سيشرح هذا الفصل أهمية الوعي في الأمان الرقمي والحفاظ على الخصوصية، ولماذا هو أهم شيء قد تمتلكه أن أردت الدخول في هذا المجال، الأمان الرقمي والحفاظ على الخصوصية. كما سيشرح بعض النصائح النظرية للحصول على مستوىً أعلى من الأمان. الوعي صفة غير موضوعية لا يوجد تعريفٌ مشترك لها. لكن يمكن تعريف الوعي ـ في هذا المجال ـ بصورة عامّة أنّه الأسلوب الذي يتبعه المُستخدم في كل تصرّفاته في العالم الرقمي ليضمن حفاظه على أمانه وخصوصيته بالشكل الذي يريده ويرتضيه. المستخدم الواعي هو من يتبع مجموعة من الإرشادات والقواعد والأساليب المدروسة بصورة صحيحة أثناء استخدامه للأجهزة الرقمية، والمستخدم غير الواعي هو من لا يبالي بذلك. الوعي مَلَكة من الصعب تعلّمها، وهذا لأنّه ليس شيئًا يمكن شرحه كبرنامج أو إضافة متصفّح مثلًا، بل هو أسلوب تفكير وتحليل للمعطيات، فهو مشتقٌ من ذكاء الإنسان وقدرته على التفكير. ولا يُمكن الإشارة للوعي بصورة مباشرة وأن يُقال: هذا هو الوعي فتعلّموه، بل على المرء أن يتعلمه بنفسه ويبنيه مع الزمن. وهو أهم وسيلة دفاع ليمتلكها المُستخدم أثناء قيامه بأيّ عملٍ رقمي، ولهذا جعلناه في مقدّمة هذه السلسلة وقبل الفصول التطبيقية الأخرى، لأنّ كل تلك الأساليب العملية لن تجديك نفعًا إن لم تمتلك المعارف والمهارات والخبرات التي تؤهلك للقيام بها على أكمل وجه، ثم متابعة القيام بها. ما قد يغذّي خزّان الوعي للقارئ هو أن يبحث في المصادر المتوفّرة على الشبكة عن مواضيع متفرقة في علوم الحاسوب؛ كيف يعمل الحاسوب والشبكات والهواتف والأنظمة المختلفة، وما هي آخر الأخبار في مجال الأمان الرقمي
والخصوصية، وما هي آخر الطرق التي استعملها المخترقون ووكالات التجسس للتنصت على المستخدمين... وغير ذلك من المواضيع المتعلّقة بالمجال. يصبح القارئ تدريجيًا واعيًا بكل هذه الأشياء المحيطة به مع مرور الوقت. إليك جملة من النصائح العامة حول أشياء يجب عليك فعلها أو تجنبها من أجل الأمان الرقمي. هذه النصائح مجرّد خطوط عامة لأمور متكررة الحدوث، وليست تفصيلية: احرص دومًا على الحصول على النسخ الأصلية من البرمجيات التي تستعملها. يقوم الكثير من الناس باستخدام برمجيات مُقرصنة (عبر التلاعب بها باستعمال برمجيات تدعى Crack) ظانّين أنه لا يوجد بها شيء، والواقع أنّ معظم هذه البرمجيات تحتوي على برمجيات تجسس أو عرض إعلانات أو إرسال بيانات خفية لا تشعر أنت كمستخدم بها. وهذا واحدٌ من الأسباب التي نستحسن بسببها البرمجيات المفتوحة المصدر (Open Source). لا تقم بتاتًا بتحميل أي برنامج أو ملف من جهة لا تعرفها. يقوم البعض بتحميل برامج ويندوز مثلًا من مواقع كـCNET وغيرها من المواقع الموجودة على الإنترنت، والحاصل هو أن كل هذه البرامج التي تقوم بتحميلها من هذه المواقع تحتوي على برمجيات تتبع لنشاطاتك أو برامج إعلانات أنت في غنىً عنها. متجر iTunes وGoogle Play، أو من المواقع الرسمية لتلك التطبيقات. جميع رسائل البريد الإلكتروني التي تصلك والتي تقول لك أنّك ربحت مبلغ كذا، أو تطلب منك الانضمام لمشروع بنك إفريقي، أو تطلب منك معلومات شخصية عمومًا، أو تطلب منك أن تُراسلهم، تكون هذه الرسائل هي رسائل خداع يرسلها ضعفاء النفوس لمحاولة الاحتيال على الناس. لا تقم حتّى بفتحها ولا الرد على مُرسليها، فقط أرسلها إلى مجلّد السبام. تأتي الكثير من رسائل الاحتيال الإلكتروني بملفّات مرفقة. فيقول لك المُرسل: "افتح الملف المُرفق لمزيد من المعلومات"، والحاصل هو أنّ الملفّات المرفقة هذه تكون محمّلة بفيروس يمكن أن يتسبب باختراقك وسرقة معلوماتك دون أن تشعر. قد تكون الشفرة الخبيثة أو الفيروس موجودة في الرسالة نفسها كمحتوى HTML، 001. png تقوم مثلًا بعض رسائل البريد الإلكتروني بتحويلك إلى موقع مثل facebok. com، وعندما تفتح الصفحة ستجد واجهة شبيهة جدًا بواجهة موقع فيس بوك، com ليس هو نفسه facebook. com ولا يتبع له، بل هو موقع تابع للمُخترقِين مثلًا، وكل البيانات التي تُدخلها هناك سوف تصل إليهم. يُعرف هذا بالتصيد الاحتيالي (Phishing). تتيح معظم مواقع الإنترنت ميّزة الحفاظ على تسجيل الدخول (Stay Signed-In)، وهو غالبًا ما يستعمله معظم المستخدمين لتجنّب إدخال اسم المستخدم وكلمة المرور في كلّ مرة يفتحون به الموقع. لهذا انتبه إلى عنوان موقع الويب الحالي إذا ما طُلب منك إدخال اسم المستخدم وكلمة المرور، فالمُفترض ألّا يحصل ذلك عادةً، لا تشارك بياناتك الحساسة كاسم المُستخدم وكلمات المرور مع أي شخص، مهما كان السبب. حتّى لو كنتَ تثق به فالمشكلة ليست الثقة وحدها بل كيف سيؤمّن هو بياناتك هذه ويحميها من الاختراق كذلك. إذا كنت لا تعرف شيئًا عن موضوع معين أو مشكلة، التصرّف لوحدك قد يتسبب لك بمشاكل إن لم تكن ذا خبرة. فكّر قبل أن تتخذ أيّ إجراء. حول رفع بياناتك وملفّاتك على الشبكة ما لا يدركه الكثير من الناس عندما يشاركون أي شيء على مواقع التواصل ـ بل وحتّى غيرها من المواقع ـ أنّ معظمها تشترط إعطاء حقوق ملكية فكرية كاملة من طرفك لتلك المنصّة. فيس بوك مثلًا ينصّ على ذلك بوضوح في شروط الاستخدام الخاصّة به [1]: ونسخه، وإنشاء أعمال مشتقة منه (بما يتوافق مع إعدادات الخصوصية والتطبيق الخاصة بك). وذلك يعني أنه، على سبيل المثال، إذا قمت بمشاركة صورة على فيسبوك، فإنك بذلك تمنحنا إذنًا يسمح لنا بالحق في تخزينها

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

ونسخها ومشاركتها مع الآخرين (ونكرر، بما يتوافق مع إعداداتك) مثل موفري الخدمات الذين يدعمون خدمتنا أو غير ذلك من منتجات فيسبوك التي تستخدمها. وتنتهي صلاحية هذا الترخيص بمجرد حذف المحتوى الخاص بك من أنظمتنا. تستعمل الشركات الأخرى مثل جوجل الصور التي ترفعها كبياناتٍ لتدريب أنظمة الذكاء الصناعي الخاصّة بها، حيث تُستعمل صورك من أجل تدريبها على التقاط بعض العناصر أو التعرّف عليها، مما يساعد جوجل في تقديم خدمات تجارية لاحقًا للشركات الأخرى [2]: من خلال تسليم أو نشر أو عرض المحتويات، فإنك تمنح Google ترخيصاً دائماً وغير قابلٍ للنقض وفي كل أنحاء العالم وبدون رسوم وغير حصري بإعادة إنتاج وتكييف وتعديل وترجمة ونشر وإنجاز علناً وعرض علناً وتوزيع أي من المحتويات التي تسلمها أو تنشرها أو تعرضها في أو من خلال الخدمات. وهذا الترخيص هو فقط لغرض تمكين Google من عرض وتوزيع وترويج الخدمات ويمكن سحبه بالنسبة لخدمات معينة كما هو محدد ضمن الشروط الإضافية لتلك الخدمات. مشاركتك على موقع Reddit مثلًا تعطي الحق لكل المستخدمين ـ وليس فقط مدراء موقع Reddit – بأن يستخدموا محتواك ويعدّلوه ويعيدوا مشاركته بأي طريقةٍ شاؤوا طالما أنهم يشيرون إلى مساهمتك الأصلية ولا يستعملونها بصورة تجارية. كل المنصّات الرقمية تطلب منك إذنًا شبيهًا عندما تقوم باستخدامها، والمشكلة هي أنّ المستخدم غالبًا ما يوافق على شروط الاستخدام دون أن يقرأ المكتوب فيها. هذا بالنسبة لتعاملك من ناحية الشركات الموفّرة للخدمات، لكن من ناحية الأفراد فالأمر أصعب، وحفظها في مجلّدٍ على أجهزتهم الشخصية وعدم إخبار أي أحد بذلك. ولن تعرف حتّى من هم ولماذا يحتفظون ببياناتك عندهم. لأجل هذا عليك اعتبار كل ما ترفعه على الشبكة من بيانات وملفّات صار منتشرًا عند كل الناس، ولا رجعة فيه. لذلك فكّر مرتين قبل أن ترفع صورك الشخصية أو تعلن عن آرائك الفكرية والسياسية في أي مكان، فلا تدري متى يخرج أحدهم بها ليحاول استخدامها ضدك. شيء مرعب ما يمكنني معرفته عنك دعونا نستعرض ما يمكننا كأفراد معرفته عن بعضنا البعض عبر المعلومات التي ننشرها على الشبكة. ما الحسابات والخدمات الرقمية التي يستخدمها أي مستخدم معاصر اليوم؟ لا بد من أن يستخدم بريدًا إلكترونيًا، وحساب فيس بوك وربما حساب تويتر أو حسابات على مواقع اجتماعية أخرى. ما الذي يمكنني معرفته عنك عبر حسابك على فيس بوك؟ يمكنني رؤية المنشورات العامّة التي تنشرها من نصوص وصور وفيديوهات، كما يمكنني غالبًا رؤية قائمة أصدقائك، والناس الذي يعلّقون عندك ويتفاعلون مع منشوراتك بالإعجابات والتعليقات والمشاركات. كان يمكنني ألّا أرّى شيئًا من هذا إن استخدمت إعدادات الخصوصية المناسبة، لكن للأسف معظم المستخدمين لا يستخدمونها ويتركون كل شيءٍ ليكون مكشوفًا للعموم. الآن إليك بعض الأشياء التي يمكنني معرفتها عنك عبر فيس بوك: يمكنني استخدام مربّع البحث في فيس بوك لرؤية كل الصور أو الفيديوهات التي رفعتَها أنت، أو رفعها أحدٌ آخر وأشار فيها إليك. مربّع البحث في فيس بوك لا يعرض لي المنشورات النصية فقط، بل يعرض لي الصور والفيديوهات كذلك إن أردت البحث عنها. كما يمكنني فلترتها حسب المدة الزمنية. يمكنني استخدام نفس مربع البحث للبحث عن اسمك، ورؤية كل التعليقات العامة التي أجريتها على فيس بوك وكل المنشورات العامة التي نشرتَها في أي مكان منذ تاريخ انضمامك إلى فيس بوك. يشمل هذا المنشورات التي تنشرها داخل مجموعات فيس بوك المختلفة، حيث يمكنني رؤيتها جميعًا عبر البحث عن اسمك في فيس بوك (إن كان المجموعات عامّة، أو حتّى لو كانت خاصّة أو سرّية إن كنتُ أنا أيضًا عضوًا فيها). يسمح فيس بوك لي كذلك برؤية كل المنشورات التي نشرتَها في مجموعة معينة منذ انضمامكَ إليها إن أردتُ ذلك. يمكنني تصفّح قائمة أصدقائك وفتح حساباتهم. ويمكنني الآن استعراض قائمة الإعجابات على منشوراتهم لمعرفة ما يعجبك أنت مما ينشرونه لأعرف المزيد عنك وعن اهتماماتك. كما يمكنني رؤية أي منشورات أو تعليقات ينشرونها عنك أنت على حساباتهم الشخصية، يكثر هذا كثيرًا في الحسابات العائلية على فكرة، حيث ينشر الأب أو الأم الكثير من المعلومات عن أولادهما دون أن يدري الأولاد بذلك. فلمعرفة المزيد عنك قد لا أحتاج الوصول إلى حسابك الشخصي أنت والمعلومات المنشورة فيه، بل يكفيني الوصول إلى حسابات أقاربك ومعارفك وأصدقائك لأعرف المزيد عنك. عبر تجميع كل هذه المعلومات مع بعضها البعض، وقد تُستعمل هذه المعلومات لتعقّبك أو إبداء الأذية لك أو لاستغلالها ضدّك في نشاطاتٍ مختلفة من الحياة اليومية. كلّ ما سبق كان عبر استخدام فيس بوك لوحده، لكن كلما ازدادت المنصّات والخدمات التي تستخدمها على الشبكة، ازدادت معها قدرة الآخرين على معرفة المزيد من المعلومات حولك. وأهم هذه المعلومات هي بريدك الإلكتروني. يظن الكثير من الناس أنّه لا مشكلة في نشر بريده الإلكتروني على العلن، فبالنهاية ما الذي سيفعلون به؟ إنّه مجرد عنوان لاستقبال الرسائل! وهذا للأسف الشديد غير صحيح بالمرّة. عنوان بريدك الإلكتروني سيكشف كامل هويتك الرقمية إن استعملته على أي منصّة رقمية تنشره. على سبيل المثال وهذا من تجربتي الشخصية، حيث كانت الجامعات في تركيا مثلًا تنشر ملفّات PDF بقوائم

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

المقبولين والمرفوضين لديها كل سنة. وللأسف لا يمنعون فهرسة هذه الملفّات من قبل محركات البحث، فكانت هذه الملفّات تظهر بسهولة عند البحث عن اسم الشخص أو بريده الإلكتروني في جوجل، فتظهر لك كل الجامعات التركية التي أرسل لها صاحب البريد الإلكتروني هذا طلب قبولٍ لديها! وهكذا يُمكن لأي شخص أن يحصّل المزيد من المعلومات عنك. ومن الأشياء المهم ملاحظتها حول البريد الإلكتروني هو أنّه عبر إزالة اسم البريد وعلامة @ منه (أي عبر البحث عن testuser بدلًا من testuser@outlook. com) ستظهر المزيد من النتائج عن معظم الناس في محرّكات البحث، وهذا لأن الكثير من الناس في الغالب يستخدمون نفس اسم المستخدم الخاص ببريدهم الإلكتروني كاسم مستخدم كذلك لحساباتهم على فيس بوك وتويتر وغيرها من الخدمات الأخرى. وهذا ما يسبب سهولة العثور عليها جميعًا في نفس عملية البحث. تويتر قصّة أخرى. إذا كان لديك حساب على تويتر فيمكن لأي إنسان أن يستعرض التغريدات التي قمتَ أنت بالإعجاب بها، أو قمتَ بالرد عليها من حسابك على تويتر مباشرةً. يُمكن كذلك عبر ميّزة البحث المتقدم في تويتر أن يستعرض أي إنسان ردودك على ردود حسابات معيّنة؛ فإذا كنت تتفاعل بكثرة مع حساب معيّن مثلًا وقد لاحظ الشخص الذي يبحث عن معلوماتك هذا، فحينها يمكنه أن يقرر رؤية ردودك على تغريدات ذاك المستخدم بالتحديد. وكما الأمر في كلّ المنصات الاجتماعية، حيث لا يمكنك منع الآخرين من الحديث عنك. ربّما قام حساب الجامعة الرسمي التي تدرس فيها مثلًا أو حساب الشركة التي تعمل فيها أو حساب لأي شخص آخر بنشر صورة تكونُ موجودًا فيها ويَذكر اسمك أيضًا. وبمجرّد البحث عن اسمك في أي محرّك بحث فستظهر معلوماتك. هناك أيضًا محرّكات بحث متخصصة للبحث عن أشخاص أو بيانات معينة لهم، على عكس محركات البحث العامّة مثل جوجل وBing مثلًا، فلا تظن أنّه بمجرد عدم العثور على نتائج عنك على جوجل فإنه لا يوجد شيءٌ عنك كذلك. عليك الحرص كذلك على التعليقات والمقالات التي تنشرها في الشبكة، وخصوصًا التعليقات. لكن محرّكات البحث تؤرشفها كذلك. ولهذا فإنّ كل التعليقات التي تدلي بها على المدونات والموسوعات والمواقع الإلكترونية الأخرى... كلّها ستكون ظاهرة عبر البحث عن اسمك. سنتحدث في الفصل اللاحق عن ضرورة استخدام أسماء وهمية في بعض المنصّات وعدم استخدام الاسم الحقيقي. لكن نريد التنويه بصورة سريعة هنا إلى أن كل الحسابات التي تستخدمها على الشبكة وتستعمل فيها نفس الاسم هي حسابات عليك أن تعتبرها بيد كل الناس الذين تراهم في الشارع حولك. لأنّهم جميعًا قادرون على الوصول إليها عبر مجرد البحث عن اسمك بالإنجليزية أو العربية أو أي لغة أخرى.
هوية الإنترنت الوهمية من الأمور التي يقوم الكثير من الناس بها هي أنهم يفصلون بين هويّاتهم المختلفة على الإنترنت. فتجدهم عندما يتصفّحون مواقع مثل Reddit أو حتى فيس بوك وتويتر، يستعملون أسماء وبيانات وهمية لا تعبّر عن هويتهم الحقيقية. بعضهم يفصل بين الحياة المهنية والترفيهية، عليك أنت أن تقرر كذلك ما نوعية الهوية التي تريد استخدامها على الإنترنت؟ الهوية الوهمية تمنحك خصوصية وأمانًا أكبر، وباستثناء المنصّة أو الخدمة التي تتصفحها فهي لديها عنوان الآي بي الحقيقي الخاص بك). إنّك بالطبع تخسر الكثير عندما تشارك على الإنترنت بأسماء وهمية (إنشاء علاقات مع الآخرين باسمك الحقيقي، ونسب مساهماتك لك أنت ونشر اسمك بين الناس. إلخ)، لكن فكّر في عواقب ما تنشره كذلك وهل من المناسب أن يلتصق باسمك وهويتك الحقيقية أم لا؟ إن كان الجواب لا، فحينها عليك استخدام هوية وهمية، والقيام بعددٍ من الإجراءات الأخرى كذلك لحماية نفسك. انتبه إلى أن الخدمة أو المنصّة أو موقع الويب الذي تزوره يمتلك عنوان الآي بي الخاص بك كذلك. وما يفعله الكثير من الناس هو أنهم يقومون بإنشاء حسابين اثنين أحدهما لهويتهم الحقيقية والآخر لهويتهم الوهمية، لكنهم يفعلون ذلك من نفس الجهاز ونفس عنوان الآي بي، تقييم المخاطر والرغبة في الحماية عليك الآن أن تتخذ قرارًا حول درجة الأمان والخصوصية التي تريد الحفاظ عليها. هل تريد مثلًا ألّا يكون هناك أي معلومة أو صورة عنك على الإنترنت على الإطلاق؟ هل تريد أن تفصل حياتك المهنية عن حياتك الترفيهية وتستعمل أسماء وهمية مختلفة؟ هل تخاف من نشر مقالٍ ما لأيّ سببٍ من الأسباب؟ هل أنت على وشك الدخول للسياسة حيث كل معلومة بسيطة عنك قد تُستخدم ضدك في المستقبل من المنافسين؟ الكل عليه محاولة الحفاظ على أمانه الرقمي، لكن إلى أي درجة؟ هذا يختلف بالطبع حسب حالتك. وهذا مهم لأن طرق الحماية والتأمين ستختلف كذلك، وكلّما أردت حماية وخصوصية أعلى، كانت التكاليف من وقت وجهد وصعوبة في الاستخدام أعلى وأكثر. ومن المهم كذلك أن تحدد ضد من تريد الحماية؟ هل تريد حماية نفسك من الشركات الأجنبية التي تستعمل خدماتها مثل فيس بوك وجوجل، أم من الأفراد والمخترقين الخارجيين، أم من أصحاب المواقع التي تزورها، أم من ماذا بالتحديد؟ من الذي يزعجك ويخيفك من بين هؤلاء؟ فكّر بهدوء ثمّ أجب عن الأسئلة التالية: ضد من أريد حماية نفسي؟ ما هي نوعية المعلومات التي لا أريدها أن تتوفر لدى شخصٍ آخر بتاتًا؟ هل نشر هذه المعلومات عنّي بعد 5 أو 20 أو 30 سنة من الآن لن يكون مشكلًا كذلك؟

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي