دليل أنير للسلامة الرقمية

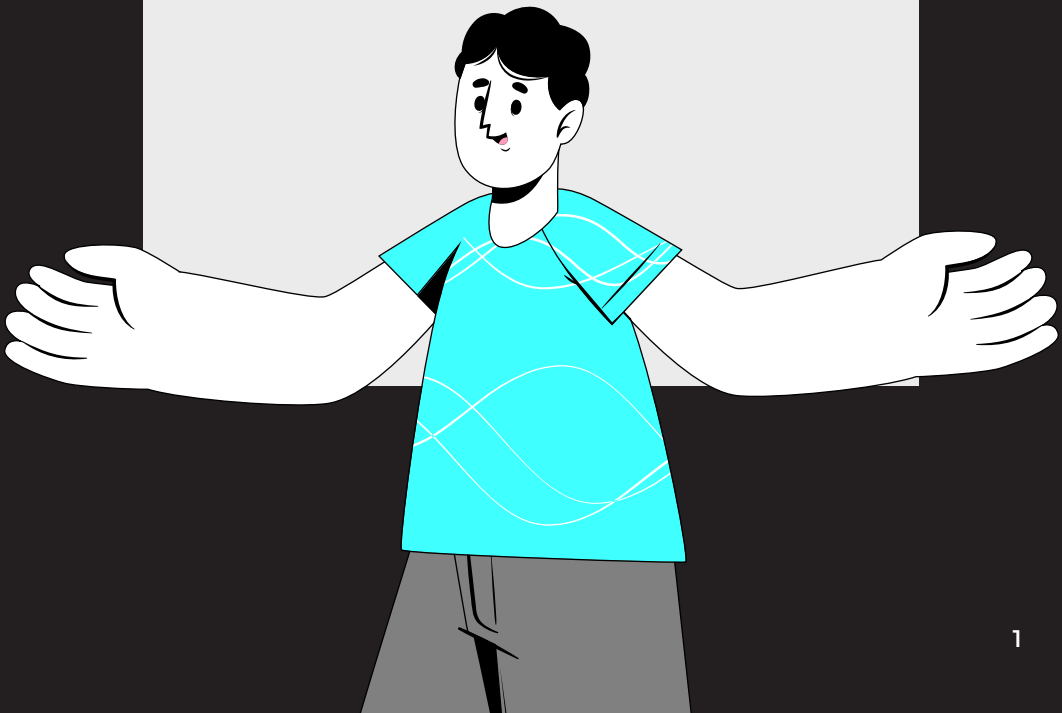
أنـــير

الفهرس

المقدمة

كوسيلة للتعلم والعمل وكذلك الترفيه، يمثل التعامل مع الأجهزة الإلكترونية وبرمجياتها جزءً كبيراً من حياتنا اليومية، ولكن نقص الوعي ببعض الجوانب قد يؤدي إلى سوء الاستخدام؛ الأمر الذي قد يترتب عليه العديد من المخاطر التي تهدد سلامتنا الرقمية وتواجدنا في هذا العالم الافتراضي -عالم الإنترنت-، وهنا تتمثل مسؤوليتك الشخصية بصفتك مستخدم ومُستهلِك، فالوعي والإدراك هما طوق نجاتك في بحر الانتهاكات الرقمية وسلاحك للدفاع عنها.

ولهذا السبب سيكون دليل أنير للسلامة الرقمية مُرشداً لكم في رحلتكم على شبكة الإنترنت، حيث ينقسم هذا الدليل إلى ثلاثة محاور، يتطرق الأول فيها إلى ماهية السلامة الرقمية، والثاني عن الممارسات الآمنة على شبكة الإنترنت، أما الثالث فيتناول أدوات أنير للسلامة الرقمية.



1

السلامة الرقمية

السلامة الرقمية [01]

يشير مصطلح السلامة الرقمية إلى: كل الطرق المختلفة والمتعددة التي يمكن استخدامها في حماية أنفسنا وجعل بياناتنا ومعلوماتنا آمنة وبعيدة عن أي تهديد. كما يمكن تعريف السلامة الرقمية بأنها: مجموعة من الممارسات التي من خلالها نستطيع حماية أجهزتنا الإلكترونية من الهجمات الضارة التي تستهدفها بغية التخريب والضرر.

مصطلح الأمان الرقمي «السلامة الرقمية»: هو مفهوم يشير إلى مجموعة من الممارسات والتدابير اللازم اتخاذها على مستوى الأفراد أو المؤسسات لحماية هويتهم وأصولهم الرقمية من التهديدات والمخاطر أو الوصول الغير مصرح به للبيانات، ويشير أيضًا إلى الحفاظ على الأمان والحماية الشخصية عند استخدام التكنولوجيا الرقمية والاتصالات الإلكترونية.

أهداف السلامة الرقمية

تهدف السلامة الرقمية إلى حماية الأفراد وبياناتهم الشخصية ومعلوماتهم الحساسة من التهديدات والاختراقات والاعتداءات الرقمية، وضمان سلامة استخدامهم للأجهزة الإلكترونية والخدمات الرقمية.

- **تعتبر السلامة الرقمية من ضروريات عصرنا الحالي -عصر التكنولوجيا- وذلك بسبب:**
  - حماية البيانات الشخصية والحفاظ على الخصوصية الرقمية.
  - الوقاية من الاحتيال والاعتداءات الرقمية.
  - الحفاظ على السلامة العقلية والعاطفية.
  - الحفاظ على سلامة الأجهزة والأنظمة.

2

الممارسات الآمنة عبر الإنترنت

الممارسات الآمنة عبر الإنترنت

سنتطرق في هذا المحور من دليل أنير للسلامة الرقمية إلى الممارسات الآمنة التي يتوجب على المستخدم اتباعها في الفضاء الرقمي لتقليل المخاطر وتعزيز السلامة الرقمية.

1. الخصوصية الرقمية [02]

تعرّف الخصوصية الرقمية بأنها: قدرة الأفراد على التحكم في بياناتهم ومعلوماتهم التي تُنشر في الفضاء الإلكتروني، إذ تعتبر الخصوصية حق لكل الأفراد يمكن ممارسته للحد من انتهاك بياناتهم واطلاع الآخرين عليها.

يمكن لهذه البيانات أو المعلومات أن تكون شخصية متمثلة في (رسائل البريد الإلكتروني أو الصور ومعلومات أخرى كمكان العمل أو طرق التواصل)، أو الأفكار والمفاهيم التي يتبناها الفرد والتي تعكس آراءه وترسم صورته داخل الفضاء الإلكتروني.

يتناسب زيادة عدد مستخدمي الفضاء الرقمي -والذي يعد طبيعي نتيجة للتقدم الفكري والتكنولوجي في المجتمع- مع سهولة انتهاك الخصوصية الشخصية للأفراد واستغلالها بطرق مختلفة، من أمثلتها:

- انتهاكات الخصوصية لأغراض تسويقية/تجارية من خلال الإعلانات التي تظهر على مواقع الإنترنت.
- انتهاكات الخصوصية من قبل الجهات التي تمارس الرقابة غير الرسمية والتي تقمع حرية الوصول إلى المعلومة والتعبير والفكر.

هناك العديد من الانتهاكات التي يمكن أن تعّرض خصوصيتنا الرقمية للخطر، سيتم ذكر البعض منها ومناقشة الآثار المحتملة التي يمكن أن تتسبب بها.

1.1. إفشاء وتسريب البيانات

يمكن تعريف إفشاء وتسريب البيانات على أنه مجموعة أحداث -مقصودة أو غير مقصودة- أدت نتائجها إلى فقدان سرية مجموعة من البيانات وانتهاكها من قبل أشخاص غير مخولين بذلك.

من الممكن أن تحدث مثل هذه العمليات نتيجة لاختراق المواقع المستخدمة من طرفنا، أو عن طريق استهدافنا بشكل مباشر بُغية الوصول لبياناتنا، وذلك بغرض استغلالها بما يتماشى مع مصالح الفاعل ملحقاً بنا الضرر سواء كان هذا الضرر ملموسًا ذا أثر فِعلي على سلامتنا الشخصية، أو غير ملموس مسبباً لنا الإزعاج عن طريق عرض الإعلانات الرقمية المتماشية مع طبيعة البيانات التي تم استغلالها.

توجد العديد من الممارسات التي يمكن اتخاذها للحد من إفشاء وتسريب البيانات، ومن أمثلتها:

1.1.1. الحفاظ على سرية البيانات الشخصية [03]

تعتبر البيانات الشخصية مجموعة مهمة من البيانات -لما تمثله من تعبير عنا وعن أفكارنا- إذ أنه سيصبح من السهل استغلالنا عن طريق الاستحواذ على هذه البيانات.

2.1.1. عدم مشاركة المعلومات المهمة [04]

يجب أن نكون شديدي الحذر في التعامل مع بياناتنا ومعرفة أي منها يمكن مشاركته وأيها نحتفظ به لأنفسنا.

3.1.1. متابعة الممارسات بشكل مستمر

كأشخاص غير تقنيين أو غير مهتمين بالتقنية يصعب علينا عادة معرفة ما يهدد سلامتنا الرقمية، إلا أنه يجب أن نكون على إطلاع دائم بالأدوات التي يمكن أن تساعدنا في الحفاظ عليها، وبالطرق والأساليب التي يتم اتخاذها لانتهاك بياناتنا وذلك لاكتساب الحصانة منها.

بعض التهديدات التي تؤدي إلى تسريب البيانات:

- مشاركة الملفات عن طريق وسائل غير آمنة.
- ضعف كلمات المرور المستخدمة وتكرارها.
- الدخول على روابط التصيد.
- استخدام شبكات الإنترنت العامة.
- استخدام البرامج غير المحدثة.

2.1. التجسس الرقمي ومراقبة البيانات

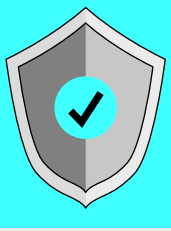
يتم تعريف التجسس الرقمي على أنه شكل من أشكال الهجوم (السيبراني) يستخدم لسرقة البيانات أو الملكية الفكرية من خلال جميع الوسائل التقنية المرتبطة بشبكة الإنترنت.

للتجسس الرقمي العديد من الأدوات، ولكن تظل (الهندسة الاجتماعية) أبرزها، حيث تُستخدم في التقصي عن بعض أنواع البيانات مثل: (أرقام الهواتف، والأسماء الكاملة، وتواريخ الميلاد، وبيانات حول أحداث مهمة في حياتنا)، فبتجميع هذه المعلومات عنا يمكن الاستفادة منها لاحقاً في محاولات التخمين والدخول الى حساباتنا الخاصة في مختلف المنصات والخدمات.

يمكن للتجسس أن يتم عبر استخدام أدوات أخرى أيضاً! كحقن بعض البرامج الضارة داخل أجهزتنا الإلكترونية، ومن الطرق المشهورة جداً لهذا النوع هي رسائل البريد الإلكتروني الضارة والتي عادة ما تحتوي على برمجيات خبيثة.

كيف نقي أنفسنا؟

- التأكد من سلامة التطبيقات التي نقوم باستخدامها وأنها من مصادر موثوقة.
- الفحص الدائم لمحتويات البريد الإلكتروني.
- التأكد من سلامة المواقع التي نستخدمها.
- استخدام وسائل التشفير وحجب الرقابة.
- استخدام برامج الدردشة التي تستعمل التشفير.
- استخدام إضافات المتصفح لمعرفة المواقع السليمة.
- استخدام محركات البحث الآمنة.
- قراءة لوائح الاستخدام وسياسات الخصوصية.



3.1. الابتزاز الالكتروني [05]

مع الانتشار الكبير للوسائل التقنية خصوصًا داخل مجتمعنا الذي يعُاني من انعدام الوعي الكافي من قبل شريحة كبيرة من المستخدمين/ات؛ يواجه العديد من الأفراد خطر الابتزاز الإلكتروني والذي بدوره سيؤدي إلى استغلالهم وتحقيق المنفعة من ورائهم.

الابتزاز الإلكتروني هو: مجموعة من الممارسات التي تَستخدم المحتوى الرقمي كالصور، ومقاطع الفيديو، والرسائل ؛ الهدف منها أن يتم تهديد الضحية واستغلالها.

ينقسم الابتزاز الإلكتروني لثلاثة أنواع:

1.3.1. الابتزاز المادي

يهدف هذا النوع من الابتزاز للحصول على منفعة مادية من الضحية، إذ أنه في الغالب ما تستمر عمليات التهديد حتى بعد حصول المبتز على المنفعة.

2.3.1. الابتزاز الجنسي

يهدف هذا النوع دائماً للحصول على منفعة جنسية من قبل الضحية.

3.3.1. ابتزاز المنفعة

عادة ما يستهدف هذا النوع من الابتزاز الشخصيات العامة أو المشهورة، حيث يتم ابتزاز الضحية مقابل الحصول على خدمة منه.

الممارسات السليمة وكيفية الوقاية

- استخدام برامج المصادقة الثنائية.
- التأكد من ضبط إعدادات الخصوصية.
- عدم التواصل والتراسل مع أشخاص لا تعرفهم في الفضاء الرقمي.
- توثيق الابتزاز إذا حدث.
- عدم الانصياع لمطالب المبتز وتبليغ الجهات الأمنية المعنية.
- الإبلاغ عن التهديدات والمضايقات.

2. كيف تحمي خصوصيتك الرقمية؟ [06]

1.2. عدم مشاركة قدر كبير من البيانات [3]

عدم الإسراف في نشر المعلومات عبر وسائل التواصل الاجتماعي، حيث يستغل المتطفلين جمع العديد من المعلومات المختلفة عن المستخدم المستهدف والتي بدورها قد تساهم بشكل كبير في انتهاك خصوصيته.

2.2. استخدام المتصفح الخفي

تسمح طرق التصفح التقليدية عبر متصفحات الانترنت بالحفاظ على عدد من السجلات مثل سجلات البحث والتصفح لديك وهذا بدوره يساهم في ظهور العديد من الإعلانات المزعجة. استعمال ميزة (التصفح الخفي) تتيح عدم احتفاظ المتصفح بأي بيانات عن كيفية استخدامك للإنترنت.

تنويه: إن استخدامك للوضع الخفي لا يعني حماية خصوصيتك بشكل كامل، حيث يمتلك مزودي خدمة الإترنت وشركات الاتصالات القدرة على معرفة نشاط التصفح لديك.

3.2. استخدام محركات بحث أكثر أماناً

يعتبر المتصفح الأكثر استخداماً حول العالم هو المتصفح التابع لشركة جوجل، ولكن هذا لا يعني أنه أكثر المتصفحات خصوصية فإذا ما أردنا الخصوصية وأقصى مستوى من الحفاظ على البيانات فيتوجب علينا أن نستخدم محركات البحث التي لا تقوم بتسجيل بيانات الاستخدام وتحافظ على سريتها.

4.2. استخدام برامج تجاوز الرقابة [07]

تسمح برامج تجاوز الرقابة بإخفاء الهوية عبر الإنترنت، فمن خلالها يمكن الاتصال بالإنترنت عبر إنشاء شبكة خاصة بعنوان إلكتروني -معرفّ رقمي- مختلف عن العنوان الأصلي للمستخدم، وهكذا سيصبح تعقب العنوان الأصلي أمراً صعباً جدا.

5.2. استخدام أنظمة المصادقة الثنائية [08] [09] [10]

تعتبر ميزة المصادقة الثنائية من أهم طبقات الحماية الإضافية التي يجب استخدامها لتأمين الحسابات على الإنترنت.

تعمل ميزة المصادقة الثنائية على تعزيز الحماية الرقمية حيث إنها تقوم بتوليد رموز يتوجب على المستخدم استعمالها للولوج إلى حسابه -بعد إدخال كلمة المرور الصحيحة وقبل الدخول إلى الحساب-، يمتلك كل رمز يتم توليده مدة زمنية معينة ليصبح غير صالح للاستعمال بعد انقضائها.

6.2. مراقبة الأجهزة المحمولة

تعمل العديد من البرامج في مختلف الأجهزة في الخلفية حتى عند عدم استخدامها، ولكونها تعمل في الخلفية هذا يعني استهلاكها بعضاً من موارد الجهاز واستغلالها بعض الصلاحيات الممنوحة للتنبؤ بسلوكيات المستخدم ومعرفة العديد من البيانات عنه كمكان تواجده على سبيل المثال؛ ولهذا السبب يجب علينا باستمرار متابعة البرامج التي نقوم باستخدامها والصلاحيات الممنوحة لها.

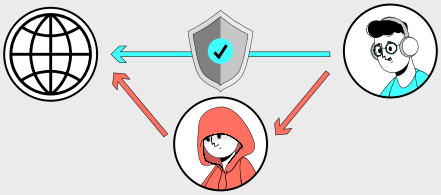
3. المخاطر الناتجة من استخدام شبكات الاتصال العامة وطرق تفاديها

يعتبر الانترنت المجاني الذي توفره شبكات الاتصال العامة من أكثر المغريات التقنية انتشاراً لكونها توفر اتصالاً بالإنترنت بشكل مجاني مثل تلك الموجودة في الأماكن العامة كالمقاهي والمطارات، كما تعتبر هذه الشبكات أحد أكثر الأشياء التي تهدد السلامة الرقمية والخصوصية، حيث تعتبر كمنجم للذهب في أعين المتسللين لأنها توفر إمكانية كبيرة للوصول إلى بيانات المستخدمين/ات ومعلوماتهم بكل سهولة.

من المخاطر الناتجة جراء استخدام الشبكات العامة:

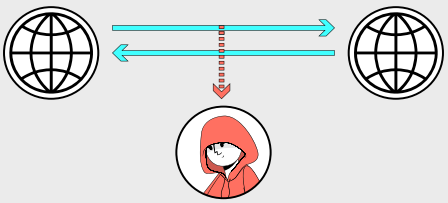
1.3. هجوم الشخص الوسيط (Man in the middle)

وهو من أشهر الهجمات التي يمكن للشخص التعرض لها عند استخدامه شبكات الاتصال العامة، حيث يتمكن المتسلل فيها من التعرف على البيانات التي يتم نقلها من المستخدم مع قدرته على التلاعب في البيانات بدون معرفة المستخدم لذلك.



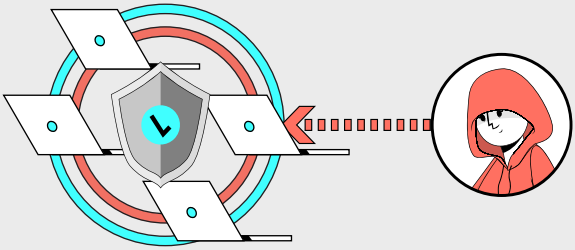
2.3. هجوم التنصت (Sniffing Attack)

يعمل هذا الهجوم كوسيلة يتم من خلالها معرفة بيانات المستخدمين/ات التي تمر عبر شبكة الاتصال من خلال برامج تقوم بتحليل جميع هذه البيانات.



3.3. هجوم نقطة النهاية (Endpoint Attack)

يستخدم هذا النوع من الهجمات مجموعة من الطرق للوصول إلى أحد الأجهزة المتصلة بالشبكة، على الرغم من كون الاتصال بين أي جهاز على الشبكة والشبكة في حد ذاتها مؤمّن ولا يمكن للمتسلل الوصول إليه، إلا أنه في حالة تمكن المتسلل من الوصول إلى أحد الأجهزة المتصلة على نفس الشبكة بطريقة معينة فستصبح باقي الأجهزة المتصلة على نفس الشبكة معرضة للخطر.



كيف نحمي أنفسنا؟

- استخدام الاتصال الآمن "SSL".
- إيقاف تشغيل مشاركة البيانات والمعلومات عند الاتصال بالشبكات العامة.
- عدم الولوج للخدمات المصرفية باستخدام الشبكات العامة.
- التحقق من أمان مواقع الانترنت عامة والتسوق الرقمي خاصة قبل الولوج إليها والدفع.
- تجنب استخدام برامج ومواقع التسوق.
- عدم ترك الأجهزة الإلكترونية متاحة بدون أي سبل حماية.
- استخدام برامج تشفير الاتصال.

4. الانتهاكات الرقمية: أمثلة ودروس مستفادة

1.4. البطاقة الانتخابية

مع قرب موعد الاستحقاق واستلام الناس بطاقاتهم الانتخابية نهاية عام 2021، لاحظنا انتشار العديد من المسابقات داخل مواقع التواصل الاجتماعي تقوم فكرتها على التقاط الصور لبطاقة الناخب ونشرها حتى يتسنى للمشترك الدخول في عملية السحب، أصحاب الفكرة حثوا الناس على حجب بياناتهم الشخصية إلا أنهم تناسوا صورة الرمز الموجود والذي من خلال مسحه يظهر رمز معين مشفر وعند فك تشفير هذا الرقم تظهر البيانات التي يحتويها من الرقم الوطني ورقم الناخب والرقم التسلسلي للبطاقة.

2.4. تسجيل الناخبين في الخارج [11]

يعمل هذا الهجوم كوسيلة يتم من خلالها معرفة بيانات المستخدمين التي تمر عبر شبكة الاتصال من خلال برامج تقوم بتحليل جميع هذه البيانات.

3.4. نشر القوائم المصرفية

في ظل الوضع الراهن الذي تمر به الدولة والذي تسبب في تزايد طلبات شراء العملة الأجنبية عن طريق مصرف ليبيا المركزي، شرعت المصارف في استقبال طلبات شراء النقد الأجنبي وإصدار البطاقات الدولية لها، إلا أن بعض المصارف باشرت في نشر أسماء من صدرت بطاقاتهم على وسائل التواصل مع أرقام هذه البطاقات والرمز الذي يوجد خلف البطاقة "CVV Code" وهذا ما يعد اعتداء صارخ على خصوصية البيانات متناسين إمكانية استغلال هذه البيانات من المتطفلين واستخدامها في الشراء عبر الإنترنت.

مثال توضيحي لنشر صفحة (مصرف الجمهورية وكالة الوحدة العربية) بيانات تخص زبائن المصرف الموضحة في الصور والتي تحتوي على الأسماء الكاملة للعملاء مرفقة بأرقام حساباتهم المصرفية.

4.4. روابط التصيد [12]

بين الحين والآخر تمتلئ مواقع التواصل الاجتماعي بالعديد من روابط التصيد والتي تستغل غياب الوعي الكافي من قبل المستخدمين/ات، تكون هذه الروابط في العادة مماثلة لأخرى حقيقية منتحلة هوية مواقع مصرفية، أو مواقع لشركات الاتصالات، وتهدف هذه الروابط إلى دفع المستخدم إلى تعبئة بياناته الشخصية لتنتقل إلى الطرف الآخر وتُخَزّن لديه ليتم استغلالها فيما بعد في أغراض غير شرعية.

مثال توضيحي لصفحة على موقع التواصل الاجتماعي (فيسبوك) تقوم بنشر روابط تصيّدية منتحلة هوية بعض شركات الاتصال المحلية.


Enter OTP
We sent a 6 digit OTP to your phone numbrer
VERIFY
123-456

3 أدوات أنيرا للسلامة الرقمية

أدوات أنير للسلامة الرقمية

سنتطرق في هذا المحور من دليل أنير للسلامة الرقمية إلى الأدوات التي يُوصى باستخدامها في الفضاء الرقمي للوقاية وحماية أنفسنا من التهديدات وتقليل المخاطر المحتملة من استخدام الإنترنت.

1. التصفح الآمن للإنترنت

يعتبر المتصفح الأكثر استخداماً حول العالم هو المتصفح التابع لشركة جوجل، ولكن هذا لا يعني أنه أكثر المتصفحات خصوصية فإذا ما أردنا الخصوصية وأقصى مستوى من الحفاظ على البيانات فيتوجب علينا أن نستخدم محركات البحث التي لاتقوم بتسجيل بيانات الاستخدام وتحافظ على سريتها. [13]

1.1. متصفحات أكثر أماناً

1.1.1. متصفح بريف "Brave"

عبارة عن متصفح ويب يركز على خصوصية المستخدم ويمنع الإعلانات وما يتبعها من الوصول إليك. يوفر متصفح بريف مانع إعلانات مبني بداخله ويستخدم محرك بحث "DuckDuckGo" كمحرك بحث افتراضي مما يساعد في عدم حفظ سجلات البحث الخاصة بالمستخدم.

2.1.1. متصفح تور "Tor"

هو متصفح مبني على فكرة إخفاء الهوية وحركة المرور الخاصة بالمستخدم، حيث يقوم بتوجيه اتصال المستخدم عبر مجموعة من الخوادم ليتم تشفير بيانات الاستخدام مما يخلق صعوبة في تتبع نشاط الاستخدام عبر الإنترنت.

2.1. إضافات المتصفح

للمتصفحات العديد من البرمجيات أو الإضافات الخاصة بها التي يمكن أن تساعد في حماية البيانات ومد يد العون في بعض المهام.

تنويه: ليست كل الإضافات الخاصة بالمتصفحات مفيدة أو آمنة، فمنها ما هو ضار وقد يشكل خطراً على المستخدم، لذلك ننصح الجميع بالتأكد من سلامة الإضافة المراد استعمالها وقراءة سياسات الخصوصية الخاصة بها قبل تثبيتها على المتصفح.

1.2.1. إتش تي تي بي إس في كل مكان "HTTPS Everywhere"

تساعد هذه الإضافة في تعزيز سلامة المستخدم أثناء زيارة المواقع المختلفة، فعن طريقها يمكن زيارة المواقع التي تحتوي على بروتوكول الأمان فقط مستخدمةً بذلك الاتصال المشفر.

2.2.1. إضافة "uBlock"

هي أداة تقوم بمنع الإعلانات غير المرغوب فيها من الظهور على المتصفح الخاص بك، تعمل هذه الأداة على الحفاظ على خصوصية المستخدم وذلك عن طريق منع تتبع أنشطة المستخدم على الإنترنت ويمكن إضافتها للعديد من المتصفحات مثل متصفح جوجل كروم أو فايرفوكس أو سفاري.

3.2.1. إضافة "Privacy Badger"

تقوم هذه الأداة بالتركيز على الحفاظ على خصوصية المستخدم وحظر أدوات الطرف الثالث التي تنتهك خصوصيته وتسمح فقط لملفات تعريف الارتباط التي قمت باستثنائها من معرفة تفضيلاتك أثناء التصفح.

3.1. التأكد من الروابط المختصرة

يجب على المستخدم التأكد من أمان الروابط المختصرة قبل فتحها مباشرة وذلك بفك الاختصار (توسيعها) والتأكد من وجهتها، حيث إن اختصار الروابط يعتبر من الطرق الفعالة في عملية انتحال الشخصية؛ لذلك يجب عليك التأكد منها قبل اتخاذ أي إجراء حيالها.

للتأكد من سلامة الروابط المختصرة يمكنك فحصها عن طريق أداة "**Where Goes**" وذلك بلصق الرابط في هذا الموقع وسيقوم بدوره بالتحقق من الوجهة الأصلية للرابط المختصر.

4.1. الـ"VPN"، برامج الشبكات الافتراضية [7]

عادة ما تقوم بعض الدول بحجب بعض المواقع الإلكترونية لتنافيها مع سياسات الدولة، أو لوازع أخلاقي، أو ديني، أو لأسباب مجهولة، من شأن هذه السياسات أن تكون مضرة بمصلحة المواطن حيث تحجب إمكانية وصوله إلى معلومة معينة أو من الولوج إلى موقع معين. في أغلب الأحيان يمكن تجاوز هذه العقبات عن طريق التمويه وتغيير عنوان الإنترنت إلى عنوان آخر لا يتأثر بالقيود المحلية.

كذلك يساعد تغيير عنوان الإنترنت لدى المستخدم من تجاوز رقابة مقاهي الإنترنت التي تحتوي على عدد كبير من المستخدمين في العادة، وهذا يساعد على حماية المستخدمين/ات وتفادي أي متطفل للبيانات يحتمل تواجده على نفس الشبكة.

تعرف برمجيات تجاوز الرقابة على أنها: عبارة عن برمجيات أو إضافات تعتمد على إنشاء شبكة خاصة افتراضية VPN تجعل الاتصال عبر الإنترنت يمر عبر خادم وسيط للوصول إلى الوجهة المرادة مساعداً على تجاوز الرقابة والحجب.

توجد العديد من الأدوات التي يمكن استخدامها لإنشاء الشبكات الافتراضية، منها ما هو مجاني يعتمد على حصة شهرية معينة من الاستهلاك وآخر مدفوع، ولكن تظل الخدمات المدفوعة والمفتوحة المصدر في الغالب هي الأفضل لأن جلّ الخدمات المجانية تقُوم بجمع العديد من البيانات عن المستخدم ومن ثم تقوم ببيعها لأطراف ثالثة.

من أمثلة هذه البرمجيات:

1.4.1. تطبيق لانترن "Lantern"

وهو عبارة عن برنامج يعمل على أنظمة تشغيل الويندوز والماك والأوبنتو، يعتمد هذا التطبيق على حصة شهرية معينة من الاستهلاك، إلا أن النسخة المدفوعة منه يمكن استخدامها بشكل كامل.

2.4.1. تطبيق سايفون "Psiphon"

وهو برنامج مفتوح المصدر، يوفر هذا البرنامج إمكانية الاتصال غير المحدود بالإنترنت ويمكن من خلاله اختيار العنوان المراد التغيير له، في حالة كان موقع البرنامج غير متاح لك يمكن التواصل مع get@psiphon3.com وعن طريق هذا البريد سيتم تزويدك بموقع بديل لتحميل البرنامج منه.

3.4.1. تطبيق نورد "Nord VPN"

يوفر هذا التطبيق تصفح آمن للإنترنت حيث يقوم بتشفير عملية التصفح على الإنترنت ويعمل على إخفاء عنوان IP الخاص بالمستخدم مما يسمح له بتصفح الإنترنت بشكل مجهول الهوية، يمكن من خلال هذا التطبيق اختيار عدة خوادم مختلفة لتمرير حركة الاتصال من خلالها.

4.4.1. تطبيق اكسبريس في بي إن "ExpressVPN"

يوفر هذا التطبيق خدمات التشفير ويوفر عدد كبير من الخوادم حول العالم. يمكن استخدام هذا التطبيق عبر مختلف أنظمة التشغيل، ومن ميزاته أنه يسمح للمستخدم بتخصيص التطبيقات التي تستخدم اتصال VPN عند استخدامها.

5.4.1. تطبيق سايبر جوست "CyberGhost"

يوفر هذا التطبيق خدمات الـVPN عبر عدد كبير من الخوادم المنتشرة في العديد من البلدان والمواقع الجغرافية. يمكن اختيار أي موقع جغرافي متوفر في التطبيق وتمرير الاتصال عبره، لا يقوم هذا التطبيق بحفظ أي بيانات متعلقة بسجلات تصفح الإنترنت ويمكن استخدامه على أنظمة تشغيل مختلفة كما يدعم في نسخته المدفوعة إمكانية تنشيط نفس الحساب على 7 أجهزة مختلفة، كما يوفر خدمات الدعم الفني على مدار الساعة في أي يوم من أيام الأسبوع.

2. أمن حساباتك الرقمية [9]

عندما نتحدث عن الحماية الرقمية نجد أن غالبية المُستخدمين يقومون بتثبيت برامج الحماية الموثوقة أو استخدام أنظمة التشغيل الأكثر آمناً مثل: (Mac OS X أو Linux)، ولكن هذا لا يعني انعدام إمكانية حدوث بعض حوادث الاختراق فهذه البرمجيات والأنظمة لا تعتبر كافية لحماية بيانات وحسابات المستخدم.

1.2. هل تم تسريب بياناتي من قبل؟

تتعرض العديد من الشركات للاختراقات وتسريب البيانات، وعادة ما يتم استغلال هذه البيانات المسروقة في بيعها لأطراف ثالثة أو تسريبها على الإنترنت. [3]

كيف أتأكد من سلامة بياناتي؟ وهل تم تسريبها من قبل؟ وما العمل؟

كمستخدمين/ات مهتمين بسلامتنا الرقمية يطرأ علينا هذا السؤال دائماً، وللإجابة عليه يمكن معرفة البيانات الخاصة بنا والتي تم تسريبها من قبل باستخدام أداة "Have I been pwned". حيث يمكن للجميع التأكد من سلامة بياناته الشخصية وذلك بوضع البريد الإلكتروني أو رقم الهاتف الذي يتم استعماله في خانة البحث وستقوم الأداة بإخبار المستخدم في حالة تم تسريب بيانات مرتبطة مع معلومات البريد الإلكتروني أو رقم الهاتف الخاص به، وذلك بعرض تقرير مفصل يحمل نوعية البيانات التي تم تسريبها ومن أي شركة بالتحديد، وأيضاً هل كانت كلمة المرور من ضمن البيانات المسربة أم لا.

في حالة وجود تسريب للبيانات وكانت كلمة المرور من ضمن البيانات المسربة يجب على المستخدم تغيير كلمات مروره حالاً.

2.2. مدير كلمات المرور [8] [9]

تعتمد قوة كلمة المرور على تنوع الرموز فيها واختلافها وعدم ربطها بأي تفاصيل شخصية وأصالتها -أي عدم تكرارها بين المواقع والخدمات المختلفة-. إذ يجب أن تحتوي كلمة المرور القوية على مجموعة من الرموز والحروف الكبيرة والصغيرة والأرقام، ويجب تجنب احتوائها المعلومات الشخصية مثل: الاسم، أو اسم المُستخدم، أو أي بيانات خاصة.

يستوجب أيضاً في كلمة المرور القوية أن تكون أصيلة وفريدة من نوعها -كأن تكون كلمة لم تخطر على بال المستخدم قط-، كما يجب اختيار كلمات مرور مُختلفة لكل حساب يمتلكه المستخدم وذلك لأنه في حال تم اختراق/تسريب بيانات حساب واحد فسيتم اختراق باقي الحسابات أيضاً إذا كانت تحميهم نفس الكلمة.

مع وجود الكثير من المواقع والخدمات الإلكترونية دائماً ما نواجه صعوبة في تذكر كلمات المرور الخاصة بكل حساب، فمن يقوم بذلك نيابة عنك؟ الإجابة هي "مدير كلمات المرور"، وهو عبارة عن برنامج أو تطبيق دوره إنشاء كلمات مرور مُعقدة وحفظ جميع حساباتك مع كلمات المرور الخاصة بها وحمايتها.

من البرامج التي تساعد في إدارة كلمات المرور:

1.2.2. برنامج "KeePass"

هو مدير كلمات مرور مجاني ومفتوح المصدر، من خلاله يمكن تخزين جميع كلمات المرور في قاعدة بيانات واحدة يمكن تأمينها بكلمة مرور واحدة ويتم تشفير كلمات المرور باستخدام خوارزميات التشفير.

2.2.2. برنامج "1Password"

عبارة عن مدير كلمات مرور يقوم المستخدم من خلاله بتخزين كلمات المرور الخاصة به والمعلومات الشخصية كمعلومات بطاقات الائتمان. يدعم هذا التطبيق مجموعة من الأنظمة المختلفة مما يساعد على تسهيل الولوج إليه.

3.2.2. برنامج "Dashlane"

من خلال هذا التطبيق يمكن للمستخدم إنشاء كلمات مرور قوية وآمنة من دون الحاجة إلى تذكرها حيث يوفر ميزة حفظ جميع كلمات المرور داخل قاعدة بيانات موحدة ويمكن الوصول لها عن طريق أي نظام تشغيل.

3.2. المصادقة الثنائية [8] [9] [10]

المصادقة الثنائية وتسمى أيضاً «ميزة التحقق بخطوتين» وهي عبارة عن ميزة توفرها العديد من المواقع والتطبيقات ومختلف منصات التواصل الاجتماعي للمستخدمين/ات؛ للرفع من مستوى الأمان لديهم، حيث يتم إضافة طبقة حماية ثانية بعد إدخال كلمة المرور بالشكل صحيح. حيث سيطلب من المستخدم إدخال الرمز الذي تم إرساله -في حالة استعمال رقم الهاتف أو البريد الإلكتروني- أو إدخال الرموز المولدة -في حالة استعمال تطبيقات المصادقة الثنائية- أو إدخال المفتاح الفيزيائي -في حالة امتلاكك له-.

للمصادقة الثنائية العديد من الأنماط، ومن أكثرها شيوعاً (رقم الهاتف – البريد الإلكتروني – تطبيقات المصادقة الثنائية – مفاتيح المصادقة الثنائية الفيزيائية) وذلك من الأقل أماناً إلى الأكثر أماناً.

تطبيقات المصادقة الثنائية:

1.3.2. تطبيق جوجل أوثونتيكيتر "Google Authenticator"

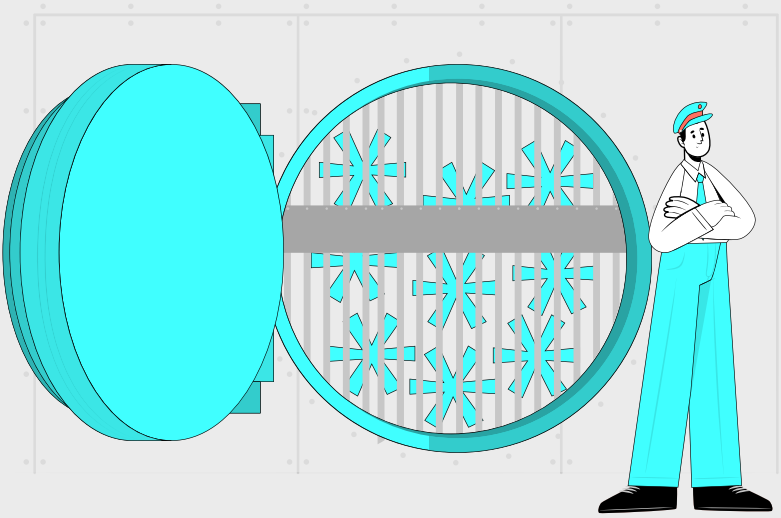
عبارة عن تطبيق من تطوير شركة جوجل بقوم بإنشاء وتوليد كلمات مرور تستخدم لمرة واحدة عند الولوج إلى أي حساب يتم ربطه بهذا التطبيق، يمكن استخدام هذا التطبيق على أكثر من نظام تشغيل ومتوافق مع العديد من الخدمات عبر الإنترنت التي توفر ميزة الربط بنظام المصادقة الثنائية.

2.3.2. مايكروسوفت أوثونتيكيتر "Microsoft Authenticator"

يعمل هذا التطبيق كغيره من تطبيقات المصادقة الثنائية ويمكن ربطه بأي حساب لتوفير طبقة حماية إضافية له ويعمل على أنظمة تشغيل مختلفة.

3.3.2. تطبيق أوثي "Authy"

يعمل هذا التطبيق كسابقه من تطبيقات المصادقة الثنائية ويوفر ميزة النسخ الاحتياطي وإمكانية المزامنة مع عدة أجهزة مختلفة في نفس الوقت، حيث تم توفير هذه الميزة للتطبيقات المذكورة سلفًا.



3. المراسلات الآمنة عبر الإنترنت

الإرسال والاستقبال عبر خدمات البريد الإلكتروني، استخدام برامج الدردشة، وغيرها الكثير. في حياتنا اليومية نقوم باستعمال طرق المراسلة عبر الإنترنت بشكل دائم، وذلك خلال أعمالنا أو حياتنا الشخصية؛ وللحفاظ على سلامتنا الرقمية يجب على المستخدم التعرف على الطرق الأكثر أماناً لاستعمال هذه الخدمات لتعزيز سلامته الرقمية والوقاية من المخاطر المحتملة.

1.3. تشفير البريد الإلكتروني

عن طريق هذه العملية يقوم المستخدم بحماية بريده الإلكتروني ورسائله الخاصة وذلك عبر تشفيرها مما سيصعب على أي متطفل إمكانية معرفة فحواها.

للقيام بالتشفير توجد عدة أدوات من شأنها أن تساعدك في هذه العملية منها:

1.1.3. مزود بريد بروتون ميل "ProtonMail"

ProtonMail

من خلال هذه الخدمة يمكن تشفير البريد الإلكتروني المرسل والمستقبل بشكل كلي عبر إحدى خوارزميات التشفير، حيث يوفر للمستخدم مفتاح أمان عام وآخر خاص، يمكن مشاركة المفتاح العام مع الأفراد الذين ترغب بالتواصل معهم بينما يبقى المفتاح الخاص مع المستخدم دون مشاركته مع أي شخص والذي من خلاله يتم إلغاء تشفير البريد الإلكتروني المستقبل. يدعم بروتون ميل ميزة تدمير الرسائل بشكل ذاتي ويوفر طبقة حماية أخرى للوصول إلى البريد عن طريق كلمة مرور خاصة به.

2.1.3. إضافة ميل فيلوب "Mailvelope"

Mailvelope

عبارة عن إضافة لمتصفحات الويب تعمل على تحسين الأمان والخصوصية الخاصة بالمستخدم وتوفر نظام التشفير بين الطرفيات ومتوافقة مع مزودي خدمة البريد الإلكتروني الأخرى.

3.1.3. مزود بريد توتانوتا "Tutanota"

عبارة عن خدمة بريد إلكتروني توفر تشفيرًا شاملًا لجميع رسائل البريد الإلكتروني والمرفقات التي يتم إرسالها أو استقبالها، يتميز بسهولة استخدامه ويدعم ميزة التقويم المشفر.

2.3. فحص الروابط والمرفقات

التعامل بالبريد الإلكتروني لم يعد أمرًا من الماضي فهو ضرورة محتمة من ضروريات عصرنا التقني، ولكن كحال غيرها من الأدوات التقنية فإن لها دورًا كبيرًا في انتهاك الخصوصية وإصابة أجهزتنا بالبرامج الضارة في حالة استعمالها الخاطئ.

لذلك يتوجب علينا عند استقبال أي بريد إلكتروني:

1.2.3. التأكد من أن مصدر هذا البريد موثوق أم لا.

2.2.3. فحص المرفقات والروابط إن وجدت:

1.2.2.3. عبر مزود الخدمة

يتم هذا الفحص في العادة بشكل أوتوماتيكي من قبل مزود خدمة البريد مثل Gmail، لكن مع هذا يجب علينا فحص المرفقات عند تحميلها وذلك باستخدام برامج الوقاية من الفيروسات قبل فتحها أو استعمالها.

2.2.2.3. باستخدام (Malwarefox)

يمكن فحص الروابط والمرفقات في البريد الإلكتروني ببساطة باستخدام أداة (Malwarefox) وذلك بإعادة توجيه الرسالة إلى (Scan@virusetotal.com)، وعندها سيتم فحص البريد الإلكتروني وكذلك المرفقات الموجودة به وإعادة إرسال تقرير تام لك.

3.2.2.3. فحص الروابط المرفقة باستخدام محاكي المتصفح

في حالة احتواء البريد الإلكتروني على رابط غير موثوق، يمكن التأكد من سلامته عبر استخدام مُحاكي افتراضي (Sandbox) يعمل في بيئة معزولة عن شبكتك، عن طريقه يمكنك الدخول والتأكد من أي موقع أو رابط مشبوه. وفي حالة وجود أي برمجيات خبيثة أو فيروسات لن يصاب المستخدم بأي ضرر لأنه وببساطة لم يتم الولوج للرابط مباشرة، بل تم الولوج إليه عن طريق المحاكي الافتراضي والذي يعمل على خوادم الشركة المقدمة للخدمة، يمكن استعمال أداة "(Browser Sandbox - محاكي المتصفح).

3.3. دردش بسرية: استخدام برامج الدردشة المشفرة [14]

من أكثر الأدوات المهمة في عالم السلامة الرقمية والتي تساعد المستخدم على الحفاظ على خصوصية مراسلاته هي تطبيقات الدردشة التي تستخدم التشفير بين الطرفيات.

من خلال تقنية التشفير بين الطرفيات "End to End Encryption" يمكن للمستخدم أن يطمئن بمعرفة أن مراسلاته وأحاديثه خلال هذه التطبيقات يتم تبادلها بطريقة مشفرة كلياً تسمح لأطراف الحديث فقط بالاطلاع على المحتوى المتبادل.

- **تطبيقات توفر التشفير بشكل افتراضي:**

3.3.1. تطبيق سيجنال "Signal"

يعتبر سيجنال أكثر تطبيقات الدردشة أماناً، حيث يوفر تشفيرًا كاملًا للرسائل النصية وللمكالمات الصوتية ومكالمات الفيديو. يقوم هذا البرنامج بتشفير جميع مراسلات المستخدم ولا يقوم بتخزينها في خوادمه، ويتميز بأنه مفتوح المصدر مما يسمح بإجراء عمليات التدقيق على الرمز البرمجي له.

- **من أبرز مميزاته:**
  - التطبيق مفتوح المصدر، ما يسمح لخبراء الأمن السيبراني والتقنيين من مراجعة الكود البرمجي الخاص بالبرنامج بكل شفافية.
  - توفير خدمة التشفير بشكل افتراضي - من دون تعيينها يدوياً في الإعدادات-.
  - تشفير "البيانات الوصفية" للمرفقات، مثل: معلومات الموقع الجغرافي المرتبط بالصور. [15]
  - لا يقوم بجمع بيانات عن المستخدم.
  - لا يقوم بسحب جهات الاتصال وتخزينها عنده.
  - لا يستعمل بيانات المستخدم في الإعلانات.

2.3.3. تطبيق واتساب "Whatsapp"

يعتبر واتساب من أكثر تطبيقات المراسلة استخدامًا، حيث يوفر العديد من المزايا ويتميز بسهولة الاستخدام. تطبيق واتساب في حد ذاته غير مفتوح المصدر على غرار بروتوكول التشفير الخاص به.

- **من أبرز مميزاته:**
  - بروتوكول التشفير مفتوح المصدر.
  - توفير خدمة التشفير بشكل افتراضي -بدون تعيينها يدوياً في الإعدادات-.
  - الاحتفاظ بالمفتاح السري "Private Key" الخاص بالتشفير على الجهاز.
  - يقوم بتشفير الرسائل وأيضاً المرفقات.
- **العيوب:**
  - التطبيق في حد ذاته غير مفتوح المصدر.
  - لا يقوم بتشفير البيانات الوصفية للمرفقات. [15]
  - اتباع نشاط المستخدم داخل التطبيق وتجميع البيانات عنه.
  - استخدام ومشاركة البيانات في الإعلانات والاستهداف ومشاركتها مع أطراف ثالثة.

- **تطبيقات توفر التشفير بشكل اختياري:**

3.3.3. تطبيق تيليجرام "Telegram"

Telegram

يعتبر التطبيق في حد ذاته مفتوح المصدر -بغض النظر عن بروتوكول التشفير- يوفر هذا التطبيق ميزة التشفير بين الطرفيات -عند تفعيلها بشكل يدوي في المحادثات السرية- ويدعم كذلك المحادثات السرية والتدمير الذاتي للرسائل ويعتبر من التطبيقات الآمنة في الاستعمال كغيره من وسائل التواصل المذكورة سابقًا.

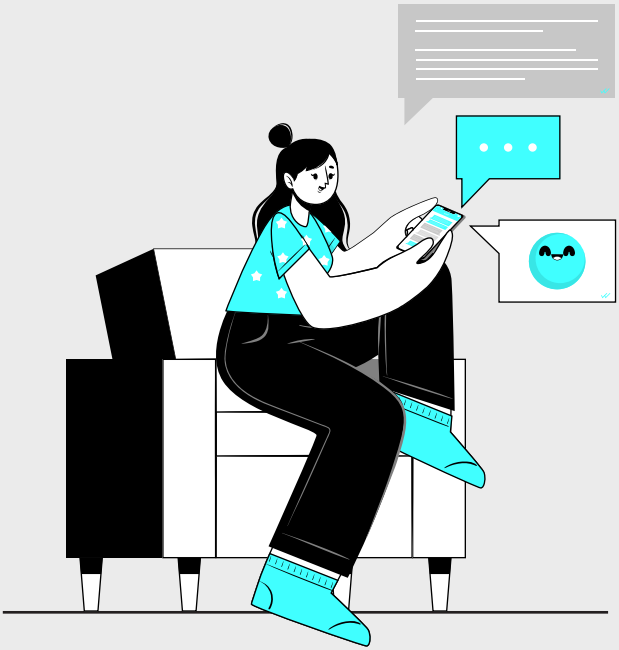
- **من أبرز مميزاته:**
  - التطبيق في حد ذاته مفتوح المصدر.
  - يحمل العديد من المزايا المستساغة لدى مستخدمي مواقع التواصل.

- **العيوب:**
  - بروتوكول التشفير غير مفتوح المصدر
  - عدم تشفير البيانات الوصفية للمرفقات. [15]
  - امكانية الشركة المالكة من الاطلاع على رسائلك الخاصة والمرفقات المرسلة في حالة عدم استعمال (المحادثات السرية).
  - تخزين بيانات جهات الاتصال للمستخدم وتجميع البيانات عنه.
  - مشاركة هذه البيانات مع أطراف ثالثة.

4.3.3. تطبيق مسنجر "Messenger"

يوفر هذا التطبيق ميزة التشفير بين الطرفيات -عند تفعيلها بشكل يدوي في المحادثات السرية- ويعتبر التطبيق الرئيسي والمرتبط مع منصة فيسبوك للتواصل الاجتماعي والمملوكة لشركة ميتا "Meta"

- **من أبرز مميزاته:**
  - بروتوكول التشفير في حد ذاته مفتوح المصدر.
  - يعد سهل الاستخدام لكونه مرتبطاً مع منصة فيسبوك بشكل مباشر.
- **العيوب:**
  - التطبيق غير مفتوح المصدر.
  - إمكانية الشركة المالكة من الاطلاع على رسائل المستخدم والمرفقات المرسلة -في حالة عدم استعمال المحادثات السرية-.
  - عدم تشفير البيانات الوصفية للمرفقات. [15]
  - عدم استخدام خدمة التشفير بشكل افتراضي (فقط عند تفعيل المحادثات السرية).
  - تخزين بيانات جهات الاتصال للمستخدم وتجميع البيانات عنه.
  - مشاركة هذه البيانات مع أطراف ثالثة.



4. التعامل الآمن مع البيانات

فيما يخص بياناتنا الشخصية، يجب علينا كمستخدمين/ات التعامل معها والحفاظ عليها وعلى أمانها وتخزينها باستخدام طرق آمنة تسمح لنا وحدنا بالوصول إليها.

1.4. تشفير البيانات

تعتبر البيانات الموجودة على أجهزة الحاسوب أو الهواتف المحمولة من البيانات الشخصية، وقد تكون هذه البيانات حساسة وسرية للغاية ولا رغبة للمستخدم في مشاركتها مع أي أحد. أيضاً يمكن لهذه البيانات أن تكون تابعة لمؤسسة ما أو لجهة معينة، ما يسبب الاطلاع عليها أو تسريبها الضرر للمستخدم، ومن هذا المنطلق نتعرف على ضرورة إخفاء جميع البيانات الحساسة عن أعين المتطفلين.

يطلق على عملية إخفاء البيانات مصطلح (التشفير) ويعرف على أنه إخفاء جميع البيانات الموجودة على الأجهزة -بمختلف أنواعها- عن الآخرين حتى وإن كانوا يتشاركون استخدام نفس الأجهزة.

توجد عدة أدوات يمكن استخدامها لتشفير البيانات والملفات منها:

1.1.4. برنامج فيراكريبت "VeraCrypt"

هو برنامج مجاني مفتوح المصدر يسمح بتشفير الملفات والبيانات والأقراص الصلبة كما أنه يسمح بإنشاء أقراص افتراضية تحتوي على بيانات ويتم تشفيرها بشكل كامل. يقوم هذه البرنامج بتشفير جزء من القرص الصلب الموجود على جهاز الحاسوب أو أي وسيلة تخزين خارجية ووضعها داخل ملف واحد يدعى الحاوية ويمكن فتحها وإغلاقها برمز سري باستخدام "Vera Crypt" وذلك لمنع أي شخص غير مخول بالدخول من الوصول إليها. يستخدم هذا البرنامج نظام التشفير الفوري "on-the-fly" عند كتابة الملفات داخل المجلد الموجود بالقرص المراد تشفيره.

2.1.4. برنامج أكس كريبت "AxCrypt"

عبارة عن برنامج لتشفير الملفات بشكل سهل وآمن، يتم التشفير فيه عن طريق استخدام مجموعة من خوارزميات التشفير القوية ويمتاز بدعمه للعديد من أنظمة التشغيل المختلفة.

2.4. التخزين السحابي "Cloud Storage"

التخزين السحابي هي العملية التي يتم فيها تخزين البيانات على خوادم شركة معينة مانحة للخدمة، حيث توفر هذه الخدمة سهولة الوصول إلى معلومات من أي مكان وتحميلها والتعديل عليها، يمكن أن تتم عملية التخزين بشكل دوري "نسخ احتياطي" لضمان عدم فقدان البيانات في حالة حدوث أي طارئ مع إمكانية استرجاعها وقت الحاجة لها.

توجد العديد من خدمات التخزين السحابي الآمنة منها:

1.2.4. خدمة سينك "Sync.com"

هي خدمة تخزين سحابي تسمح بمشاركة البيانات وتخزينها بشكل آمن وتوفر ميزة تشفير لكل الملفات التي يقوم المستخدم برفعها على السحابة، وتتيح له تعيين تواريخ انتهاء صلاحية روابط الملفات التي تتم مشاركتها مع مستخدمين/ات آخرين.

2.2.4. خدمة بي كلاود "pCloud"

وهي خدمة تخزين سحابي توفر تشفيرًا كاملًا للملفات التي يقوم المستخدم برفعها مع إتاحة إمكانية العمل الجماعي على الملفات المرفوعة بدرجة أمان عالية.

3.2.4. خدمة سبايدر أوك "SpiderOak"

عبارة عن خدمة نسخ احتياطي توفر المزامنة الدائمة للملفات، تتميز بالأمان وبتشفير الملفات عند رفعها باستخدام مفتاح تشفير خاص؛ مما يساعد في حفظ الملفات بأمان تام. بمعنى آخر لا يمكن الوصول للبيانات المرفوعة والمشفرة على السحابة إلا بوجود مفتاح فك التشفير الخاص، وتوفر هذه الخدمة أيضاً ميزة النسخ الاحتياطي من عدة أجهزة في آن واحد.

4.2.4. تشفير البيانات قبل رفعها على السحابة باستخدام "Boxcryptor":

لزيادة الحماية أكثر، يمكن تشفير البيانات قبل رفعها على السحابة والاحتفاظ بمفتاح التشفير، لتبقى الملفات قابلة للرؤية والاطلاع فقط من قبلك أنت -المالك لمفتاح التشفير- وذلك عبر أداة "**Boxcryptor**".

5. كن دائماً على اطلاع

1.5. سياسة الخصوصية والشروط والاستخدام [6]

عند اشتراكك في أي موقع أو خدمة جديدة أو حتى عند تحميلك لتطبيق معين وتسجيلك فيه لأول مرة ستلاحظ طلب التطبيق/الموقع الموافقة على سياسات الخصوصية الخاصة بهم وشروط الاستخدام لاستكمال شروط التسجيل واستعمال الخدمة بنجاح. في العادة من النادر جداً أن يقوم المستخدم بالاطلاع على هذه الصفحات الطويلة من السياسات، فمعظم المستخدمين/ات يقومون بالموافقة عليها باستهتار من دون إدراكهم لما قد وافقوا عليه أو ما تحمله هذه الشروط من تهديدات صريحة لسلامتهم الرقمية وخصوصيتهم.

لحل مثل هذه المشاكل يمكن استخدام أداة "**Terms of services didn´t read**"، فقط بوضع اسم الموقع أو التطبيق في خانة البحث سيظهر لك ملخص لطيف يحتوي على تقييم مدى انتهاك الخصوصية مع تلخيص كل تلك الصفحات في تقرير بسيط يمكن للمستخدم العادي أن يتعامل معه.

2.5. الصلاحيات الممنوحة للتطبيقات

تحمل أجهزتنا الإلكترونية معظم بياناتنا الشخصية والتي تتمثل في الصور وجهات الاتصال والبيانات المصرفية ...الخ، تمثل هذه البيانات الخطر الأكبر لنا إذا ما تم استغلالها بشكل غير مناسب من أشخاص غير مخولين، ومع كثرة استخدام وتحميل التطبيقات من المتاجر الرسمية أو من مصادر غير معروفة يتوجب علينا التركيز والتدقيق على الصلاحيات التي يتم منحها لكل تطبيق منها حتى لا نكون عرضة للخطر.

بمعنى آخر، حتى تشتغل التطبيقات بصورة صحيحة يتطلب على المستخدم منح الأذونات المطلوبة من التطبيق. في بعض الأحيان تستغل بعض الشركات والمطورين هذه الأذونات وعدم دراية المستخدم لصنع تطبيقات يمكنها الوصول لمعلومات وبيانات حساسة عن المستخدم نفسه، لذلك يتوجب علينا معرفة الأذونات أو الصلاحيات التي يتطلبها كل تطبيق قبل تثبيته وكذلك لمسح أي تطبيق مثبت ويمتلك الصلاحيات

للوصول لبياناتنا الحساسة.

يمكن التأكد من الصلاحيات في الأجهزة التي تشتغل بنظام أندرويد كالتالي: [16]

أولاً: من خلال متجر التطبيقات نفسه حيث يتيح لنا إمكانية معرفة الصلاحيات التي يريدها كل تطبيق (أذونات التطبيق)

ثانيًا: عن طريق الجهاز نفسه:

- افتح تطبيق "الإعدادات" على جهازك.
- انقر على التطبيقات والإشعارات.
- انقر على التطبيق المراد.
- انقر على الأذونات.
- اختر الأذونات التي تريد أن يمتلكها التطبيق، مثل الكاميرا أو سجل الأسماء.

يمكن التأكد من الصلاحيات في الأجهزة التي تشتغل بنظام آي أو إس كالتالي: [17]

- أولاً: انتقل إلى الإعدادات ثم الخصوصية.
- ثانياً: اسحب الشاشة للأسفل وقم باختيار البرنامج الذي تريد التأكد من صلاحياته.
- ثالثاً: اختر إذا ما كنت تريد أن تمنح الصلاحية للتطبيق أم لا.

3.5. كيفية استخدام شبكات التواصل الاجتماعي بطريقة آمنة [6]

تعود شبكات التواصل الاجتماعي بالفائدة على مستخدميها من ناحية تداول الأخبار والأفكار والتواصل مع الأصدقاء والعالم، إلا أن استخدامها بشكل غير مناسب قد يسبب العديد من المشاكل والتهديدات الخطيرة لسلامتنا الرقمية، ولهذا السبب يجب علينا أن نكون على وعي بأساليب الاستخدام الآمنة لمواقع التواصل الاجتماعي.

بياناتنا على مواقع التواصل:

تحمل مواقع التواصل الاجتماعي العديد من البيانات عنا، كتلك التي نقدمها بشكل طوعي عند تسجيلنا فيها (الاسم، والعمر، والجنس، ومحل الإقامة ...الخ) أو البيانات التي نشاركها عن حياتنا الشخصية فيها، أو البيانات التي تجمعها هذه المواقع عنا كسجلات النشاط مثل سجلات البحث.

يمكن أن تُستغل هذه البيانات بشكل يؤثر سلباً على سلامتنا الرقمية ويضع حريتنا وخصوصيتنا على الإنترنت في موضع خطر، كأن:

- يتم استغلال البيانات الحساسة التي تقدم بشكل طوعي من قبل أي متطفل، في عمليات الابتزاز أو الهندسة الاجتماعية.
- استغلال بياناتنا الشخصية والبيانات التي تجمعها هذه المواقع في إعداد الإعلانات أو بيعها إلى شركات أخرى.

فعند استخدام هذه المواقع يجب أن نطرح على أنفسنا بعض الأسئلة، ومنها:

- من الذي يتحكم في البيانات والمعلومات التي نشاركها؟
- هل نحن على معرفة شخصية بجميع من نتواصل معهم عبر وسائل التواصل الاجتماعي؟
- من بإمكانه الوصول إلى المعلومات التي نشاركها؟
- هل يوافق أصدقائي ومعارفي على مشاركة بياناتهم وصورهم؟

تسلط هذه الأسئلة الضوء على جوانب مهمة يجب أن نفكر فيها كثيراً حيث إنها توضح كيف يمكن للبيانات والمعلومات أن تؤثر على سلامتنا.

4.5. إعدادات الخصوصية وسياسة الاستخدام [6]

معظم البيانات التي نشاركها عبر مواقع التواصل الاجتماعي تكون في يد الشركات المالكة للموقع والتي من الممكن أن تُستغل بطرق ذات عواقب سلبية لنا، لهذا السبب يجب علينا الاطلاع دورياً على إعدادات الخصوصية وسياسة الاستخدام والتي تعتبر عملية صعبة بالنسبة لأغلب الأشخاص، إلا أنها تحتوي على جميع القواعد المتبعة داخل الموقع مع كيفية إدارة بياناتك والحفاظ عليها.

لكل منصة تواصل اجتماعي قواعد وسياسات خاصة بها إلا أن هناك أنماط مشتركة بينها، ومنها:

- إعدادات الخصوصية تميل عادة إلى توضيح من يمكنه رؤية منشوراتك (العموم، أو الأصدقاء، أو أصدقاء الأصدقاء، أو أنت فقط)، كذلك تفاصيل الاتصال الخاصة بك وإمكانية البحث عنك داخل هذه المواقع.
- إعـدادات الأمـان والتي من خلالها يمكنك معرفة طريقة تأمين حسابك، أيضاً يمكنك منع الحسابات المتطفلة من التعرف على نشاطك، ومن خلال إعدادات الأمان تستطيع أن توثق حسابك بشكل رسمي مما يساعدك في استرجاعه حالة حدوث أي مشكلة أو خرق أمني.
- يتم تفعيل المصادقة الثنائية عن طريق إعدادات الأمان، كما باستطاعتك اختيار مجموعة من جهات الاتصال الذين تثق بهم ليكونوا عوناً لك في حالة فقدان حسابك.
- الاطلاع بتمعّن على سياسات الاستخدام لجميع المنصات.

يمكن أن نقوم بضبط إعدادات الخصوصية الخاصة بنا في منصات التواصل الاجتماعي عن طريق:

فيسبوك:

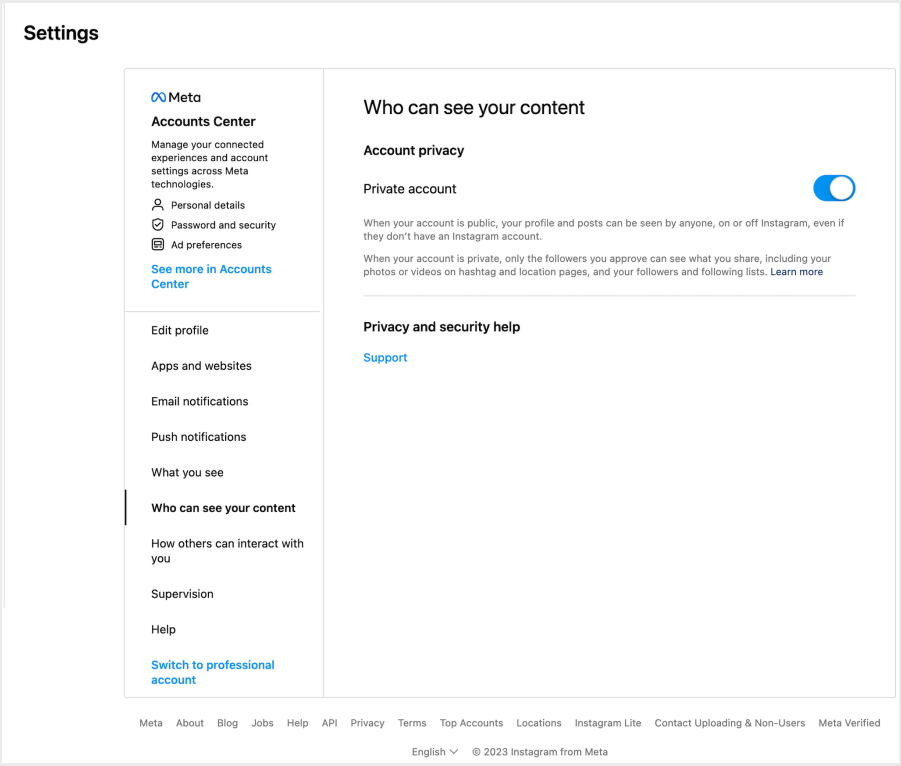
التوجه إلى الإعدادات والخصوصية من ثم اختيار التحقق من الخصوصية. [18]

تويتر:

الإعدادات والدعم من ثم اختيار الخصوصية والأمان. [19]

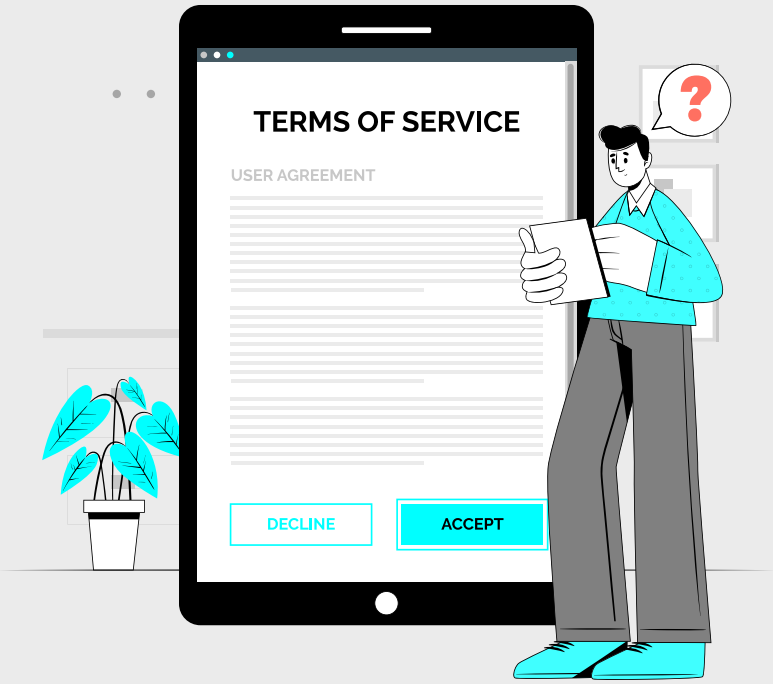
انستغرام:

الإعدادات من ثم اختيار الإعدادات المتعلقة بالخصوصية. [20]



تنويه

لا يمكننا أن ننسى أن مع كل هذه الأدوات والممارسات إلا أن للمتطفلين دائمًا وسائل أخرى؛ لذا يتوجب علينا دائماً الحذر والاطلاع على ما هو جديد حتى نكون بمنأى عن أذى الآخرين.



إخلاء طرف

مبادرة أنير غير ملزمة بأي تغيير في المعلومات المذكورة في هذا الدليل بعد موعد نشره وحتى إصدار نسخة جديدة منه. المعلومات المذكورة في هذا الدليل تمت كتابتها استنادا على مصادر موثوقة ضمن فترة نشر هذا الدليل، قد تتغير بعض المعلومات القابلة للتطوير مثل سياسات منصات مواقع التواصل الاجتماعي.

عن أنير [21]

أنير هي مبادرة ليبية مستقلة، محايدة وغير سياسية، مختصة في التوعية بشؤون الإنترنت الآمن والتحقق من الأخبار الزائفة والمعلومات المضللة. نشأت عام 2020، وتتخذ من الفضاء الإكتروني منصة لها تهدف إلى رفع الوعي بالممارسات السليمة لخوض تجربة إنترنت أكثر أمانا.

تقوم أنير بنشر محتوى توعوي حول السلامة والحقوق الرقمية والتكنولوجيا، كما تكافح اضطراب المعلومات وذلك عبر التوعية بشؤون التربية الإعلامية والمعلوماتية، والتحقق من الأخبار الزائفة والمضللة المنتشرة عبر وسائل التواصل االجتماعي.

سياسة استخدام دليل أنير للسلامة الرقمية

تجدون في الهوامش روابط لأمثلة متوسعة تقدم تفاصيل وتوضيحات إضافية حول المفاهيم والاستراتيجيات المطروحة.

– الهوامش

01 أنير - علاش مفروض نهتموا بالسلامة الرقمية؟

02 أنير - علاش مفروض نهتموا بالخصوصية في العالم الرقمي؟

03 أنير - مش مهم: أثر بياناتك غير المهمة

04 أنير - هل هناك ما لا يجب أن نشاركه على الانترنت؟

05 أنير - التنمر الرقمي

06 أنير - الحفاظ على الخصوصية في عصر تجميع البيانات

07 أنير - VPN: مقدمة قصيرة جداً

08 أنير - هل كلمة السر بروحها كافية؟

09 أنير - كن يقظاً: أفضل الممارسات لتأمين حساباتك على الإنترنت

10 أنير - المصادقة الثنائية وكيفية تفعيلها

11 أنير - خصوصية الناخبين عبر الرسائل البريدية

12 أنير - شن هو التصيد الإلكتروني؟ وكيف نحموا أنفسنا منه؟

13 أنير - ما هي الكوكيز أو ملفات تعريف الإرتباط؟

14 أنير - هل تقرأ الشركات محادثاتنا؟ وشن هو التشفير بين الطرفيات؟

15 أنير - البيانات الوصفيّة والقوّة الخفيّة!

16 أنير - يوتيوب - كيف تتأكد من الصلاحيات الممنوحة للتطبيقات - نظام Android

17 أنير - يوتيوب - كيف تتأكد من الصلاحيات الممنوحة للتطبيقات - نظام iOS

18 فيسبوك - أدوات وإعدادات الخصوصية الأساسية

19 تويتر - السلامة والأمان

20 انستغرام - إعدادات الخصوصية والمعلومات

21 أنير - من نحن