Cyber Security

Raghad Kareem Qasim
Risk Analyst

16 October 2020

التوعية في الأمن السيبراني

قبل ماندخل في تفاصيل حماية حساباتنا لازم نطرح سؤال مهم وهو: ماذا لو أهملنا جانب المعلومات؟

من القصص التي أنتشرت شخص تم إختراق حسابه في Google، بعدها بفترة قصيرة تم إختراق حسابه في Twitter، وبعدها تم إختراق حسابه في Apple ID.

المشكلة أنه بعد إختراق حسابه في Apple ID أستطاع المخترقين أنهم يفرمتوا ويمسحوا جميع البيانات من أجهزته IPhone, iPad and Mac، المختصين عادة مايسمعوا هذه القصص بشكل دائم وعملية حماية نفسك من هذه المخاطر شيء بسيط ممكن تعمله بنفسك ولكن عدم الإهتمام بهذا الجانب ممكن يضر حياتنا ممكن يضر حتى سمعتنا ، كثير من الأشخاص يتم إختراق حساباتهم على Social Media، ويتم إبتزازهم ويتم نشر معلومات عنهم فضلا عن عمل Follow -Like، لأشياء غير محببة عندنا في المجتمع، هذه الأشياء ممكن تضر بسمعة الشخص.

أيضا الأشخاص العاملين في القطاعات الحكومية والشركات تجد أن معظم الملفات الحساسة موجودة في أجهزتها، فلو تم إختراق أحد الأجهزة سيضر بسمعة المؤسسة، لذا يجب علينا اليوم نبدأ في حماية أنفسنا وتوعية أنفسنا في هذا الجانب.

بداية راح نتكلم عن بعض المخاطر المحيطة بنا مثل البرامجيات الخبيثة أو الإصطياد الإلكتروني.

البرامجيات الخبيثة:

إذا أجينا نعرّف البرامجيات الخبيثة هي أي Software Code يتم صنعه لهدف خبيث،ممكن يتم عمله لإختراق جهازك بعد مايخترق جهازك ممكن يفتح Camera ، ممكن يفتح Microphone، ممكن يشوف Location ، ويستخدم لسرقة ملفاتك الخاصة، طبعا Malware لها أنواع عديدة وكل نوع له طبيعته الخاصة ، مثلا إذا تكلمنا عن Viruses ، أو Worms ، لما نتكلم عن Ransomware التي تستخدم في تشفير الملفات، إذا أجينا على أحد الأمثلة المشهورة جدا هو WannaCry .

WannaCry كان نوعا ما مميز لأن يتم الدمج فيه أكثر من طبيعة للبرامجيات الخبيثة كان يستخدم لبرمجة معينة للوصول إلى الجهاز وبعدها يشفر جميع الملفات ويبحث في الشبكة ويخترق الأجهزة الأخرى، وبحسب إحصائية av-test.org، هو موقع مشهور في إختبار مكافحة الفيروسات تم نشر إحصائية على أنه في اليوم الواحد تقريبا يتم الكشف عن 390.000 نوع من البرامجيات الخبيثة لهذا يجب أن نكون واعيين في حماية أنفسنا من هذا العدد الهائل الذي يتم صنعه في اليوم الواحد.

طيب من الأسئلة التي تنتشر بكثرة :

هل البرمجيات الخبيثة فقط تصيب الوندوز؟

الإجابة طبعا لا.

يتم إستهداف أنظمة الوندوز فقط لأن الهكرز يستهدفوا أكبر عدد ممكن من المستخدمين ولكن توجد برامجيات ضارة لجميع الأنظمة صارت تنتشر بكثرة خاصة للأندرويد وأصبحنا نراها حتى في Play Store .

كيف يتم الإصابة بالبرامجيات الخبيثة؟

عادة ماتكون ثلاث طرق رئيسية :

1. هو الضغط على روابط أو مرفقات مشبوهه: (أول ماتضغطها يتم عمل أكشن معين في جهازك).
2. أنك تستخدم برامج غير موثوقة: (أحيانا يوجد أشخاص يثبتوا تطبيق لتشغيل الفلاش مثلا لكن هذا التطبيق من الخلفية يحاول أنه يدخل على الأسماء وياخذها) هذه البرامج طبعا تكون مشبوهه، لهذا يجب أن نتأكد من جميع البرامج التي يتم إستخدامها حتى Permission أو التصاريح التي يتم إعطاؤها.
3. الثغرات: هي عبارة عن ضعف في أما نظام الجهاز نفسه أو ضعف في البرنامج الذي يتم إستخدامه، عادة ماتستخدم نقاط الضعف لتوصيل البرامجيات الخبيثة والأخطر منها لما يتم توصيل البرامجيات الخبيثة والمستخدم لايشعر بهذا الشيء.

الإصطياد الإلكتروني Phishin:

يعرف على أنه هجوم معين، من خلال هذا الهجوم يتم إستهداف شخص معين أو مجموعة أشخاص أحيانا لخداعهم ولجذبهم لعمل شيء معين أما فتح ملف أو فتح رابط معين أو تزويد الهكر بمعلومات خاصة يستفيد منها مثل البطاقات المصرفية وغيرها. وبحسب إحصائية Trustwave في عام 2016 ذكروا على أنه 1 من كل 20 إيميل يتم إرسالها تحتوي على نوايا ضارة Malicious intentions لإستهداف أشخاص معيينين.

كيفية تمييز وحماية نفسك من الإصطياد الإلكتروني؟

الأن عرفنا معنى الإصطياد الإلكتروني وعرفنا إحصائية تبين كثرة إنتشاره، الآن لازم نعرف كيف نميّز هذه الرسائل أو هذه الإيميلات؟ عادة ما توجد نقاط معينة أنت ممكن تميّز بها هذه الرسائل:

1. المبالغة: أن يكون الأمر مبالغ فيه مثلا يجيك إيميل أو رسالة إنك أنت فزت بـ 5000 $ وهو أمر غير معقول
2. الإحساس بالخطر.

كيف ممكن أن نميّز الإيميلات الخبيثة عن الإيميلات العادية؟

عادة مايتم فيها ملف مرفق أو أنه يكون فيها رابط معين، الهكر راح يحاول يجذبك بحيث أنك تضغط على هذا الملف أو على الرابط، وبعد ماتضغط عليهم واحد من الشيئين أنه ممكن يصير أما أن يتم زرع برمجية خبيثة في جهازك لإختراقك أو أنه راح يوديك لصفحة خارجية لسرقة بياناتك، هذه الصفحة تحتوي مثلا على Username و Password إذا حطيت Username الأصلي وPassword الأصلي ماراح تروح للموقع راح تروح للهكر نفسه.

الشيء الثالث الذي يخليك تتأكد أنو الإيميل ماواصلك من PayPal إذا حطيت الماوس على الخانة الزرقاء الموجودة في الإيميل راح يظهر العنوان الأصلي الي راح يوديك للصفحة وهنا راح تتأكد أن هذا الإيميل أبدا ماواصلم من PayPal.

لذا حتى نميّز الإيميلات يجب الإنتباه إلى الأشياء الأساسية التي تم ذكرها :

1. عنوان المرسل.
2. الأخطاء اللغوية الموجودة.
3. تتأكد من العنوان الي راح يوصلك للموقع.

4. من الأمور والنقاط المهمة جدا إذا وصلتك هذه الرسائل لاتضغط على الرابط أذهب لـ Google بنفسك وأبحث عن الموقع أعمل Log in وشوف شنو المشكلة بالضبط، عادة ماراح تشوف أي مشكلة أصلا.

كيف تحمي أجهزتك الإليكترونية؟

بعد ما تعرفنا على بعض من المخاطر التي تحيط بحساباتنا وأجهزتنا لازم نعرف كيف نحمي أنفسنا.

1. مكافح للفيروسات: لما نتكلم عن أجهزة الcomputer نتأكد بداية أنها تحتوي على مكافح الفيروسات وهذا المكافح يتم تحديثه بشكل دوري.
2. Firewall: نتأكد من جدار الحماية يكون مفعّل .
3. تحديث للبرامج: أيضا لازم نتأكد أن النظام نفسه والبرامج الموجوده فيه يتم تحديثها بشكل دوري وآلي لحماية أجهزة الcomputer.
4. عدم الضغط على أي ملف مرفق: حاول أنك ماتضغط على أي ملف مرفق ما متأكد من محتواه ولا متأكد من الشخص المرسل، لاتضغط على أي روابط مشبوهه.

5. إستخدم مواقع مثل VirusTotal للتأكد من خلو هذه الإيميلات أو هذه المرفقات من أي فيروسات ممكن أنها تضر بجهازك. هناك أمر آخر يعتمد على حماية أرقامك السرية وهو حساباتك، إذا ضبطت عملية حماية الأرقام السرية وإستخدامها بشكل صحيح راح تحمي جميع حساباتك ال Online. ولكن من الأمور التي أريد أن أنوه لها هي الأسئلة التي يتم سؤالك عنها في الموقع، لو أفترضنا أنك جيت تفتح حساب في Apple .

بعض الممارسات الخاطئة حول الأرقام السرية:

عادة مايتم سؤالك مثلا عن ما هي أول سيارة إستخدمتها، أول مدرسة درست فيها، المشكلة أنو أحنه نجاوب على هذه الأسئلة بكل صدق والمشكلة الأكبر أو أحنه نشارك هذه المعلومات في وسائل التواصل الإجتماعي (أنا درست هنا، أنا أشتريت هذه السيارة) في ناس ممكن يستغلوا هذه المعلومات لعمل Reset للرقم السري لحسابك و إختراقه، لذلك حاول إنك ماتحط إجابات صحيحة في هذه الأسئلة، إستخدم إجابات أخرى أنت ممكن تعرفها لكن هي ليست حققية أبدا.

وهذا الشيء راح يصعب عملية وصول الناس لمعلوماتك الحقيقية التي ممكن يستخدموها في إختراق حساباتك.

حماية حساباتك وأرقامك السرية:

الآن بعد ماتعرفنا على الممارسات الخاطئة لازم نتعرف على كيفية الإستفادة من البرامج الموجودة للحصول على أكبر حماية لأرقامنا السرية:

1. مثلا ممكن نستخدم Password Managers وظيفة هذا البرنامج يعمل رقم سري صعب مميز لكل موقع.
في مكان معين وللوصول إلى هذه الأرقام تحتاج أنك تحفظ رقم واحد فقط، لو أفترضنا أنك عندك 50 إيميل، كل إيميل راح يحتوي على رقم سري صعب مميز، أنت راح توصل لهذه الأرقام السرية عن طريق حفظ رقم سري واحد فقط، الأمر هذا راح يسهل لك عملية حفظ هذا الرقم السري الصعب وأيضا راح يصّعب على الأخرين أنهم يوصلوا لحساباتك ال Online.

2. تفعيل التحقق بخطوتين: لجميع الحسابات الموجودة لديك، إذا رحت لموقع Two-Factor.org وبحثت عن أي خدمة أو أي موقع راح يخبرك كل خدمات التحقق بخطوتين التي يوفرها الموقع، أنت هنا راح تشوف شنو الأنسب لك وتستخدمه، مثلا ممكن تستخدم الإيميل أو الإتصال (Call) أو حتى ممكن Third Party Two Authentication، مثلا Google Authenticator. مثلا لما نتكلم عن حسابات الOnline ولما نتكلم عن ال Passwordأعتقد أن الجميع ممكن ينسى الرقم السري، ولكن الأهم من ذلك هو كيف أنك تسترجع الحساب بأسرع طريقة؟ المواقع صارت توفر طرق تخليك تحتفظ برقم سري تسخدمه لمرة واحدة، وكيفية الإستفادة من هذه الطرق تختلف من منصة لأخرى ولكن ممكن أنك تروح للإعدادات والSecurity وراح تحصل Additional Method، الي راح تعطيك Password تحتفظ فيه Online وممكن تستخدمه لمرة واحدة فقط.

طرق للمحافظة على توافرية بياناتك:

آخر أمر ضروري لازم نتكلم عنه هو حماية البيانات من ناحية التوافرية، بمعنى عادة مانسمع أنه جهاز أخترق وأنك ماتستطيع أن توصل للبيانات الي فيه أو أنه ممكن يصيب الجهاز Ransomware، بعدها سيتم تشفير جميع البيانات الي فيه وتكون خسرت كلشي.

لهذا دائما حاول أنك تتأكد من وجود نسخة إحتياطية للبيانات المهمة Online، في Google Drive أو غيره، أو حتى Offline في Hard disk خارجي تحتفظ فيه في مكان آمن، هذا الأمر ضروري ولازم ماتستهين فيه أبدا.

الخاتمة:

في الخاتمة خذعا قاعدة بما أنك قبلت على نفسك أنك تستخدم جهاز ذكي لازم تقبل على نفسك أنك تتعلم كيفية حمايته والمحافظة على بياناته، هذه الأمور غير صعبة ولكن تحميك من مخاطر كثيرة.

تم بعون الله