالية يفعل ذلك ويجب عليك فعل ذلك أيضاً لأنك لا تعرف ابداً كيف يتم اختراق جهازك أو الوصول للكاميرا ومراقبتك

النصيحة رقم 55: لا تقم بتحديد مكانك

لا تقم بعمليات check in عند مغادرك للمنزل لفترات طويلة لقضاء الاجازة وهذا الأمر يتضمن أيضاً عدم نشر صور تذاكر الطيران وصور العطلات والرحلات على الأقل في الوقت التي تتواجد فيه بعيداً عن المنزل لأن هذا الأمر قد يتحول لكابوس مرعب

العديد من الأشخاص شاركوا هذه المعلومات وتفاخروا بالأماكن الرائعة التي يزورونها وعندما عادوا إلى منازلهم اكتشفوا أنها كانت هدف للصوص، أنت لا تعرف أبداً من يمكنه رؤية هذه المعلومات التي تقوم بنشرها حتى لم قمت بتقييد الوصول لها ومشاركتها مع الأصدقاء فقط

النصيحة رقم 56: للآباء والأمهات، يرجى عدم نشر صور لأطفالكم

الآباء والأمهات الأعزاء يرجى عدم نشر صور لأطفالكم على مواقع التواصل الاجتماعي في البداية فكر انه عندما يكبر طفلك ستكون حياته متاحة للعامة وممكن أن يتم استخدام صوره لأمور لن تكون بمصلحته وممكن ان يكون هذا الأمر مزعج له، ثانياً أنت لا تعرف أين سينتهي الأمر بهذه الصور وممكن أن تصل

للمتحرشين أو الأشخاص السيئين، تخيل أن يقوم أحد هؤلاء الأشخاص بجمع المعلومات عن طفلك من خلال الصور ومعرفة الحديقة التي يلعب بها طفلك أو المدرسة التي يذهب لها طفلك

النصيحة رقم 57: حافظ على المتصفحات محدثة بشكل دائم

يعتبر المتصفح أحد أكثر البرامج التي نستخدمها أثناء الاتصال بشبكة الانترنت

تحوي المتصفحات على ثغرات ونقاط ضعف امنية وإذا لم تقم بعملية التحديث لتطبيق الإصلاحات الخاصة بهذه الثغرات فمن الممكن ان يتم استغلالها من قبل المهاجمين والوصول لجهازك أو إصابة جهازك ببرمجيات خبيثة، لذا حافظ على المتصفحات والإضافات الخاصة بها بأحدث إصدار

النصيحة رقم 58: قم بإزالة العلامة الجغرافية للمنشورات السابقة في مواقع التواصل الاجتماعي

في نصيحة سابقة تحدثنا عن مخاطر تحديد مكانك عبر المنشورات على مواقع التواصل الاجتماعي وإذا فاتك هذا الأمر، يوجد خيار في موقع الفيسبوك يسمح لك بحذف كل المواقع والصور السابقة وإيقاف هذا الأمر للمنشورات المستقبلية

كما ننصحك بإزالة كل العلامات الجغرافية لكل الصور قبل مشاركتها

النصيحة رقم 59: كن حذراً من تطبيقات الهواتف المحمولة

نعود ونكرر القاعدة الأساسية في الأمن السيبراني، فقط قم بتحميل وتنصيب التطبيقات من المتاجر الرسمية وتأكد من تعطيل خيار السماح بتثبيت التطبيقات من المصادر الخارجية وهذا الأمر يتضمن أيضاً عدم تنصيب أي تطبيقات تحصل عليها من قبل اصدقائك أو عبر الانترنت ويجب أن تدرك أيضاً بان المتاجر ليست آمنة بشكل مطلق أو بنسبة 100% ففي العديد من الحالات ثبت إصابة التطبيقات الموجودة في المتاجر الرسمية

النصيحة رقم 60: استخدم حسابات بريد الكتروني متعددة

قم بإنشاء عدة حسابات بريد الكتروني منفصلة تماماً لاستخدامها في مواقع أو أغراض مختلفة

- حساب بريد الكتروني للاشتراك في النشرات الإخبارية
- حساب آخر خاص لمواقع التواصل الاجتماعي
- حساب مختلف آخر للعمل
- حساب خاص للأمور الشخصية

قد يبدو إنشاء كل هذه الحسابات وإدارتها أمر صعب ولكنه يستحق هذا العناء فهو يساعدك على تقليل تلقي البريد العشوائي spam وفي حال تعرض أحد حساباتك للاختراق فسيكون الضرر محدود ولن يمس بكامل حياتك الرقمية

النصيحة رقم 61: يمكن لأدوات منع الإعلانات أن تقلل من خطر الإصابة بالبرمجيات الخبيثة

إذا لم تكن قد سمعت عن البرامج او الإضافة الخاصة بمنع الإعلانات من قبل فإليك الشرح المختصر لها:

هي إضافات أو برامج يتم تنصيبها لمنع الإعلانات عبر الانترنت وقادرة على منع النوافذ المنبثقة وجميع أنواع الإعلانات الأخرى ضمن نتائج البحث ومقاطع الفيديو

يعتبر حظر الإعلانات المزعجة هو أهم أمر تتفاخر به أدوات من منع الإعلانات إلا أنها تتمتع بميزة أخرى وهي القضاء على الإعلانات الخبيثة والتي ممكن ان تؤدي لإصابة جهازك ببرمجيات خبيثة وهذا الأسلوب مستخدم على نطاق واسع من قبل مجرمي الانترنت لنشر أكوادهم البرمجية الخبيثة وحقنها ضمن الإعلانات ضمن المواقع الشرعية

النصيحة رقم 62: أهم البرامج المصابة بالثغرات

يجب أن تطلع بشكل دائم على أخبار الحماية ومعرفة البرامج المصابة بالثغرات ويمكنك الحصول على هذه المعلومات من خلال متابعة مدونتنا

من المهم أن تدرك أن جميع الأنظمة تحوي على ثغرات لذلك يعتبر من المهم أن تطلع على أخبار الامن السيبراني وتعرف متى يجب ان تقوم بعمليات التحديث لإصلاح الثغرات

النصيحة رقم 63: معرفة الفرق بين الفيروسات وبرامج الفدية والأنواع الأخرى من البرمجيات الخبيثة

من المهم ان تعرف الأمور الأساسية في الأمن السيبراني وهذا يشمل معرفة الأنواع المختلفة للبرمجيات الخبيثة، إليك بعض الأنواع بشكل سريع:

- **الفيروسات:** هي نوع من البرامج الخبيثة لها القدرة على نسخ نفسها وتحتاج لتفاعل من قبل المستخدم ليتم تشغيلها
- **برامج الفدية:** هي نوع من البرمجيات الخبيثة تقوم بتشفير ملفاتك ومنع الوصول لها وإظهار رسالة لك تطالبك بدفع مبلغ مالي كفدية لفك تشفير ملفاتك

لن نطيل الحديث عن البرمجيات الخبيثة يمكنك الاطلاع على كل أنواع البرمجيات الخبيثة من خلال كتاب "البرمجيات الخبيثة – الإصدار الثاني"

النصيحة رقم 64: أفضل طريقة لعمل نسخة احتياطية لصورك

أنا شخص بسيط، أقوم بإلتقاط الكثير من الصور ولا توجد طريقة أو الوقت الكافي لاختيار المهم منها للاحتفاظ بها كذكرياتي، **إن كنت تعاني من نفس المشكلة فإليك الطريقة التالية والتي يمكنك من خلالها الحفاظ على صورك بشكل آمن:**

- قم بعملية النسخ الاحتياطي ضمن Google Photos هذه الخدمة المجانية تقدم من غوغل ويمكنك القيام بهذا الأمر بشكل يومي عند الاتصال بشبكة wifi المنزلية

- احتفظ بنسخة من صورك المهمة على ذاكرة خارجية وقم بعملية النسخ الاحتياطي بشكل دوري
- قبل نسخ صورك بشكل احتياطي على الذاكرة الخارجية قم بتشفير الصور حتى لا يتمكن أي شخص من الوصول لها في حال تمكن من الوصول لهذه الذاكرة

يستغرق هذا الأمر بضع دقائق ويجب أن يكون من عاداتك الروتينية

النصيحة رقم 65: المفاهيم الخاطئة حول الامن السيبراني – الجزء الأول

حان الوقت لكسر بعض المفاهيم الخاطئة حول الأمن السيبراني والتي قد لا تزال تؤمن بها

الاعتقاد الخاطئ: أنا لا احتاج لاستخدام برامج للحماية لأنني لا اتصل مع مواقع غير آمنة

الحقيقة: الفطرة السليمة ضرورية على شبكة الانترنت ولكنها ليست كافية لحمايتك من التهديدات الالكترونية حتى المتخصصين في مجال الحماية يعترفون بأن بعض التهديدات ماكرة لدرجة أنهم في بعض الحالات يواجهون صعوبة في تحديدها او اكتشافها ويجب أن تدرك أيضاً بأن الهجمات الالكترونية يمكن أن تتم من المواقع الشرعية والجديرة بالثقة

أن تكون آمناً على شبكة الانترنت يشبه بشكل كبير قيادة السيارة، قد تكون سائق محترف ولديك الحس السليم وتنتبه لكل المخاطر المحتملة ولكن هل تتوقع دائماً ما يقوم به الأشخاص الآخرين من حولك

النصيحة رقم 66: المفاهيم الخاطئة حول الأمن السيبراني – الجزء الثاني

إليك اعتقاد خاطئ أخر وهو: شبكات التواصل الاجتماعي آمنة والأصدقاء فيها هو أصدقاء حقيقيون

الحقيقة: كلما زادت المعلومات التي تشاركها على مواقع التواصل الاجتماعي كلما زادت جاذبيتك لدى مجرمي الانترنت ويجب أن تدرك بأن مواقع التواصل الاجتماعي هي المكان المناسب لمجرمي الانترنت للقيام بمهامهم بالشكل الأمثل من انتحال للشخصية أو التلاعب أو سرقة البيانات أو الأموال وتعريض حسابك للخطر

حتى لو كنت خبيراً بالأمن السيبراني فهذا لا يعني أن كل أصدقائك على موقع الفيسبوك هو أصدقاء حقيقيون

النصيحة رقم 67: مشكلة البرامج الغير مدعومة

نقرأ بشكل دائم ضمن الأخبار التقنية عن إيقاف الدعم عن برنامج او نظام معين وهذا الأمر يعني ان الجهة المصنعة لن تقوم بإصدار تحديثات خاصة بإصلاح الثغرات بعدد الآن

إن كنت من الأشخاص الذين مازالوا يعملون على الأنظمة الغير مدعومة فيجب أن تدرك بأن نظامك الغير مدعوم يحوي على ثغرات قابلة للاختراق ولن تتمكن من إصلاحها بسبب إيقاف الدعم من قبل الجهة المصنعة وبقاء هذه الثغرات بدون إصلاح سيعرض أمنك للخطر وسيتمكن مجرمو الانترنت من استغلال هذه الثغرات واختراق جهازك والوصول لبياناتك ومعلوماتك الحساسة، لذا لا تقم باستخدام أي نظام أو برنامج غير مدعوم وحافظ على تحديث نظامك وبرامجك بشكل دائم

النصيحة رقم 68: احذر من برامج مكافحة الفيروسات المزورة

تعتبر هذه الحيلة من أقدم أساليب مجرمي الانترنت، لقد رأينا جميعاً الرسالة أو النافذة المنبثة التي تظهر على الشاشة "أنت معرض للحظر، قم بتنزيل مضاد الفيروسات التالي لحماية جهازك" يجب أن تدرك بأن الشركات المصنعة لمضادات الفيروسات لن تعلن أبداً عن منتجاتها بهذا الأسلوب وهذا الأسلوب مستخدم من قبل المخادعين ومجرمي الانترنت على نطاق واسع لدرجة أنه قادر على خداع شريحة كبيرة من الأشخاص

ما الذي يمكن أن يفعله مضاد الفيروسات المزيف بنظامك:

- يمكن أن يصيب جهازك ببرامج الإعلانات الخبيثة
- ممكن أن يصيب جهازك ببرمجيات خبيثة كبرمجيات الفدية ransomware والتي ستقوم بتشفير كل ملفاتك ومنعك من الوصول لها ومطالبتك بدفع مبلغ مالي كفدية للتمكن من استعادة الوصول لملفاتك

هذا الأسلوب مستخدم أيضاً ضمن أجهزة الموبايل لذا تأكد دائماً من حصولك على برامج الحماية ومضادات الفيروسات من المصادر الموثوقة فقط

النصيحة رقم 69: ليس كل الهاكرز سيئين (يوجد عدة أنواع)

من الغريب أن تسمع ذلك ولكن بالحقيقة يوجد أنواع من الهاكرز الجيدين

في البداية لنقم بتعريف كلمة هاكر: هو "شخص محترف" والذي يدرس أنظمة التشغيل ولغات البرمجة وخوارزميات التشفير وقواعد البيانات وطرق استخراج المعلومات وآلية انتقال البيانات عبر الشبكة وأمور أخرى.

كلمة هاكر تستخدم أيضاً للإشارة إلى الشخص الذي يرتكب جرائم إلكترونية مثل إيقاف أنظمة الكمبيوتر أو اختراق خصوصيات الناس وسرقة معلوماتهم الشخصية وإلحاق الأذى بهم.

أنواع الهاكر:

بشكل عام يمكن أن يتم تصنيف الهاكر ضمن ثلاثة أنواع فقط (الأبيض والأسود والرمادي) ولكن في الفترة الأخيرة ظهرت تصنيفات جديدة وهي:

- **Black Hat Hacker:** وهو الشخص الشرير الذي يقوم بأعمال مؤذية وجرائم الكترونية وهو شخص يعمل على اختراق أشخاص أو مؤسسات والهدف من ذلك سرقة المعلومات الشخصية أو البنكية أو الحصول على معلومات من الضحية لاستخدامها في أعمال مؤذية وغير شرعية.

- **White Hat Hacker (الهاكر الأخلاقي):** هدف هذا الشخص هو تخطي الحماية و اختراق الأنظمة من أجل كشف الثغرات ونقاط الضعف والبحث عن المشاكل الأمنية وتبليغ المسؤولين عنها وليس استغلالها لهدف خبيث، بعض من هؤلاء الأشخاص قام بالعديد من المشاريع الحرة والمفيدة مثل إنشاء نواة أنظمة تشغيل مفتوحة المصدر مثل نظام Linux وتطوير البنية التحتية للشبكات وتقديم استشارات أمنية لكبرى الشركات العالمية والحكومات والمؤسسات الضخمة.

- **Gray Hat Hacker:** وهو شخص غامض غير محدد الهدف لأنه يقف في منطقة حدودية بين الهاكر الأسود والأبيض فممكن في بعض الحالات أن يقوم بمساعدتك وفي حالات أخرى يمكن أن تكون هدفه وضحيته القادمة وفي الغالب يقوم هذا النوع عند اكتشافه لثغرة ما بنشرها لعموم الناس بدلاً من إبلاغ المسؤولين عنها وممكن أن يقوم بكسر تشفير البرامج والتراخيص الخاصة بالبرامج (حقوق النشر) ونشرها على الانترنت بدون مقابل.

- **Blue Hat Hacker:** وهو متخصص في مجال الحماية ويقدم استشارات أمنية بعد فحص النظام من الخارج في محاولة لإيجاد المشاكل والثغرات الأمنية قبل إطلاق النظام في السوق والسبب في تسميته بهذا الاسم (القبعة الزرقاء) بالتحديد لأن شركة مايكروسوفت (صاحبة اللون الازرق) هي من أوائل الشركات التي فعلت ذلك وقامت باستقدام مجموعة من الهاكر لتقيم منتجاتها من الناحية الأمينة.

- **Green Hat Hacker:** وهو شخص لديه شغف ومحبة للدراسة ورغبة في التعلم ولكنه لا يقوم بأي عمليات اختراق فقط دراسته تأتي من دافع الفضول.
- **Script Kiddie (أطفال الهاكر):** هذا النوع يتواجد بكثرة في الوطن العربي والمقصود من الاسم شخص ليس لديه أي معلومات عن الكومبيوتر أو مهارته ضئيلة أو شبه معدومة ويستخدم أدوات أو برامج أو سكريبتات جاهزة لاختراق ومهاجمة الأخرين أو تخريب المواقع دون فهم معنى ما يستخدمه أو طريقة عمله.
- **Hacktivist:** وهو شخص (أو مجموعة) يقوم بعمليات اختراق لإظهار دعمه أو نضاله لقضية ما سواء كانت سياسية أو حتى اجتماعية وأشهر مثال على ذلك مجموعة أنونيموس والجيش السوري الالكتروني.
- **Spy Hacker:** وهو شخص يتم استئجاره من قبل شخص أو شركة لاختراق هدف معين مقابل مبلغ مادي وهذا النوع يتواجد بكثرة في أوروبا الشرقية وروسيا والصين.

النصيحة رقم 70: هل يجب أن تدفع في حال تعرضك لهجوم ببرمجيات الفدية

لدينا سيناريوهان لهذه الحالة:

1- إذا كان لديك نسخة احتياطية من ملفاتك فمن المؤكد الإجابة هي لا لذا تأكد دائماً من القيام بعمليات النسخ الاحتياطي لملفاتك وبياناتك المهمة، بالتأكيد الأمر ليس سهل ولكنه يستحق هذا العناء

2- إذا لم يكن لديك نسخة احتياطية من ملفاتك فالإجابة أيضاً هي لا، **إليك السبب:**

- المهاجمون عبر الانترنت ليسوا أشخاص جديرين بالثقة لذلك فإن عملية الدفع لن تضمن لك الحصول على مفتاح فك التشفير واستعادة ملفاتك
- من خلال عملية الدفع فأنت تغذي اقتصاد البرمجيات الخبيثة والتي بالفعل هي بازدهار وتقدم مستمر وهذا الأمر سيؤثر علينا جميعاً من خلال الأضرار القادمة
- كل فدية مدفوعة تغذي هجوماً آخر على أشخاص آخرين والضحية التالية قد تكون شخصاً تحبه

بياناتك مهمة ولكي لا تكون بهذا الموقف اتخذ الخطوات الصحيحة الآن وقم بعمليات النسخ الاحتياطي لملفاتك بشكل دوري وقم باستخدام أكثر من طبقة حماية، للمزيد من الخطوات التي يمكنك اتباعها في حال تعرضك لمثل هذا النوع من الهجمات يمكنك الاطلاع على دليل " نصائح للحماية من برمجيات الفدية"

النصيحة رقم 71: فعل تحديد موقع هاتفك الذكي عن بعد

في حال فقدت هاتفك أو تمت سرقته يمكن تحديد مكانه إن كنت قد فعلت هذه الميزة بشكل مسبقاً وهي موجودة في معظم الهواتف بالنسبة إلى Apple تسمى Find my iPhone وبالنسبة لأجهزة الأندرويد موجودة ضمن الإعدادات أيضاً باسم Find my Device لذا تأكد من تفعيل هذا الخيار على جهازك

النصيحة رقم 72: الاعتقاد الخاطئ في الأمن السيبراني – الجزء الثالث

"أنا أقوم بفتح رسائل البريد الالكتروني القادمة فقط من الأشخاص الذين اعرفهم لذا يجب أن أكون آمن بشكل دائم"

الحقيقة التي يجب أن تدركها بأن حملات التصيد الاحتيالي phishing attack غالباً ما تتم من خلال رسائل البريد الالكتروني ومن خلال عناوين منتحلة وعنوان المرسل يبدو لك كأنه عنوان شرعي لشخص او جهة ممكن ان تكون معروفة بالنسبة لك وهذا الأمر يتم بشكل متقن ليتمكن المهاجم من خداعك لتضغط على الرابط أو تفتح الملفات المرفقة الخبيثة لذا يجب ان تدرك بأن هذا الأمر ليس حصراً على العناوين أو الجهات الغير معروفة وممكن أن يبدو لك العنوان خاص بصديق أو شخص تعرفه وهذا الأمر يمكن أن يكون حقيقة (في بعض الحالات يتم اختراق اشخاص واستخدام حساباتهم لاختراق أهدف أخرى محيطة بهم) وهذا الأسلوب متبع بشكل كبير من قبل مجرمي الانترنت

عندما تتلقى رسائل تدعوك للضغط على رابط مرفق أو لتحميل المرفقات من صديقك او من جهة معروفة بالتأكيد لا تقم بذلك وقم بالاتصال بصديقك أو هذه الجهة واسألهم عن هذا الأمر

النصيحة رقم 73: تذكر القيام بعملية إعادة ضبط المصنع

عن التخطيط لبيع هاتفك تأكد من قيامك بعملية ضبط المصنع قبل ذلك لضمان مسح البيانات ومنع الوصول لحساباتك المفتوحة داخله

وتأكد من نسخ كل بيناتك ومعلوماتك بشكل احتياطي على ذاكرة خارجية وقم بعملية المسح الآمن لها لكي لا يتمكن مالك الهاتف الجديد من استعادتها

النصيحة رقم 74: فكر كصحفي

أفضل طريقة للبحث عن أي معلومة تجدها على الانترنت هي التفكير كصحفي للتأكد من مصدر أي معلومة وهذا الأمر ليس فقط للحماية ولكنه سيساعدك أيضاً في التمييز بين البيانات والمعلومات الجيدة والسيئة:

- لا تثق بالمعلومات الغير مدعومة بمصادر
- تحقق من المعلومات من 3 مصادر موثوقة على الأقل
- حافظ على موقف انتقادي تجاه المعلومات التي تتلقاها
- اتخذ موقف الشك تجاه الادعاءات التي تجد صعوبة في تصديقها أو حتى تلك التي يسهل تصديقها

النصيحة رقم 75: الإصابة ببرمجيات الفدية

تطورت الأساليب المستخدمة لنشر هذا النوع من البرمجيات كونها أصبحت نوع من العمل ومكسب مربح للأموال لذلك كن حذراً من تحميل البرامج والتطبيقات ولا تقم بتحميلها من المصادر الغير معروفة وخاصة النسخ المجانية للبرامج المدفوعة والأمر الأهم في الحماية ضد برامج الفدية هو النسخ الاحتياطي لذا تأكد من نسخ كامل ملفاتك المهمة بشكل منظم حتى لو تم تشفير ملفاتك فلن يكون لهذا الأمر تأثير سلبي كونك تملك نسخه احتياطية في مكان آمن ويمكنك العودة لها متى تشاء

النصيحة رقم 76: الاعتقاد الخاطئ في الأمن السيبراني – الجزء الرابع

هل تؤمن بالخرافة أو الاعتقاد الخاطئ التالي: "أنا أقوم بتنزيل البرامج والتطبيقات من مصادر موثوقة وهذا الأمر يبقيني آمن بشكل دائم"

الحقيقة هي: يمكن للتهديدات الأمنية الحالية أن تصل لك حتى من أكثر المواقع والبرامج شهرة وأكثرها حماية لذلك لا يجب أن تعتقد أنك محمي إذا كنت تصل فقط للمواقع أو البرامج تعرف أنها آمنة

تحدثنا سابقاً عن الإعلانات الخبيثة وتأثيرها وطريقة انتشارها ضمن المواقع الآمنة

النصيحة رقم 77: اجعل تطبيق الواتساب أكثر أماناً

قم بتفعيل التحقق بخطوتين ضمن الواتساب و ضمن كل تطبيقات المراسلة الفورية المشابهة

هذا الأمر يؤمن طبقة من الحماية ويمنع سرقة محادثاتك السرية في حال حاول المهاجم تفعيل الواتساب الخاص برقمك على جهاز آخر كونه لا يملك الكود السري الخاص بعملية التحقق بخطوتين

النصيحة رقم 78: تأكد من حماية حسابك على موقع الفيسبوك

هل سبق وأن قمت بعملية فحص للحماية لحسابك على موقع الفيسبوك؟

لنقم بهذا الأمر الآن:

- قم بعملية تسجيل الخروج من كل التطبيقات الغير مستخدمة والمرتبطة بحسابك على الفيسبوك لأنها ممكن ان تعرض بياناتك للخطر
- قم بتفعيل الإشعارات لتنبيهك عند أي عملية تسجيل دخول
- استخدم كلمة سر قوية
- قم بتفعيل المصادقة الثنائية

النصيحة رقم 79: قم بإزالة الإشارات الجغرافية السابقة ضمن صور انستغرام الخاصة بك

إذا كان لديك صور مع علامات جغرافية منشورة على الانستغرام (تدل على المكان الذي تم إلتقاط الصور به) فقم بالوصول لهذه الصور وتأكد من إزالة العلامة الجغرافية

الهدف من هذا الأمر هو عدم السماح لمجرمي الانترنت معرفة الأماكن التي تزورها باستمرار وهذا الأمر يساعد بالحفاظ على امنك وسلامتك في الحياة الرقمية وفي الحياة الواقعية

النصيحة رقم 80: الاعتقاد الخاطئ في الأمن السيبراني – الجزء الخامس

حان الوقت لكسر اعتقاد خاطئ أخر حول الأمن السيبراني وهو "ليس لدي أي معلومات مهمة أو بيانات حساسة على جهازي"

الحقيقة: في البداية اسمح لنا أن نسألك هذا السؤال

هل انت متأكد من أنه لا يوجد لديك أي شيء مهم أو ذو قيمة على جهازك؟

ألا تقم بحفظ كلمات السر ضمن المتصفحات؟ أليس لديك سجل للتصفح؟ ألا تقوم بإرسال رسائل بريد الكتروني تحوي على مستندات أو معلومات أخرى؟ هل تعتقد بان بياناتك غير مهمة بالنسبة لمجرمي الانترنت؟

هل تعلم بأن مجرمي الانترنت يمكنهم جمع معلومات عنك من مصادر مفتوحة كوسائل التواصل الاجتماعي والمنتديات والمواقع الأخرى ويمكنهم الحصول على عنوان البريد الالكتروني ورقم الهاتف الخاص بك ويمكنهم لاحقاً استخدام هذه المعلومات للقيام بسرقة هويتك على شبكة الانترنت أو لاستخدامها ضدك والأمر الأهم الذي يجب أن تدركه هو حتى لو لم يكن لديك معلومات مهمة على جهازك فيمكن ان يتم اختراق جهازك ليكون ضمن شبكة bot ويتم استخدامه لتنفيذ هجمات على جهات أخرى

النصيحة رقم 81: هل استخدام مضاد الفيروسات يجعلني آمن بنسبة 100%

لقد قمت بتنصيب مضاد فيروسات قوي وله تقييمات جيدة وهذا يعني أنني محمي بنسبة 100% ولا يمكن لأحد ان يقوم بمهاجمتي أليس كذلك؟

هذا الاعتقاد خاطئ، مضاد الفيروسات ضروري للحماية ولكنه غير كافي ويجب عليك أن تستخدم أكثر من طبقة للحماية وفي حال فشل إحدى الطبقات سيكون لدى الطبقات الأخرى فرصة لكشف او منع التهديد

- مضاد الفيروسات غير قادر على كشف الهجمات التي تتم باستخدام برمجيات متطورة
- مضاد الفيروسات غير قادر على حمايتك عندما تقوم بفتح الروابط الخبيثة والمزورة

- مضاد الفيروسات غير قادر على حمايتك إن لم تقم بتحديث قاعدة البيانات الخاصة بالتوقيعات الرقمية ضمنه
- مضاد الفيروسات غير قادر على حمايتك من هجمات التصيد الاحتيالي

نحن لا نقول لك أن مضاد الفيروسات غير ضروري على العكس فهو ضروري جداً ولكنه غير كافي

النصيحة رقم 82: لا ضرر بالبحث أو فتح رسائل البريد العشوائي spam

كنت أتوقع انها وثيقة مهمة أو صور مرسلة من قبل صديق لي؟ ماذا لو كانت الرسالة مهمة وانتهى الأمر بها عن طريق الخطأ ضمن البريد العشوائي أو الغير مهم؟

هذه هي الطريقة التي تبدأ بها معظم القصص حول الإصابة بالبرمجيات الخبيثة، إليك بعض التلميحات التي ستساعدك على معرفة اكتشاف الأمور المريبة:

- الإشارة الأولى: إذا انتهى الأمر برسالة في مجلد الرسائل العشوائية او الغير مهمة فمن المؤكد ان هناك أمر مريب بها لذا ثق في تقنية التصفية الخاصة بالبريد العشوائي
- أنت كنت شخص عنيد فالخطوة التالية ستكون إلقاء نظرة على عنوان البريد المرسل، هل هو مطابق لأحد عناوين اصدقائك؟ لا، إذاً فهو ليس شرعي وهنا يجب أن تتحقق من الاختلافات البسيطة بالأحرف والأسماء ممكن أن يتم التلاعب ببعض الأحرف لانتحال شخصيه موقع أو شخص معين

- إن لاحظت وجود مرفقات فانظر إلى امتداد الملف قبل فتحه ويجب أن تدرك خطورة الملفات التنفيذية exe وحتى ملفات word and excel لأنها ممكن ان تحوي على وحدات ماكرو خبيثة تؤدي لاختراق جهازك

النصيحة رقم 83: قم بإيقاف تشغيل وحدات الماكرو macro ضمن ملفات الأوفيس

إن كنت تعتمد على حزمة برامج الأوفيس للقيام بأعمالك فيجب عليك تعطيل وحدات الماكرو

ما هي وحدات الماكرو: هي أجزاء من التعليمات البرمجية المضمنة في مستندات الأوفيس والتي من الممكن أن تكون خطيرة جداً وتجعلك عرضه للاختراق أو الإصابة ببرمجيات خبيثة، لذا قم بتعطيلها واسمح بتشغيلها فقط لملفات محددة عندما يكون المستند قادم من مصدر موثوق بالنسبة لك

النصيحة رقم 84: حافظ على حساب الانستغرام الخاص بك تحت السيطرة من خلال جعله private

هل تريد الحفاظ على نسبة جيدة من الحماية ضمن حسابك على الانستغرام؟

إن لم تكن شخصية عامة أو لم يكن لديك أعمال بحاجة للتسويق عبر الانترنت فيجب أن تجعل ملفك الشخصي على الانستغرام "خاص" وهذا الأمر يسمح لك بمشاركة صورك مع المستخدمين الذين تختارهم فقط مثل أصدقائك المقربين وأفراد عائلتك

عندما تجعل حسابك خاصاً هذا يعني أنك ستتحكم بمن يرى صورك ومقاطع الفيديو التي تقوم بنشرها وفي كل مرة يريد شخص متابعتك يجب عليه الحصول على موافقتك أولاً

النصيحة رقم 85: كيف تعرف فيما إذا تم اختراق حسابك

في يومنا الحالي هناك اختراقات تتم بشكل يومي وقد تتساءل فيما إذا كان حسابك من ضمن الحسابات المخترقة؟

أليك بعض الأمور التي تساعدك على معرفة ذلك:

- الإنذارات الخاصة بالاختراقات: من خلال متابعة أخبار الحماية والتكنلوجيا بشكل عام يتم نشر أخبار عن اكتشاف اختراقات وتسريبات لقواعد البيانات الخاصة بمواقع او خدمات معينة
- موقع have I pwned والذي يسمح له بمعرفة فيما إذا كان عنوان البريد الالكتروني الخاصة بك ضمن التسريبات أو الاختراقات التي تمت

النصيح رقم 86: حافظ على الحماية للتطبيقات من الطرف الثالث

من المؤكد أنك قد قمت بتسجل الدخول باستخدام حساباتك على مواقع التواصل الاجتماعي للعديد من التطبيقات من الطرف الثالث كالألعاب أو الخدمات الأخرى

إذا كنت قلقاً من ناحية الخصوصية والحماية فأحرص على الاهتمام بالتطبيقات التي تسمح لها بالاتصال بحساباتك ولديها الحق بالوصول إلى ملفات التعريف الخاصة بك

ومعلوماتك الشخصية لذلك يجب عليك الموافقة فقط على التطبيقات الجديرة بالثقة ومن وقت لآخر قم بتنظيف وحذف التطبيقات التي لم تعد تستخدمها

النصيحة رقم 87: تنظيف تطبيقات الهاتف المحمول

بما أننا نتحدث عن التطبيقات فقد حان الوقت لتقوم بجولة على التطبيقات المثبتة على جهازك المحمول وتحذف الغير مستخدم منها لأنها قد تشكل مخاطر أمنية محتملة ويجب أن تقوم أيضاً بالتحقق من الصلاحيات التي تمنحها لهذه التطبيقات وتعطيل الغير ضروري منها

النصيحة رقم 88: احذر من الذواكر المحمولة USB ومحركات الأقراص الخارجية

لا تقم ابداً بإدخال أجهزة USB أو أقراص خارجية قادمة لك من مصادر غير موثوقة إلى جهازك الحاسب فهي تعتبر أكبر حامل للبرمجيات الخبيثة كالفيروسات وبرامج الفدية وأحصنة طروادة وتأكد من تعطيل خيار التشغيل التلقائي واستخدام برامج مضاد الفيروسات لفحصها

النصيحة رقم 89: فحص الحماية لحساب غوغل الخاص بك

هل قمت بتفعيل خيارات الحماية المتاحة ضمن حساب Google الخاص بك؟

إن لم تكن قد فعلت ذلك لقد حان الوقت للقيام بهذا الأمر، من خلال إعدادات الحماية ضمن البريد الالكتروني قم بمراجعة وتفعيل كل طرق الحماية والخصوصية الممكنة

يجب أن تدرك أهمية الحماية الخاصة بالبريد الالكتروني تخيل وصول المهاجم لبريد الالكتروني عندها سيكون له المقدرة على الوصول لكل حساباتك الأخرى المرتبطة بهذا الحساب

النصيحة رقم 90: لا تكن كسولاً توقف عن حفظ تفاصيل بطاقتك داخل المواقع

توقف عن حفظ تفاصيل بطاقتك على حساباتك عبر الانترنت، لا تقم بهذه العملية ضمن أي مكان بعض النظر عن مدى صغرها أو عدم أهميتها، إن كنت ترغب بشراء شيء ما عبر الانترنت فخذ وقتك وقم بملىء تفاصيل بطاقة الائتمان بكل مرة وبشكل يدوي ممكن أن يستغرق هذا الأمر 30 ثانية ولكنه سيحميك من هجمات ومخاطر أخرى

تخيل أن يصل المهاجم لحسابك ضمن هذا الموقع ، سيمكنه شراء ما يشاء كون معلومات بطاقتك محفوظة داخل الموقع

النصيحة رقم 91: احذر من البرامج الإعلانية Adware

هذا النوع من البرمجيات يعمل على عرض إعلانات على نظامك وعادةً ما تظهر على شكل نوافذ منبثقة مزعجة وتؤدي لإبطاء عمل الجهاز وبعض أنواع هذه البرمجيات ممكن أن لا يكون خطير ولكن البعض الآخر منها ممكن ان يقوم بتتبع نشاطك والتجسس عليك وسرقة معلوماتك الحساسة

النصيحة رقم 92: كيف تعمل مجموعات الاستغلال

ربما قد سمعت بهذا المصطلح من قبل "مجموعات الاستغلال" وهي إحدى الأدوات المستخدمة من قبل مجرمي الانترنت للقيام بهجماتهم من خلال البحث واكتشاف الثغرات ونقاط الضعف في الأنظمة والبرامج والعمل على استغلالها للوصول لجهازك واختراقه والتحكم به

يعتبر استخدام هذه الأدوات أمر سهل ويتم بشكل اتوماتيكي لذلك فهي مستخدمه على نطاق واسع من قبل المهاجمين وأفضل طريقة للحماية هي القيام بعمليات التحديث لكل الأنظمة والبرامج بشكل دائم لأن عمليات التحديث تعمل على إصلاح الثغرات ونقاط الضعف الموجودة

النصيحة رقم 93: أنواع البرمجيات الخبيثة التي يمكن أن تتواجد على شبكة الانترنت

ربما قد تسألت عن أنواع البرمجيات الخبيثة الموجودة على شبكة الانترنت وما هي الاختلافات بينها؟

إليك شرح سريع عن أنواع البرمجيات الخبيثة:

- **Adware:** برامج الإعلانات والتي تقوم بعرض إعلانات سيئة وتقوم بجمع المعلومات عنك ومن الممكن أن تقوم أيضاً بإصابة جهازك بأنواع أخرى من البرمجيات الضارة

- **Bot:** أكواد برمجية ضارة تعمل على إصابة جهازك وجعله جزء من شبكة متحكم بها لتنفيذ هجمات او أمور مؤذية أخرى
- **Ransomware:** برامج الفدية والتي تعمل على تشفير ملفاتك ومنعك من الوصول لها ومطالبتك بدفع مبلغ مالي كفدية للقيام بعملية فك التشفير
- **Rootkit:** نوع من البرمجيات الخبيثة يمنح المهاجم إمكانية الوصول لجهازك بطريقة خفية يصعب على مضاد الفيروسات اكتشافها
- **Spyware:** برامج التجسس والتي تعمل على تتبع نشاطك كعادات التصفح وتسجيل كل حرف تقوم بكتابته وسرقة معلوماتك المالية وترسل هذه الأمور لسيرفر خاص بالمهاجم
- **Trojan Horse:** أحصنة طروادة والتي يمكنها إخفاء نفسها ضمن برامج تبدو على أنها برامج شرعية لخداع المستخدم ليقوم بتثبيتها على جهازه
- **Virus:** الفيروسات والتي يمكنها نسخ نفسها والانتشار ضمن الأنظمة الأخرى من خلال إرفاق نفسها بملفات وبرامج أخرى وتعمل على تنفيذ تعليمات ضارة على الجهاز المصاب
- **Worm:** الديدان والتي تنتشر بشكل تلقائي داخل الشبكة وتعمل على استهلاك موارد النظام ولها القدرة على الانتشار والتكاثر بشكل ذاتي دون أي تفاعل من المستخدم

النصيحة رقم 94: القلق من مخاطر برامج الفدية

هل أنت قلق من مخاطر برامج الفدية؟

أليك أفضل طريقة لمواجهة هذا التهديد وهو النسخ الاحتياطي لملفاتك ومعلوماتك المهمة بشكل دوري وعندها حتى لو تعرضت لهذا الهجوم وتم تشفير ملفاتك فيمكنك الوصول لها من النسخة الاحتياطية

النصيحة رقم 95: مبادئ أمن المعلومات الأساسية

على الرغم من ان أمن المعلومات يعتبر مصطلح عام ولكن يمكن تعريفه على انه الإجراءات المتبعة للحفاظ على سرية وسلامة وإمكانية الوصول للمعلومات وحمايتها من أي وصول غير مصرح به أو من التعديل والتلاعب أو من منع إمكانية الوصول لها

عناصر أمن المعلومات الأساسية هي:

عناصر أمن المعلومات الأساسية هي السرية Confidentiality والسلامة integrity والتوافر أو إمكانية الوصول للمعلومات availability والتي يشار لها باسم مثلث CIA

- **السرية:** هي عدم كشف المعلومات للأشخاص الغير مصرح له برؤية هذه المعلومات وأفضل طريقة لتطبيق السرية هو تشفير المعلومات.
- **السلامة:** هي القدرة على التأكد من أن البيانات لم يتم التلاعب بها أو تغيرها وهذه العملية لا تنطبق فقط على البيانات بل على الأنظمة أيضاً للتأكد من

أن إعدادات السيرفر أو أجهزة الشبكة أو أجهزة الحماية لم يتم التلاعب بها وتغيرها

- **التوافرية:** تشير إلى إمكانية الوصول للمعلومات من قبل الأشخاص المصرح له بذلك في أي وقت وبدون أي قيود أو معوقات

النصيحة رقم 96: المعتقدات الخاطئة حول الأمن السيبراني – الجزء السادس

"في حال تعرضي للاختراق أو للإصابة ببرمجية خبيثة فسوف ألاحظ ذلك"

الحقيقة هذا الأمر كان في الماضي عندما كنت تلاحظ بطئ في عمل الجهاز أو ظهور النوافذ المنبقة ولكن يجب أن تدرك بان الهجمات في يومنا الحالي تتم باستخدام طرق وتقنيات متقدمة ويصعب اكتشافها ولن تلاحظ وجودها أو إصابة جهازك بها

النصيحة رقم 97: ما هي شبكات البوت botnet

لقد قمنا بتعريفها بشكل سريع عند الحديث عن النصيحة الخاصة بأنواع البرمجيات الخبيثة

Botnet: هي نوع من البرمجيات الخبيثة وتسمح للمهاجم بالتحكم بشبكة من الأجهزة المصابة لتنفيذ هجمات أو اعمال ضارة أخرى والتي يمكن ان تختلف من إرسال رسائل البريد العشوائي Spam إلى حملات التصيد الاحتيالي إلى هجمات منع الخدمة الموزعة DDoS ، يمكن للمهاجم التحكم بهذه الشبكة من الأجهزة المصابة

عن بعد لخدمة مصالحه وهذا الأمر يسمح له بالتخفي ومنع كشفه من قبل الجهات القانونية

النصيحة رقم 98: كيف يعمل مضاد الفيروسات

هل تسألت يوماً ما كيف يعمل مضاد الفيروسات؟ إليك الإجابة على هذا السؤال

مضادات الفيروسات تستخدم طرق مختلفة من أجل كشف البرمجيات الخبيثة وأكثر هذه الطرق شيوعاً هي كشف البرمجيات عن طريق التوقيع الرقمي Signature حيث يحوي مضاد الفيروسات على قاعدة بيانات فيها التوقيعات الرقمية الخاصة بالبرمجيات الخبيثة وهي عبارة عن أكود رقمية مميزة وعندما يتم فحص البرمجية من قبل مضاد الفيروسات فهو يقوم بمقارنة الأكواد الخبيثة ضمن قاعدة البيانات الخاصة به مع الكود الخاص بالبرمجية التي يقوم بفحصها ومن ثم يظهر نتيجة الفحص فيما إذا كانت هذه البرمجية التي تم فحصها سليمة أو أنها عبارة عن برمجية خبيثة.

طريقة أخرى تستخدمها مضادات الفيروسات تعتمد على Heuristic-based Method حيث يتم التعرف على البرمجية الخبيثة من خلال سلوكها المشبوه والمثير للشك وهذه الطريقة فعالة ومفيدة ضد الأنواع الجديدة من البرمجيات الخبيثة

النصيحة رقم 99: كيف ترتبط حساباتك على الانترنت

هل فكرت يوما ما في الآلية المستخدمة لربط حساباتك على شبكة الانترنت؟

هل تعتقد أن هذا الأمر غير مهم بالنسبة لمجرمي الانترنت؟ دعنا نوضح لك ذلك:

يحوي عنوان البريد الالكتروني الخاص بك على معلومات مهمة عن جميع حساباتك بالإضافة للمعلومات الحساسة حول عملك وحياتك الشخصية

- وصول المهاجم لبريدك الالكتروني سيسمح له الوصول لحسابك على الفيسبوك والذي يحوي على معلومات شخصية عنك بالإضافة لأصدقائك وعائلتك وتفضيلاتك والأمور التي تهتم بها وتتابعها والأماكن التي قمت بزيارتها
- وصول المهاجم لبريدك الالكتروني سيسمح له بالوصول لحسابك على Amazon وسوف يتعرف على الأمور التي تقوم بشرائها وقائمة الرغبات الخاصة بك ومعلومات الشحن وعنوانك وتفاصيل بطاقتك الائتمانية، القائمة تطول وتطول

هل أنت متأكد من أن بياناتك ليست مهمة وليس لديك ما تخشى عليه من الاختراق، مجرمو الانترنت يمكنهم الوصول لك بألف طريقة

النصيحة رقم 100: لماذا لا يجب عليك ابداً إعادة استخدام نفس كلمة السر

بعد الحديث عن طريقة ربط الحسابات عبر شبكة الانترنت تخيل ماذا سيحدث إذا تمكن المهاجم من الوصول لكلمة السر الخاصة بأحد حساباتك على شبكة الانترنت، على سبيل المثال حسابك على الفيسبوك

هل تستخدم نفس كلمة السر في مواقع أخرى؟ إذا كانت الإجابة نعم يؤسفنا إعلامك بأن المهاجم لن يوفر هذه الفرصة وسيقوم بالوصول لكل حساباتك التي لها نفس كلمة السر

هل تسمع بالتسريبات الخاصة بالمواقع، هذا الأمر خطير جداً ويجب أن تدرك أن استخدامك لنفس كلمة السر في أكثر من مكان سيعرضك للخطر في حال تمكن المهاجم من الوصول لكلمة السر الخاصة بك بأحد المواقع من خلال مهاجمتك او من خلال البحث ضمن التسريبات باستخدام عنوان بريدك الالكتروني

لذا تأكد من استخدام كلمة سر قوية وفريدة لكل حساب وبالتأكيد سيكون من الصعب عليك تذكر كل هذه الكلمات في هذه الحالة يمكنك استخدام تطبيق خاص لإدارة كلمات السر وعندها ستحتاج لحفظ كلمة سر واحدة قوية للدخول لهذا التطبيق وستكون باقي كلماتك السر محفوظة داخل هذا التطبيق

النصيحة رقم 101: قم بإدارة نشاط الصوت والصورة ضمن غوغل

هل تعلم بأن غوغل يحتفظ بتسجيلات صوتية لك ضمن حسابك ليتمكن من معرفة صوتك عند استخدام ميزات البحث الصوتي ولكن إن كنت تفضل الحفاظ على خصوصيتك فقم بالوصول إلى Voice & Audio Activity وقم بحذف العناصر الموجودة داخلها

النصيحة رقم 102: أفضل تطبيقات المراسلة المشفرة

التشفير هو طريقة للحفاظ على سرية المعلومات لمنع الأشخاص الغير مصرح لهم بالاطلاع على هذه المعلومات

استخدام التشفير ضمن تطبيقات المراسلة الفورية أمر مهم جداً فهو يؤمن الحماية والخصوصية للمستخدم لذا تأكد دائماً من استخدامك لتطبيقات المراسلة الفورية الموثوقة والتي تعتمد على خوازميات تشفير قوية

مبدئياً ننصحك باستخدام التطبيق Signal كونه من أفضل التطبيقات من ناحية الخصوصية والأمان

النصيحة رقم 103: تحقق من عناصر الحماية التالية ضمن مواقع الويب الخاصة بالخدمات المصرفية

ربما قد سمعت عن البرمجيات المالية الخبيثة وإن لم تسمع بها فيجب عليك أن تقرأ عنها وتعلم التكتيكات والأساليب المستخدمة لخداعك وسرقة أموالك، التالي هو بعض الأمور التي يجب التحقق منها قبل إجراء أي معاملة مالية عبر الانترنت:

- تحقق من أن موقع الويب يستخدم التشفير من خلال النظر إلى بداية الرابط ضمن شريط العنوان هل يبدأ ب https وهذا يدل على أن بياناتك سيتم نقلها بشكل آمن من وإلى سيرفرات الموقع
- تحقق من الروابط وتأكد من انها روابط صحيحة ولا تحوي على أحرف مبدلة أو أخطاء إملائية ويجب أن تدرك بأن هذا الأسلوب متبع من قبل المهاجمين لتقليد او محاكة المواقع الموثوقة او المشهورة ليمكنوا من خداع المستخدمين
- تحقق من حقول تسجيل الدخول هل تحوي على حقول إضافية غير المعلومات المعتادة، لن يطلب منك أي بنك معلومات بطاقتك أو رقم التعريف الشخصي الخاص بك أثناء عملية تسجيل الدخول وإذا رأيت مثل هذا الأمر في مكان لا يتوقع وجده به فأغلق الموقع واتصل بالبنك وتأكد من طريقة إتمام المعاملة بشكل آمن
- تحقق من الصور والشعارات الموجودة ضمن الموقع غالباً ما يحاول مجرمو الانترنت تقليد صفحات تسجيل الدخول الخاصة بالبنوك أو التعاملات المالية وإذا

وجدت أي أمر مثير للشك فقم بالبحث عبر غوغل عن المواقع الرسمية وقارن بينها واتصل مع البنك وأبلغهم عن الأمر

- تحقق من تذييل الموقع وتأكد من المعلومات الموجودة فيه إذا كانت معلومات حقيقية عن البنك او الشركة وكلما كانت المعلومات المكتوبة بشكل غير احترافي فهذا يعطي المزيد من الشك وعدم الثقة

النصيحة رقم 104: مثال على محاولة تصيد

أعتقد أن الأمثلة هي أفضل طريقة لفهم هجمات التصيد الاحتيالي لنرى هذا المثال لنفهم كيف تتم هجمات التصيد الاحتيالي على PayPal

وصلتك رسالة عبر البريد الالكتروني لها العنوان "راجع بيان حساب PayPal الخاص بك"

عزيزي العميل نحن نتفهم أنه من المحبط عدم الوصول الكامل إلى حساب PayPal الخاص بك ونريد أن نعمل معك لإعادة حسابك إلى طبيعته في أسرع وقت ممكن كجزء من إجراءاتنا الأمنية نتحقق بانتظام من نشاط حسابات المستخدمين ونطلب المعلومات لأننا اكتشفنا نشاط وتحويلات غير طبيعة تتم باستخدام حسابك لذا قم بتحميل الملف المرفق للتحقق من ملف التعريف الخاص بك واستعادة الوصول إلى حسابك بشكل كامل، تأكد من إدخال المعلومات بدقة وحسب التنسيق المطلوب واملئ كل الحقول المطلوبة.

شكراً لانضمامك إلى ملايين الأشخاص الذين يعتمدون علينا لإجراء معاملات مالية آمنة حول العالم

ما هي العلامات المثيرة للشك التي لاحظتها:

- عنوان البريد المرسل والذي من الممكن أن يبدو عنوان منتحل او غير شرعي
- البنوك والشركات التي تعمل على تقديم الخدمات المالية لا تقوم ابداً بإرسال الملفات المرفقة وتطلب من العملاء تنزيلها

بعض النصائح الخاصة بالحماية من هجمات التصيد الاحتيالي:

- استخدام حلول الحماية ومضادات الفيروسات القوية:

يمكن أن يساعد مضاد الفيروسات على الحماية من هجمات التصيد الاحتيالي لأنه مصمم لفحص الملفات بحثاً عن أي أثر للأكواد الخبيثة وعند اكتشاف أي تهديد سيتم منع تنفيذ الملف المصاب وهذا يمنع من إيصال الحمولة الخبيثة لهجمات التصيد لذلك يجب على الشركات استخدام مضادات الفيروسات من الجيل الجديد NGAV – next-generation anti-virus والتي تملك ميزات فحص متقدمة بالإضافة إلى احتوائها على جدران نارية بشكل مدمج مما يجعلها خيار مناسب جداً للحماية ضد العديد من الهجمات المتقدمة

- تحديث المتصفحات بشكل دائم:

يسعى المهاجمون لاستغلال الثغرات الأمنية الموجودة في البرامج والتطبيقات القديمة للوصول للأنظمة واختراقها ولسوء الحظ فإن المتصفحات هي الأكثر عرضة لمثل هذا النوع من الهجمات

يعمل المطورون على إصدار تصحيحات الأمان وإصلاحات الثغرات وإيصالها عبر التحديثات ولكن للأسف يفشل العديد من الأشخاص في تثبيت التحديثات في الوقت

المناسب مما يجعل أجهزتهم عرضة للهجمات والتهديدات المختلفة ولإصلاح هذه الأخطاء تحتاج المؤسسات لأداة تدير عمليات التحديث وإصلاح الثغرات الأمنية بشكل تلقائي وهذا النوع من الحلول يعمل على تطبيق الإصلاحات الخاصة بالبرامج والتطبيقات فور إصدارها وهذا الأمر يؤمن سد الثغرات الأمنية بشكل فعال ومنع عملية استغلالها

- استخدام حلول مراقبة وتصفية بيانات DNS:

لزيادة الحماية الرقمية للشركات نوصي باستخدام حلول تصفية وفلترة لحركة البيانات على مستوى DNS والتي تساعد على إضافة طبقة حماية أخرى وباستخدام هذه الأدوات يمكن فحص حركة البيانات وتسجيلها وتحليلها وحظر الخبيث منها وحظر أي دومينات ضارة أو خبيثة يتم العثور عليها

العديد من الشركات تقدم هذه الحلول والتي تزيد وبشكل فعال من استراتيجية الوقاية من هجمات التصيد والهجمات الأخرى من خلال الحماية ضد الروابط الخبيثة وهذا يمنح الشركة طبقة للحماية ضد الهجمات السيبرانية المتقدمة التي تتم من قبل مجرمي الانترنت بهدف سرقة البيانات الحساسة

- تعطيل النوافذ المنبثقة ومرفقات الماكرو:

كخط دفاع أخر يجب أن تقوم بتعطيل النوافذ المنبثقة ومرفقات الماكرو وهما وسيلتان يتم من خلالهما في معظم الأحيان تسليم الحمولة الضارة في هجمات التصيد الاحتيالي ومع ذلك يجب أن تضع في اعتبارك أن هذا الأمر قد يصبح مرهقاً

جداً لمدراء الأنظمة على مستوى الشركات ولكن بالتأكيد هذا الأمر يستحق ذلك لتجنب الأضرار التي يمكن أن تحدث بسبب الهجمات والتهديدات المختلفة

- تطبيق سياسة للإبلاغ عن الحوادث والاستجابة لها:

في النهاية لا يوجد نظام آمن بشكل كامل ولا يمكن لأي وسيلة أن تؤمن لك الحماية بنسبة 100% فمن الممكن أن يتم خداع وتجاوز أقوى أنظمة وحلول الحماية أو خداع أفضل الموظفين تدريباً من قبل جهات خبيثة تستخدم طرق وتقنيات جديدة ومبتكرة وفي حال حدوث ذلك فإن وجود سياسة للإبلاغ عن الحوادث يساعد على التخفيف من حدتها ويحدث فرقاً كبيراً في حجم الخسائر

النصيحة رقم 105: الاتجاهات الرئيسية في الأمن السيبراني بحسب الخبراء

هناك بعض الاتجاهات الرئيسية في عالم الأمن السيبراني والتي تؤثر علينا جميعاً كمستخدمين وهي:

- الدول القومية تعمل على تنفيذ هجمات لسرقة البنوك والتجسس الالكتروني
- لن تختفي برامج الفدية وستستمر بالتطور الدائم مع تقنيات وتكتيكات جديدة وهذا الأمر يرتبط بالجوانب التقنية والغير تقنية وحيل الهندسة الاجتماعية
- الجريمة الالكترونية في ازدياد مستمر
- يربح مجروا الانترنت أموالاً طائلة من برامج الفدية والبرامج الخبيثة المالية الضارة

- لا تزال كلمات السر الضعيفة تمثل أكبر المخاطر على الامن السيبراني والأسواء من ذلك هو إعادة استخدام كلمات السر في أكثر من حساب

النصيحة رقم 106: الإصابة بدون معرفة المستخدم

الهجمات التي تتم بدون معرفة المستخدم من خلال استغلال ثغرة في متصفح أو تطبيق قديم فمثلاً عندما تتصفح موقع معين وتلاحظ وجود إعلان وهذا الإعلان يحوي على أكواد خبيثة تقوم بفحص نظامك بشكل اتوماتيكي واكتشاف الثغرات واستغلالها ولن تعرف ابدأ ما حدث في الخلفية لذا ننصحك دائماً بتحديث كل الأنظمة والبرامج واستخدام أكثر من طبقة للحماية

النصيحة رقم 107: قم بمراجعة الأجهزة التي قمت بتسجيل الدخول منها لحسابك على الفيسبوك

يحتاج الأمر لدقيقتين فقط قم بالانتقال لإعدادات الحماية في الفيسبوك واختر التبويب الحماية والأمان وتأكد من الأماكن التي تم فتح حسابك بها وإن وجدت أحد الأجهزة الغريبة قم بإنهاء الجلسة وتغيير كلمة السر

النصيحة رقم 108: هل حسابك موجود ضمن البيانات المسربة للمواقع المخترقة

عندما يتم تسريب معلومات المواقع المخترقة سيؤثر هذا الأمر عليك بدون معرفتك لذا تأكد دائماً من أن عناوين البريد الالكتروني الخاصة بك غير موجودة ضمن هذه التسريبات، يمكنك القيام بذلك من خلال الموقع have I pwend وللتقليل من الضرر إليك بعض النصائح:

- حافظ على هدوئك وقم بتغيير كلمة السر للحساب المسرب وتأكد من استخدام كلمة سر جديدة قوية وفريدة وغير مشابهة للكلمة السابقة
- قم بتفعيل المصادقة الثنائية فهي تؤمن لك طبقة حماية إضافية وتمنع المهاجم من الوصول لحسابك حتى لو تمكن من الحصول على كلمة السر الخاصة بك
- في حال كنت تستخدم نفس كلمة السر ضمن أكثر من حساب توقف عن ذلك من فضلك وقم بتغيير كلمات السر لتكون كلمة فريدة لكل حساب
- استخدم تطبيق مدير كلمات السر لمساعدة في حفظ كلمات السر الفريدة

النصيحة رقم 109: توقف وتحقق قبل القيام بعملية النقر

النقر على الروابط التي لا تعرف إلى أين ستأخذك ليس بالأمور الجيد من وجهة نظر الحماية، لا يهم إن كنت قد تلقيت هذا الرابط من مديرك في العمل او شريكك او أحد أصدقائك أو حتى أحد اقاربك، إذا كنت لا تريد أن ينهي الأمر بك في فخ التصيد الاحتيالي أو البرامج الضارة فتحقق من الروابط قبل النقر عليها من خلال تحريك الماوس فوق الرابط ورؤية العنوان الذي سيوجهك إليه أو نسخ عنوان الرابط وفتحه من مواقع على شبكة الانترنت تسمح لك بعرض محتوى الروابط التي ترغب بها

النصيحة رقم 110: توقف عن الكسل عندما يتعلق الأمر بالأمن السيبراني

عندما يتعلق الأمر بالعادات الصحيحة الخاصة بكلمات السر فنعلم أننا أحياناً نبدو كالأم المزعجة، "أفعل هذا" ، "لا تفعل هذا" من خلال النصائح التي تطلب منك استخدام كلمة سر قوية وطويله تحوي على أرقام وأحرف ورموز وأجعل كلمة السر فريدة ولا تستخدمها في أكثر من حساب

نعم الأمن السيبراني صعب ويحتاج للوقت وهو يستحق هذا العناء لذا خذ الوقت الكافي لتطبيق النصائح السابقة لكل كلمات السر الخاصة بحساباتك

أنت لا تستخدم نفس المفتاح للسيارة وللمنزل لأنك إذا فقدته سينتهي بك الأمر بسرقة منزلك وسيارتك إذا لماذا لا تقوم بنفس الأمر ضمن حياتك الرقمية

النصيحة رقم 111: البرامج الضارة المكتوبة بلغة جافا سكريبت

لا تقلق لن نخوض بالتفاصيل التقنية ولكن يجب عليك معرفة ذلك، تعد البرامج الضارة المكتوبة بلغة البرمجة JavaScript تهديد متزايد وله تأثير كبير كون هذه اللغة مستخدمة في معظم مواقع الويب التي نتصفحها بشكل يومي

النصيحة رقم 112: شاهد Mr. Robot

ننصحك بمتابعة مسلسل Mr. Robot من خلال مشاهدته ستحصل على نظرة عميقة عن كيفية حدوث الهجمات والاختراقات وقد يساعدك أيضاً في معرفة الدوافع التي تكون وراء هذه الهجمات

النصيحة رقم 113: كيف تحمي جهازك من خلال طبقات متعددة

أفضل طريقة للحماية عبر الانترنت هي الطبقات المتعددة وهذا الأمر يتم من خلال استخدام أكثر من نظام أو برنامج للحماية مثل مضاد فيروسات وبرنامج خاص لاكتشاف البرمجيات الخبيثة المتقدمة وبرامج كشف ومنع الاختراق

النصيحة رقم 114: كيف يمكن أن يصاب جهازك بالبرمجيات الخبيثة أثناء نقل الملفات

مجرمو الانترنت يستغلون أي شيء يمكن استغلاله لكسب ثقتك وخداعك لتنزيل برامج ضارة وهذا الأسلوب متبع على نطاق واسع حيث يعمل مجرمو الانترنت على تزوير رسائل البريد الالكتروني لتبدو على أنها قادمة من مصادر موثوقة ومشهورة وبمجرد النظر لهذه الرسائل ستبدو على أنها رسائل حقيقية وسينخدع المستخدم ويقوم بالضغط او تحميل وفتح المرفقات

النصيحة رقم 115: لا شيء مجاني على شبكة الانترنت

يجب ان تدرك جيداً هذا الأمر، التطبيقات والبرامج المجانية هي ليست بالفعل مجانية فأنت تمنحها حق الوصول لبياناتك ومعلوماتك الشخصية

النصيحة رقم 116: كيفية اختيار مزودي الخدمة

كيف اختار مزود خدمة يحافظ على أمان معلوماتي؟

غالباً ما نشارك معلوماتنا الشخصية مع جميع أنواع الشركات والمؤسسات ونحن نفعل هذا الأمر طوال الوقت وهذا لا يعني أن هذه المؤسسات حريصة على الحفاظ على أمان بياناتنا، لذا عند اختيار مقدم الخدمة يجب أن تضع في اعتبارك الأمور التالية:

- السمعة العامة للشركة
- الحوادث الأمنية السابقة (بحث بسيط ضمن غوغل يمكن أن يظهر ذلك)
- ما مدى الحماية المطبقة ضمن الموقع

- ما مدى تركيز الموقع على مسائل الخصوصية (هل يحوي الموقع على تفاصيل سياسة الخصوصية وشروط الاستخدام)
- ما مدى سهولة الاتصال بالشركة إذا كنت بحاجة لذلك (هل يوجد معلومات للاتصال أو ما مدى توفر دعم العملاء على وسائل التواصل الاجتماعي)
- ما كمية ونوع البيانات المطلوبة منك

النصيحة رقم 117: تتبع حركة بيانات الويب الخاصة بك على الخريطة العالمية

هل سبق لك تخيل كيف تبدو حركة البيانات على شبكة الانترنت؟

هل تعلم إلى أين يذهب طلبك عندما تطلب موقع ويب معين؟

يمكنك تتبع حركة البيانات الخاصة بك من خلال الأداة التالي:

https://traceroute-online.com

الأمر يتم خلال ثواني معدودة وهذا يساعدك لفهم مدى سرعة عمل الهجمات الإلكترونية وعمليات إعادة التوجيه إلى صفحات ومواقع ضارة

النصيحة رقم 118: كيف تمنع غوغل من تتبعك وتتبع أطفالك

الخصوصية والأمان مرتبطان بشكل وثيق ولا يمكن الحصول على واحد منهم دون الأخرى وعندما يتعلق الأمر بالأشخاص الذين نحبهم لا يوجد شيء لا نفعله لحمايتهم، وهذه بعض الأمور التي يمكن أن تساعد في ذلك:

- إيقاف التتبع
- إيقاف الإعلانات المرتبطة بالاهتمامات
- استخدام محركات بحث بديلة

النصيحة رقم 119: لماذا يسرق المهاجمون سجلات الرعاية الصحية

نسمع بشكل دائم أخبار متعلقة بتسريب البيانات الخاصة بالمنظمات الصحية وإذا كنت تتسأل عن سبب استخدام مجرمي الإنترنت لأدواتهم ومهاراتهم لاستهداف مؤسسات الرعاية الصحية فإليك بعض الإجابات:

- تحوي سجلات الرعاية الصحية على معلومات قيمة بالنسبة لمجرمي الانترنت كأرقام الضمان الاجتماعي وعناوين المنازل
- المؤسسات الصحية غير مجهزة لحماية المعلومات الشخصية ضد الهجمات المحتملة

النصيحة رقم 120: لا يمكن أن تفقد ما ليس لك

فكر ملياً قبل إنشاء أي شيء رقمي لا تريد كشفه بما في ذلك الرسائل والصور ونفس الأمر للمعلومات الأخرى التي تقوم بنشرها ومشاركتها ضمن مواقع التواصل الاجتماعي ويجب أن تدرك هذا الأمر عندما يتم نشر المعلومات على شبكة الانترنت على نطاق واسع فسيصبح من المستحيل التحكم بها

النصيحة رقم 121: ابتعد عن الشبكات اللاسلكية العامة:

عندما تكون في مقهى جديد ورائع، تجلس وامامك مشروبك المفضل، محاطاً بالإنارة الرائعة وعندها بالتأكيد سوف تأخذ هاتفك وتقرر نشر صور لك على الانستغرام وبالتأكيد سوف تتصل بالشبكة اللاسلكية العامة الخاصة بالمقهى

يجب أن تدرك المخاطر الأمنية للشبكات اللاسلكية العامة كون الاتصال بها يسمح بتتبع نشاطك وحتى إلتقاط كلمات السر الخاصة بك وننصحك باستخدام VPN عند الاتصال بالشبكات اللاسلكية العامة

النصيحة رقم 122: ما مدى أمان متاجر التطبيقات الرسمية

أنا متأكد من أنك قد سمعت مسبقاً عن أهمية عدم تثبيت تطبيقات من خارج المتاجر الرسمة وقد تم تحذيرك من أن التطبيقات من خارج المتاجر الرسمة تشكل تهديد أمنياً لك ولكن يجب أن تدك بإنه مهما كانت الإجراءات التي تتخذها شركات مثل Apple and Google للحفاظ على أمان متاجر التطبيقات الرسمية الخاصة بهم فيوجد بعض التطبيقات الضارة القادرة على تجاوز هذه الإجراءات

يوجد العديد من التطبيقات الخبيثة على المتاجر الرسمية والتي تتطلب سماحيات وأذونات عالية والبعض منها لا يقوم بتخزين البيانات بشكل آمن

النصيحة رقم 123: الأحداث الرياضية الكبرى وتهديدات الأمن السيبراني

الأحداث الرياضية الكبرى هي فرصة رائعة للمحتالين قد لا تستخدم عادةً التطبيقات الرياضية أو مواقع الويب الخاصة بالرياضة ولكنك تصبح من محبي الرياضة أثناء الأحداث الكبرى مثل كأس العالم والألعاب الأولمبية

يستغل مجرمي الانترنت هذه الأحداث لنشر هجماتهم من خلال رسائل البريد الالكتروني المزورة والتي تعرض بطاقات مجانية لحضور المباريات أو أمور مشابهة أخرى ومواقع الرهانات الرياضة لذا كن حذراً من الروابط التي تضغط عليها ومن التطبيقات التي تقوم بتنزيلها أو الصفحات التي تدخل فيها معلوماتك الحساسة

النصيحة رقم 124: جهازك البطيء قد لا يكون علامة للإصابة بالبرامج الضارة

هل جهازك يعمل بشكل أبطئ من المعتاد؟ هل يستغرق الأمر وقتاً أطول لفتح بعض البرامج؟

تميل البرامج الضارة إلى إبطاء النظام وتستهلك من موارد الشبكة والنظام، إذا لاحظت أي شيء من هذا القبيل فتحقق أولاً من بعض الأمور الأخرى فقد تكون المروحة الخاصة بالتبريد مليئة بالغبار وتحتاج إلى التنظيف وإذا لم تجد أي من

الأسباب المحتملة الأخرى عندها يمكنك البدء في التفكير أن جهازك مصاب بالبرمجيات الخبيثة أو انه جزء من شبكة bot يتم التحكم به من قبل المهاجم لتنفيذ أمور أو هجمات أخرى

النصيحة رقم 125: احذر من الموظفين السابقين

إليك الإحصائية التالية المثيرة للقلق، ما يقارب من ثلثي الموظفين يسرقون بيانات الشركة عند الاستقالة أو عند طردهم من العمل لذا تأكد من إزالة كل الصلاحيات للحسابات الممنوحة لهم وكن حذراً بخصوص كلمات السر الخاصة بالحسابات والتي يجب ان يتم تبديلها واستخدام كلمات سر قوية وفريدة وغير مستخدمة مسبقاً وقم أيضاً بتفعيل المصادقة الثنائية لإضافة طبقة حماية أخرى وفعل عمليات النسخ الاحتياطي بشكل تلقائي لضمان عدم فقدان أي من المعلومات المهمة

النصيحة رقم 126: حماية جهازك المحمول من التطبيقات الضارة

إليك بعض النصائح لحماية هاتفك المحمول من الإصابة بالتطبيقات الضارة:

- قم بتثبيت التطبيقات فقط من المصادر المعروفة والموثوقة
- قم بإزالة التطبيقات القديمة والغير مستخدمة
- تخلص من كل التطبيقات التي تتطلب أذونات كثيرة
- حافظ على تحديث كل تطبيقاتك بشكل دائم
- قم بتثبيت برنامج مضاد فيروسات جدير بالثقة

النصيحة رقم 127: قائمة كلمات السر الضعيفة

بغض النظر عن نوع الحساب الذي تستخدمه لا تقم ابداً وتحت أي ظرف من الظروف باستخدام إحدى كلمات السر التالية:

- أي من الكلمات التي تحوي على admin or password
- اسمك الأول أو اسم عائلتك
- اسم أحد ابنائك أو والديك
- اسم حيوانك الأليف
- تاريخ ميلادك
- رقم هاتفك
- رقمك الوطني
- تسلسل من الأحرف أو الأرقام (qwerty – abc123 – 123456)

النصيحة رقم 128: هل تستخدم الرد التلقائي في المكتب؟ لا تكشف الكثير من المعلومات

لقد ذكرنا سابقاً ضرورة عدم كشف مكان وجودك ومدى استفادة المجرمين من هذه المعلومة، لا تقم بتحديد مكان وجودك من خلال منشورات على مواقع التواصل الاجتماعي عندما تكون في الإجازة أو العطل وبغض النظر عن جمال المناظر الطبيعية انتظر لتعود إلى المنزل وقم بذلك لا تعطي فرصة للمجرمين بمعرفة مكان وجودك وخلو منزلك واحرص دائماً على ان تكون المعلومات في الرد التلقائي عندما

تكون خارج المنزل او خارج المكتب لا تحوي على شيء يمكن أن يستفيد منه المجرمون

النصيحة رقم 129: استخدام بطاقة منفصلة للتسوق عبر الانترنت

أسهل وأفضل طريقة للحماية أثناء التسوق عبر الانترنت هو امتلاك بطاقة منفصلة تستخدم فقط لهذا النشاط ويتم تحويل الأموال لها في كل مرة ترغب باستخدامها وخلاف ذلك اتركها فارغة تقريباً وبهذه الطريقة إذا تمكن أحد من اختراق حسابك أو الحصول على معلومات بطاقتك فلن يتمكن من التسبب بضرر جسيم لك

النصيحة رقم 130: تعلم أساسيات الأمن السيبراني