خطوات عملية
في الحماية الرقمية

سوريون
من أجل
الحقيقة
والعدالة

Syrians
For Truth
& Justice

خطوات عملية في الحماية الرقمية

خلاصة ورشات تطبيقية حول الأمن الرقمي

المادة العلمية: وائل موسى
إعداد: نينار خليفة
تصميم الغرافيك: نينوس شابو

الطبعة الأولى: تشرين الثاني/نوفمبر 2018

تم إنجاز هذا الدليل من قبل منظمة سوريون من أجل الحقيقة والعدالة STJ بدعم من LIFELINE

منظمة سوريون من أجل الحقيقة والعدالة:

هي منظمة سورية مستقلة، غير حكومية وغير ربحية، تأسست عام 2015.

تعمل المنظمة من أجل "سوريا" التي يتمتع فيها جميع المواطنين والمواطنات بالكرامة والعدالة وحقوق الإنسان المتساوية، ويتركز عملها بشكل أساسي على توثيق انتهاكات حقوق الإنسان في سوريا وقضايا المناصرة في المحافل الدولية.

مشروع لايفلاين"LIFELINE":

وهو عبارة عن مشروع يدعم مجموعة متنوعة من منظمات المجتمع المدني التي تقوم بالدفاع عن حقوق الإنسان وتعزيزها وحمايتها و/أو العمل في هيئة رقابية، بما في ذلك منظمات حقوق الإنسان وجمعيات الصحفيين ومجموعات الطلاب والنقابات العمالية ومراكز الفكر وغيرها.

لإبداء الرأي والملاحظات حول هذا الدليل يرجى مراسلتنا على البريد الالكتروني التالي: editor@stj-sy.org

الفهرس

مقدمة:

في عالمنا اليوم، بات التعرّف على مفهوم "الأمن الرقمي" و "وسائل الحماية الإلكترونية" ضرورة مُلحّة لضمان سلامة الأفراد والمؤسسات، وحماية خصوصيتهم وسرّية بياناتهم، فقد أصبحت المخاطر والتهديدات تزداد يوماً بعد يوم على مستخدمي تكنولوجيا المعلومات، بما في ذلك وسائل التواصل الحديثة وما أنتجته من طفرة رقمية هائلة. ومن هنا تأتي أهمّية القدرة على التحكم بالمخاطر والتهديدات من خلال إجراءات أمنيّة بسيطة ومتاحة، وقد يؤدي إهمال هذه الإجراءات لأمننا الرقمي إلى نتائج كارثية لا تحمد عقباها، والتي قد لا تستثني أيًا منّا وخاصة في حالات الاختراق والقرصنة والابتزاز وسرقة البيانات والتعدّي على الخصوصية والملكية الفكرية والتي باتت حوادث نسمع عنها بشكل يومي.

وفي الوقت الذي أصبح فيه حفظ وتخزين وتبادل المعلومات بالوسائل الإلكترونية أمراً أساسياً في حياتنا اليومية، ازدادت في المقابل نسبة حالات "الجرائم الإلكترونية" وسرقة المعلومات الشخصية أو المتبادلة إلكترونياً. وكما أنّنا نعتمد في "حياتنا الواقعية" طرقًا ووسائل لحماية ممتلكاتنا من السرقة أو الاعتداء، عن طريق إقفال أبواب منازلنا واستخدام كاميرات المراقبة وأجهزة الإنذار على سبيل المثال، فإنّ "حياتنا الإفتراضية/الرقمية" تستدعي ضرورة تحصينها من المخترقين والعابثين أيضاً. ومع التطور المتسارع في عالم التكنولوجيا، تغدو مواكبة مستجدات أدوات ووسائل "الأمن والحماية الرقمية" عملية مستمرة، تستدعي تحديث معرفتنا بالممارسات الأمنية وإعادة تقييمها بشكل دوري.

إنّ حقيقة كون بياناتنا ومعلوماتنا محمية في الشهر أو الأسبوع الماضي، لا تعني أنّها لا تزال آمنة اليوم !

هدف الدليل:

يأتي هذا الدليل في إطار مشروع طموح من قبل سوريون من أجل الحقيقة والعدالة وشركائها الدوليين، ويهدف إلى نشر الوعي في مجال الأمن الرقمي والحماية ضمن فئات المجتمع السوري، وخاصّة تلك التي تعمل في إطار توثيق انتهاكات حقوق الإنسان ووسائل الإعلام ومنظمات المجتمع المدني.

وقد جاء هذا الدليل كحصيلة لست ورشات تدريبية عُقدت في الفترة ما بين شهري آذار/مارس 2018 وتمّوز/يوليو 2018، حيث تضمّنت تلك الورشات طرح مفاهيم أساسية حول "الأمن الرقمي" بالإضافة لشرح خطوات عملية وتطبيقية حول تثبيت واستخدام أدواته الأكثر أهمية، إلى جانب عرض الحلول التي يمكن الاعتماد عليها بهدف الحفاظ على الخصوصية الرقمية وحماية المعلومات الحساسة، الأمر الذي يتيح العمل في بيئة أكثر أمناً بعيداً عن مختلف أنواع التهديدات التي قد تواجهنا من جهات عديدة.

ففي الوقت الذي أصبح فيه استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي على وجه الخصوص حاجة يومية يستحيل الاستغناء عنها، برزت تحديات أمنية جديدة أمام المستخدمين، تكمن في حماية أنفسهم من منظومة مراقبة وتعقّب قامت بالتعدّي على خصوصياتهم، وحوّلت معلوماتهم الشخصية وبياناتهم اليومية إلى سلعة تجارية ربحيّة أحياناً، وإلى أدوات لتهديد استقرار دول والتدخّل في شؤونها في أحيان أخرى.

عن الحق في الخصوصية:

"لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمسّ شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات."

المادة ١٢ من الإعلان العالمي لحقوق الإنسان

الفصل الأول: الأمن الرقمي وأهميته:

أ. مفهوم الأمن الرقمي:

في عصرنا الحالي باتت حماية بيانات المستخدمين ومراسلاتهم والمحتوى الذي يتفاعلون معه على مواقع التواصل الاجتماعي، تشكل جزءاً لا يتجزأ من أمنهم، وهو لا يقلّ أهمية عن حماية أنفسهم ومقرّبيهم وممتلكاتهم المادية على أرض الواقع.

ب. أهمية الأمن الرقمي:

تأتي أهمية الأمن الرقمي لحماية بياناتنا من التهديدات الالكترونية المتمثلة بـ:

1. البرمجيات الخبيثة: Malware

هي برمجيات مصممة للقيام بأفعال غير مرغوب بها على جهاز المستخدم دون علمه أو موافقته بهدف إيذائه، وقد تعمل هذه البرامج على سرقة كلمات السر أو تسجيل أنشطة المستخدم بشكل سري أو حذف بياناته، ويتراوح أذاها بين مجرد عرض الإعلانات، إلى تدمير القرص الصلب وعرقلة نظام التشغيل.
ومن أشهرها: الفيروسات، والديدان، وأحصنة طروادة.

2. برمجيات التجسس: Spyware

وهي البرامج التي تنقل معلومات من جهاز المستخدم إلى مكان آخر عبر شبكة الإنترنت دون علمه، عبر مراقبة الكتابة، أو المواقع الإلكترونية التي يزورها، وتجميع المعلومات الشخصية المتنوعة عنه، وقد يكون ذلك بهدف سرقة المعلومات مثل كلمة المرور، أو التجسس لأغراض تجارية.

تعاريف:

المعلومات: Information
وهي كافة البيانات المقروءة والمسموعة والمرئية مهما كانت طبيعة محتوياتها.

تكنولوجيا المعلومات: Technology Information
هي دراسة أو استخدام الأنظمة (خاصة أجهزة الكمبيوتر والاتصالات) لتخزين المعلومات واسترجاعها.

أمن المعلومات: Security Information
وهي حماية معلومات معينة (قد تكون مكتوبة على ورق أو موجودة في ملف ما على الإنترنت) من أن تستخدم من قبل أشخاص غير مُخوّل لهم بذلك، أو من أن تُكشف للعلن، أو تُوزع، أو تُعدّل، أو تُحذف.

الأمن الرقمي: Security Digital
مجموعة الأدوات والتطبيقات التي يتم استخدامها لحماية المعلومات على الكمبيوتر والانترنت.

وهي ليست برامج نقوم بتنصيبها، وإنما إحدى الإضافات التي قد تكون موجودة مع برنامج آخر، وتكون عادًة مخفيّة عن أنظار المستخدمين.

3. التصيد: Phishing

وهو محاولة للحصول على معلومات شخصية أو مالية للشخص المستهدف، عن طريق إرسال رسائل إلكترونية زائفة قد تحتوي على روابط تقوم بتوجيه المستخدم إلى مواقع الكترونية مُصمّمة خصيصاً لسرقة معلومات المستخدم. كما قد يقوم المتصيد بتحميل برامج خبيثة على جهاز الضحية تسمح له بالوصول إلى معلوماته، أو قد يستخدم أسلوب الهندسة الاجتماعية دون اللجوء إلى أي أدوات وذلك عبر خداع الضحية واستدراجه للحصول على ما يرغب فيه.

4. انتحال الشخصية: Identitie User Falsifying

يعمد منتحل الشخصية إلى استخدام هوية شخص آخر في العالم الافتراضي، وذلك بهدف الحصول على معلومات سرية أو أمنية أو مبالغ مالية مستخدمًا معلومات غير صحيحة أو غيرها من المعلومات التي قد تكون متاحة على مواقع التواصل الاجتماعي، والتي يرى فيها المنتحلون كنزاً معروضًا أمامهم لاستخدامها في عملياتهم الاحتيالية، أو قد يقوم المنتحل بإرسال رسالة تتضمن روابط صفحات مشابهة تمامًا للموقع الأصلي طالباً من المستخدم معلومات معيّنة عنه، كأن يطلب تحديث بياناته البنكية أو معلومات سرّية أخرى، وفي أحيان أخرى قد يلجأ المنتحل إلى الاتصال المباشر بالشخص المستهدف وطلب معلومات سرية بحجة أنه بحاجة إليها لتحديث النظام كونه يعمل في شركة الاتصالات.

5. هجمات الفدية: attacks Ransom

سُمّيت بذلك لأنها تعمل على تشفير بيانات حاسوب الضحية يتبعها عملية ابتزاز للضحية لدفع مبلغ من المال مقابل فك التشفير مرة أخرى، بدون وجود أي ضمانات حقيقية لفك التشفير في حال إرسال المبلغ. ومن الطرق التي يعتمدها القراصنة للإختراق: رسالة بريد إلكتروني تتضمّن مرفقًا مُلوثًا بالفيروس، الروابط الملغومة، المواقع الوهمية.

الفصل الثاني: الخصوصية والسرية:

من حقّ كلّ شخص الاحتفاظ بمعلوماته مخفية عن الآخرين إلّا ما ارتضى إظهارها، كما من واجب الآخرين الاعتراف له بهذا الحق وحفظه، ولكن استخدام الحاسوب والانترنت على نحو واسع أتاح الدخول السهل والسريع للمعلومات، وحتى ما هو منها خصوصي أو سري صار بإمكان المتطفلين أو ذوي النوايا الخبيثة الوصول إليه واستغلاله لغايات استفزازية أو ربحية.

وتؤدي مثل هذه الانتهاكات ـ والتي تعتمد على الاستخدام السلبي للإنترنت ووسائل التواصل الاجتماعي واستغلالها لأغراض غير قانونية وغير أخلاقية ـ إلى إلحاق الضرر بالأفراد، ويتعدّاه ذلك إلى الضرر العام بالدول، إذ أصبحت المواقع الإلكترونية الحساسة مثل تلك الخاصة بأجهزة الدولة والتي تحمل ملفات سرية في غاية الأهمية، عرضة للاختراق، الأمر الذي حوّل هذه الاعتداءات إلى حروب إلكترونية بين الدول.

وفي حين تسعى قوانين الجرائم الإلكترونية المطبّقة في بعض الدول للحفاظ على الخصوصية والأمان لمستخدمي الإنترنت، تبقى هذه القوانين غائبة في دول أخرى، وبشكل عام تقع على مستخدمي الإنترنت مسؤولية حفظ أمنهم الرقمي بشكل شخصي وحماية معلوماتهم الخاصة والسرية عن طريق أخذ الاحتياطات اللازمة.

للمعلومات مستويات عدة تتراوح بين العام والخاص والسري، وإن كل المعلومات مهما كانت طبيعتها قابلة للاستخدام، لذلك فمن الضروري الأخذ بعين الاعتبار تمييز مستوى المعلومة حسب المتلقي، وعدم الاستهتار بأية معلومة يمكن خسارتها.

"يُجرّم القانون في العديد من الدول درجات معينة من انتهاك الخصوصية الفردية، بينما تقوم حكومات كثيرة في نفس الوقت بانتهاك خصوصية الأفراد من خلال التجسس عليهم"

يمكن التفريق بين مفهومي الخصوصية والسرية الإلكترونية على النحو التالي:

السرية: هي حالة حفظ أو الاحتفاظ بالمعلومة مخفية إلا عن الأشخاص المخوّلين بالاطلاع عليها.
ومن الأمثلة على المعلومات التي يجب الحفاظ على سريتها: كلمات مرور الحسابات الالكترونية والبنكية.
الخصوصية: هي الحد الذي يفصل بين ما يحق للمجتمع (الآخرين) معرفته عن حياتنا الخاصة وما لا يحق لهم معرفته.
وفي تعريف آخر: هي قدرة أو حق شخص أو مجموعة من الأشخاص في البت بما يمكن نشره من معلومات عنهم على العلن وما لا يمكن نشره.

ويمكن للخصوصية على الإنترنت أن تتضمن معلومات محددة لشخصية مستخدم الإنترنت كتاريخ ميلاده وعنوانه ورقم هويته أو جواز سفره، أو معلومات غير محددة للشخصية مثل سلوك زائر ما لموقع ما على الإنترنت.
رغم اهتمام وسائل التواصل الاجتماعي بإعدادات الخصوصية واعتمادها آليات لتأمين هذه المواقع، إلا أنه لا توجد وسيلة لتوفير الحماية الكاملة لها، ويبقى من الضروري اتخاذ خطوات احترازية.
قد يستخدم المخترقون حيلًا للحصول على المعلومات السرية للأشخاص عبر حساباتهم على مواقع التواصل الاجتماعي، واستخدامها في أغراض غير مشروعة قد تصل إلى ارتكاب جرائم كالابتزاز والاحتيال المصرفي والاستغلال الجنسي.
وتحتوي وسائل التواصل الاجتماعي على ثغرات تمكّن من يمكن اعتبارهم طرفًا ثالثًا من الوصول إلى المعلومات الخاصة. فعلى سبيل المثال: تتضمن الخصوصية على موقع فيس بوك اختيار فيما إذا كنا نريد أن يكون المنشور عاماً أو مقتصراً على الأصدقاء، إلّا أن غالبية الأشخاص لديهم

عدد كبير من الأصدقاء الافتراضيين دون معرفتهم في العالم الحقيقي، ومن الصعب التعرف على من قد يقوم بانتهاك خصوصية معلوماتنا كإعادة نشرها أو استخدامها دون معرفتنا مثلًا.

بتاريخ 25 أيار/مايو 2018 دخل قانون حماية البيانات أم ما يعرف بنظام حماية البيانات العام RPDG حيز التنفيذ في الاتحاد الأوروربي والذي يسعى إلى حماية الحقوق الرقمية لمواطني الاتحاد الأوروبي من خلال قوانين أكثر صرامة للبيانات ومراقبة أكبر لكيفية إدارة الشركات للموعلومات الشخصية للأشخاص، ويمكن أن يؤدي عدم الالتزام باللائحة الجديدة إلى فرض غلامات تصل إلى 20 مليون يورو.

الفصل الثالث: الهندسة الاجتماعية:

قد لا يكفي تحصين أجهزتنا ببرمجيات الحماية من القرصنة ومكافحة الفيروسات وغيرها لحمايتها من الاختراق الإلكتروني، فمع كل ما يمكن لمطوّري النظم الأمنية ابتكاره في هذا المجال، يبقى لجانب آخر ربما يكون أكثر أهمية دورًا في ذلك وهو العنصر البشري المتمثل بالمستخدم.

وقد يعتمد المخترق على العنصر البشري فقط للوصول إلى ما يريده من معلومات سرية مستخدمًا أساليب الحنكة والمكر، ومن دون أن تتوافر لديه بالضرورة معرفة تقنية عميقة، هذا الأسلوب هو ما بات يعرف بالهندسة الاجتماعية.

يمكن تعريف الهندسة الاجتماعية في سياق أمن المعلومات على أنها استخدام الخداع للتلاعب بالأفراد من أجل الكشف عن معلوماتهم السرية أو الشخصية والتي يمكن استخدامها لأغراض احتيالية.

وفي الأساس تُعرّف الهندسة الاجتماعية على أنها فن الوصول إلى المباني أو الأنظمة أو البيانات عن طريق استغلال علم النفس البشري بدلًا من استخدام تقنيات القرصنة التقنية.

أ- أساليب الهندسة الاجتماعية:

يُطوّر "المهندسون الاجتماعيون" بشكل مستمر أساليب جديدة لخداع ضحاياهم ومن أساليب الهندسة الاجتماعية:

1ـ استغلال الشائعات:

يستغل المهندسون الاجتماعيون الشائعات والتي تنتشر بشكل سريع على وسائل التواصل الاجتماعي، كغلاف جذاب لتمرير محتواهم الخبيث، ليصبح كل من يساهم في نشر الشائعة عرضة لاختراق حساباته الاجتماعية وربما أجهزته.

2ـ استغلال عواطف الضحية وطباعه الشخصية:

يستغل المهندس الاجتماعي عواطف الضحية من أجل جمع بيانات عنه، واستخدام هذه البيانات في الدخول إلى حساباته الشخصية ومواقع التواصل الاجتماعي الخاصة به. كأن يستخدم نصوصاً أو صوراً تخاطب عاطفة الضحية (انتقام، حقد، حب، شوق...) أو تؤجج مشاعره الدينية أو القومية، وتوقعه في فخ فتح الرابط الخبيث.

3ـ استغلال المواضيع الساخنة:

يستغل المهندسون الاجتماعيون المواضيع الساخنة التي تنتشر على شكل أخبار عاجلة بوسائل الإعلام لتمرير عملياتهم الاحتيالية، مستفيدين من اهتمام الجمهور بها مما يجعلها طعمًا ملائمًا لإيهام الضحية بأنها روابط آمنة.

4ـ استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية:

قد يعمد المهندس الاجتماعي لإنشاء حساب مستعار للتحايل على الضحية، كما قد يستغل ضعف خبرة الضحية بموضوع الأمن الرقمي عبر دفعه لفتح رابط أو ملف خبيث على أنه آمن.

5ـ انتحال الشخصية:

يعمد المهندس الاجتماعي للتواصل المباشر مع الضحية عبر الهاتف أو من خلال إنشاء حسابات وهمية مطابقة لإسم صديق أو مقرب من الضحية ليقوم بعدها بالاستجرار التدريجي للمعلومات.

6ـ استغلال السمعة الجيدة لتطبيقات معينة:

يقوم المهندس الاجتماعي بالإيحاء للضحية بأنّ ملفًا أو رابطًا هو نسخة محدّثة عن تطبيق معين بينما يكون رابطًا خبيثًا.

7ـ اصطياد كلمات السر:

يعمد المهندس الاجتماعي إلى الخداع من أجل الحصول على كلمة سر الضحية، فقد يرسل إلى الضحية صفحة من تصميمه تشبه صفحة تسجيل الدخول لأحد المواقع الشهيرة من حيث الشكل، لكنها تحمل عنوانًا مختلفًا عن العنوان الأصلي، وعندما يُدخل الضحية كلمة السر للولوج في حسابه تصل بكل بساطة إلى المخترق ويكون الضحية قد وقع بالفخ دون أن يشعر بالخداع.

8ـ استغلال التواجد الفيزيائي للمهاجم قريبًا من الضحية:

فعندما يتواجد المهندس الاجتماعي والضحية في نفس المكان يتمكن المهاجم من الوصول إلى جهاز الضحية عبر الحنكة.

فقد يترك المهندس الاجتماعي نقطة الوصول (WIFI) مفتوحة عمدًا حتى يتصل بها الضحية فيخترق حاسوبه، أو قد يطلب منه توصيل بطاقة ذاكرة مع جهازه مما يفسح المجال أمام الملفات الخبيثة للانتشار في نظام الحاسوب وتدمير البيانات.

9ـ خيانة الثقة:

قد يكون المهندس الاجتماعي صديقًا أو زميلًا في العمل، يستغل الثقة الممنوحة له من الضحية لاختراق جهازه والتلصص عليه.

ب- نصائح للحماية من الهندسة الاجتماعية:

- التثقيف بمجال الأمن الرقمي وأساليب الاختراق المتجددة.
- تجنب إعطاء أي معلومات سرية أو بيانات شخصية إلا بعد التأكد من هوية الشخص المتحدث، وأن الاتصال تم من جهة رسمية أو معروفة.
- تجنب الحديث في الأسرار الشخصية مع الأصدقاء المجهولين عبر وسائل التواصل الاجتماعي.
- عدم فتح مرفقات البريد الإلكتروني المرسل من أشخاص غير معروفين.
- العمل على تأمين هواتفنا أو حواسيبنا واستخدام برامج لمكافحة الفيروسات.

الفصل الرابع: التواصل الاجتماعي:

أتاحت وسائل التواصل الاجتماعي المجال واسعًا أمام مرتاديها للتعبير عن أنفسهم، ومشاركة مشاعرهم ومشاريعهم وأفكارهم مع الآخرين، وإلى جانب توفيرها سهولة التواصل بين الأفراد، وسرعة وسهولة تداول المعلومات، أمّنت هذه الشبكات خدمات تعليمية وإخبارية وتجارية وخدمية وحكومية.

ولكن بموازاة ذلك ومن جانب آخر سهّلت هذه الشبكات نشر الشائعات والأخبار الكاذبة، كما استخدمها البعض في عمليات التحايل والتزوير والنصب والابتزاز، فضلاً عن انتحال الشخصيات وانتهاك الخصوصية.

فكيف يمكن التعامل مع شبكات التواصل الاجتماعي وما هي المعلومات التي يجب عدم ذكرها.

تنقسم المعلومات التي يتوجب عدم ذكرها على وسائل التواصل الاجتماعي إلى:

أ. معلومات خاصة:

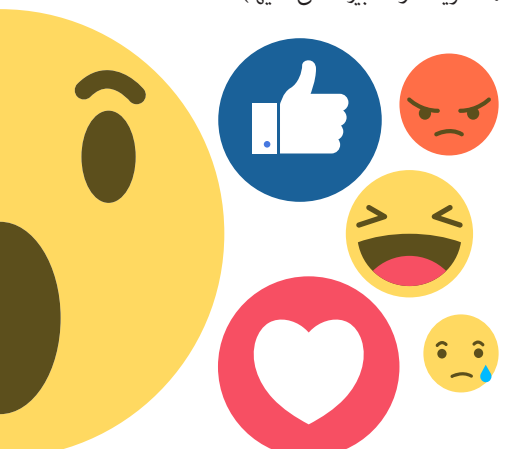
- الصور الشخصية: التي لا نرغب بمشاركتها مع الجميع حتى وإن تم إرسالها عبر رسالة خاصة.
- الآراء الشخصية: التي تؤثر على الوضع المهني/ القانوني/ السياسي/ الاجتماعي الحالي أو المستقبلي.
- التعبيرات النفسية: الناتجة عن حالة معينة كالغضب والحقد والقدح والذم والتهديد.

ب. معلومات حساسة:

- معلومات الهوية الشخصية (تاريخ الميلاد، اسم الوالدين، مكان الإقامة، مكان الولادة، رقم القيد، رقم الهوية، رقم الهاتف الشخصي).
- أنشطة غير مرغوب فيها من قبل جهات قادرة على أن تشكل خطرًا على ممارسيها.
- تحديد مواعيد وأماكن التنقل قبل وأثناء الحدث.

ج. معلومات سرية:

المعلومات السرية أياً كان نوعها يجب تجنّب تداولها عبر وسائل التواصل الاجتماعي، بما في ذلك ضمن الرسائل الخاصة حتى وإن كانت مموّهة (كاستخدام ألقاب أو أسماء مزيفة أو تعابير متّفق عليها).



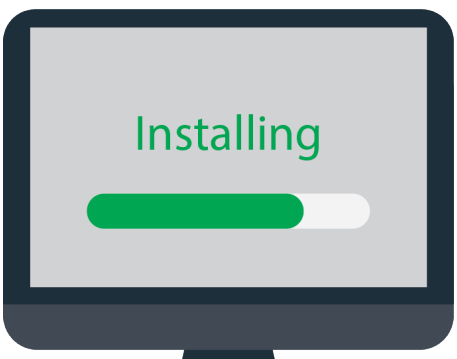
الفصل الخامس: البرامج والتحديثات:

أ. البرامج المقرصنة: Pirated software

قرصنة البرامج هي النسخ أو التوزيع أو الاستخدام غير القانوني لبرامج الحاسوب المختلفة.

بدأت ظاهرة القرصنة مع بدايات ظهور الحاسوب، وازدادت بشكل كبير مع استخدام تقنية الشبكات، وهي عملية تتطور بسرعة فائقة باستخدام تقنيات حديثة، وبات من المتاح بشكل شائع رؤية مواقع على الانترنت مختصّة بترويج البرامج المقرصنة مجاناً أو مقابل مبلغ مادي رمزي.

تعدّ قرصنة البرامج تجارة مربحة لفتت انتباه جماعات الجريمة المنظمة في عدد من البلدان، وهي تؤدي إلى خسائر مادية باهظة جدًا للشركات التي قد تستطيع الكبيرة منها مقاومتها بينما تفضي إلى إفلاس الشركات الناشئة.



وقد دفعت قرصنة البرامج الشركات المختصة في صناعة البرامج إلى الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات "منظمة اتحاد برمجيات الأعمال" Business Software Alli-ance"والتي تعرف باختصار "BSA"، ووفقًا للمنظمة تم سرقة نحو 36% من جميع البرامج المستخدمة عام 2005.

مخاطر البرامج المقرصنة:

تعود قرصنة البرامج بأضرار على كل من الشركات المنتجة لبرامج الحاسوب، وعلى المؤلفين والمستخدم نفسه.
إذ يسهم شيوع استخدام البرامج الأصلية بين المستهلكين في خفض أسعارها، بينما يؤدي الاعتماد على البرامج المقرصنة إلى ارتفاع أسعار هذه البرامج، وذلك فضلًا عن أن القرصنة ستؤدي إلى زيادة تكلفة المنتجات بسبب دفع الشركات مبالغ كبيرة لحماية منتجاتها منها.
وتؤثر القرصنة كذلك بشكل مباشر على مصادر تمويل عمليات تطوير البرامج، والتي سيخشى مستثمروها من المخاطرة في أموالهم ببرامج قد لا تحقق الربح بسبب السطو عليها ونشرها.
وفي ذات السياق يتأثر مؤلفو ومطورو البرامج، والذين يبذلون جهدًا ووقتًا على التطوير المستمر لهذه البرامج وعرضها للاستخدام أمام المستهلكين معتمدين في ذلك على الأرباح التي سيجنوها من بيع منتجاتهم.

- في عام 2010 بلغت الخسائر بسبب قرصنة البرامج 59 مليار دولار على مستوى العالم.
- من بين 3000 لعبة تم تطويرها لم تحقق سوى 150 لعبة نجاحًا يضمن استرداد الأموال المستثمرة وتحقيق هامش ربح جيد.

شركة مايكروسوفت

مخاطر كبيرة للبرامج المقرصنة على المستخدمين يتوجب الحذر منها:

غالباً تحتوي البرامج المقرصنة على برمجيات خبيثة تعمل على تجميع المعلومات وإرسالها بشكل دوري، الأمر الذي قد ينتج عنه مخاطر متعددة قد تصل لبيع المعلومات الشخصية، أو حتى لإستخدام الجهاز المصاب كأداة لتنفيذ عمليات إجرامية دون علم صاحب الجهاز.

ماذا يؤمّن استخدام البرامج الأصلية؟

بإمكان مستخدمي البرامج الأصلية ضمان التمتع بالدعم الفني وخدمات ما بعد البيع والتي تشمل:

- ضمان الجودة وإمكانية استبدال نسخة البرنامج في حال وجود أي خلل فيها.
- إمكانية التواصل الهاتفي مع المنتج للإجابة عن أي استفسار، أو للاطلاع على أحدث الإصدارات.
- إمكانية التدريب على استخدام البرنامج.
- حماية جهاز الحاسوب من الفيروسات.

تنتشر قرصنة البرامج بشكل أكبر في الدول النامية مقارنة بالدول المتقدمة خاصة تلك التي تعتمد قوانين مكافحة الجرائم الالكترونية وحماية حقوق الملكية. ويعود ذلك لأسباب عدة منها: غياب الرقابة الحكومية على من ينشرون المنتجات المقرصنة على الإنترنت ومن ينتهكون حقوق الملكية للآخرين، وغلاء أسعار المنتجات الأصلية مقارنة بمتوسط دخل الفرد، وانتشار المنتجات المقرصنة بكثرة في الإنترنت والأسواق والمكتبات، فضلًا عن ضعف المعرفة حول البرمجيات مفتوحة المصدر والتي سنتعرف عليها في الفقرة القادمة.

ب. البرامج مفتوحة المصدر (البرمجيات الحرة): Open source software

هي البرامج التي تتيح الاستخدام والتعديل والنشر دون قيود، إذ تكون شفرتها البرمجية متاحة للجميع، ويمكن تطوير هذه البرامج بطريقة تعاونية، أي يمكن لأي شخص التعديل على النسخة الأصلية من البرنامج بحيث يصنع نسخته الخاصة منه.

وهي بذلك تختلف عن البرامج مغلقة المصدر "الاحتكارية" والتي لا تتيح شفرة المصدر الخاصة بها، ولا تسمح إلا للمطورين الرسميين بالتعديل عليها.

فوائد البرامج مفتوحة المصدر:

- آمنة لأنها تخضع لمراقبة مفتوحة من المطوّرين.
- مجانية أو بتكلفة بسيطة لأنها غير قائمة على الربح فقط.
- مستمرة في التطور والنمو بالتناسب مع عدد المستخدمين.

لا يمكن اعتبار البرامج مفتوحة المصدر غير ربحية تماماً، فبعض الشركات تمكنت من جني ملايين الدولارات عبر بيع البرامج مفتوحة المصدر وتسويقها ودعمها.
ومن هذه البرامج: نظام تشغيل الهواتف النقالة "أندرويد"، المتصفح غوغل كروم، وبرنامج الاتصال الآمن تور.

أمثلة على برامج مفتوحة المصدر:

يمكن إيجاد أي برنامج بمصدره المفتوح والمرخّص للاستخدام مجانًا بشكل قانوني عبر محركات البحث من خلال كتابة وصف للبرنامج مع عبارة "مفتوح المصدر" باللغتين العربية أو الإنجليزية.

فيما يلي رابط لمستودع آمن ومشهور لبرامج مفتوحة المصدر: https://sourceforge.net/

ج. التحديثات: Updates

يطرح التعامل مع التحديثات تساؤلات حول أهميتها ومخاطر إهمالها، وقد يلجأ البعض لإغلاقها بشكل نهائي، أو تركها بحسب إعداداتها الافتراضية، بينما يعاني البعض الآخر من صعوبة الحصول عليها .

فما هي هذه التحديثات وكيف يمكن الاستفادة منها؟
التحديثات: هي عملية إجراء تعديل أو استبدال أو إضافة على المميزات بعد صدورها من قبل المطوّر، وذلك لتوفير مزايا جديدة أو إغلاق ثغرات أو حل مشاكل، وأهم ما في هذه التحديثات هي التحديثات الأمنية.

تعمل التحديثات بشكل عام على تأمين الحماية لأجهزتنا، إذ أن التحديثات الأمنية للتطبيقات وأنظمة التشغيل تعمل على معالجة الثغرات التي قد تفتح المجال للتجسس وسرقة المعلومات، وبالتالي تؤمن هذه التحديثات حماية كبيرة لخصوصيتنا.

وكمثال على ذلك: التحديث الذي أطلقه تطبيق واتساب لتفعيل ميزة جديدة للتشفير من المستخدم إلى المستخدم.

وليس بالضرورة أن يحتوي التحديث على ميزة جديدة تمامًا، إذ من الممكن أن يهدف لمعالجة ميزة موجودة مسبقًا، مثل تحديثات برامج الحماية لكي تتمكن من التعرف على الفيروسات والتهديدات الحديثة، كالتحديثات على أنظمة التشغيل التي تعالج بعض المميزات لتطوير قدراتها وسد الثغرات بوجه أدوات التجسس والمراقبة.

إن الهدف الأساسي للتهديدات التي تعمل على استغلال الثغرات هو سرقة المعلومات وهو ما يشكل اختراقا للخصوصية، بغض النظر عن النتائج النهائية المختلفة بحسب نوع التهديد، فلولا قدرة هذه التهديدات على اختراق الخصوصية والتعرف على معلومات خاصة لما تمكنت من الوصول لهدفها النهائي، والذي قد يكون تدمير الملفات أو تشفيرها أوسرقتها.

أهمية التحديثات:

1ـ تحديثات أمنية: ترسل شركات البرمجيات تحديثات أمنية ضرورية بشكل مستمر، حرصًا منها على سد الثغرات التي قد تُكتشف في برامجها وأنظمتها.

2- تحسين الأداء: على سبيل المثال تعمل الشركات على تحديثات يمكنها تحسين أداء المعالج الخاص بالجهاز وبالتالي رفع كفاءته، أو العمل على تحسين كفاءة ذاكرة الجهاز وبالتالي تأمين سرعة أكبر له.

3ـ توافق أفضل مع الأجهزة والتطبيقات: قد تواجه بعض المستخدمين مشكلة في عدم توافق أجهزتهم مع بعض التطبيقات التي يرغبون في تحميلها، ولتفادي ذلك تقوم الشركات بإطلاق تحديثات جديدة دومًا خاصة بعد صدور تحديثات رئيسية للنظام، وذلك لجعلها متوافقة مع الإصدارات الجديدة، بالتالي من الضروري تحديثها حتى تكون مستقرة.

4ـ ميزات جديدة: تسعى الشركات طوال الوقت لإطلاق المزيد من الميزات الجديدة، في محاولة منها لإرضاء المستهلكين والإبقاء عليهم وجذب المزيد منهم.

إن حاجتنا لتحديث برامجنا بشكل دائم مرتبط بشكل وثيق بأهمية الحفاظ على بياناتنا وخصوصيتنا، لذلك من الضروري الحصول على التحديثات فور وصولها وعدم تجاهلها.

الفصل السادس: أمن الهاتف المحمول:

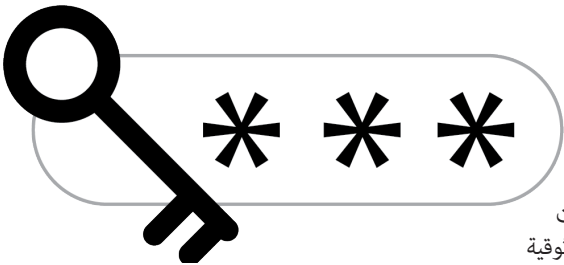
أصبح لأمن الهاتف المحمول أهمية كبيرة مع زيادة اعتمادنا عليه في حياتنا اليومية، فهو لم يعد وسيلة للاتصال الهاتفي فحسب، بل بتنا نُخزّن عليه معلوماتنا الشخصية والتجارية، ومشاريعنا العملية والحياتية، فضلًا عن كونه يرافقنا في كل الأوقات والأماكن.
إضافة لذلك أتاحت الهواتف الذكية ميزة الوصول إلى الإنترنت واستخدام البريد الإلكتروني ووسائل التواصل الاجتماعي وتحميل التطبيقات والألعاب.
وغيرها مع كلّ ما قد يشكله ذلك من مخاطر على خصوصيتنا التي أصبحت سهلة الاختراق.

لذلك يجب التعرّف على وسائل الحماية لهواتفنا، وطرق تقليل المخاطر الإلكترونية والتي لا يمكن منعها بشكل كامل.

خطوات يجب أن نقوم بها للحصول على هاتف آمن:

1- اختيار جهاز من شركة تهتم بإصدار التحديثات.
2- استخدام قفل للهاتف: أفضل طريقة لقفل الهاتف هي اختيار الرقم السري.
3- استخدام خاصية المصادقة الثنائية من غوغل: "التحقق بخطوتين".
4- استخدام التطبيقات حصرًا من متجر غوغل "للهواتف التي تعمل بنظام أندرويد"، و آيتون "للهواتف التي تعمل بنظام IOS" مع الانتباه لتفقّد المعلومات حول المنتج للتطبيق، وإلقاء نظرة على آراء المستخدمين.
5ـ استخدام تشفير الجهاز الكامل: تحتوي أنظمة تشغيل الهواتف على خاصية لتشفير الهاتف يمكن تفعيلها عن طريق الإعدادات في الهاتف ثم الأمان أو الحماية.
كما يمكن تفعيل التشفير لبطاقة الذاكرة الخارجية SDcard.
6- استخدام VPN لتشفير الاتصال بالانترنت عند الحاجة: "الشبكة الخاصة الافتراضية" وهي الطريق الأكثر أماناً للاتصال بالانترنت، إذ تقوم بالمحافظة على بيانات المستخدمين ونشاطاتهم مخفية ومشفرة عبر إنشاء نفق وهمي بين الجهاز ومزود خدمة VPN مما يعني عدم قدرة أي أحد على اعتراضها.
7- تجنب حفظ كلمات المرور على المتصفح واستخدام برنامج إدارة كلمات المرور:
تحدث أبرز عمليات الاختراق على الإنترنت بسبب ضعف كلمات المرور والاستخدام المتكرر لها في حسابات متعددة، ولذلك يكون الحل الأفضل هو استخدام أحد برامج إدارة كلمات المرور لحفظ معلومات الدخول بالحسابات المختلفة.
8- استخدام برنامج مكافحة الفيروسات:
تعمل برامج مكافحة الفيروسات على اكتشاف التطبيقات الخبيثة التي قد تصيب جهاز الهاتف وإزالتها، كما أنها قد تعمل في النسخ المدفوعة كمراقب وناصح لحماية الخصوصية أثناء التصفح واستخدام تطبيقات وغيرها.
9- إغلاق الاتصال بالانترنت في حال عدم الحاجة إليه.
10- إزالة التطبيقات التي لا نستخدمها.

الفصل السابع: كلمة السر:



تعتبر كلمة السر أو كلمة المرور بمثابة المفتاح للوصول إلى كافة معلوماتنا وبياناتنا الشخصية المخزّنة على أجهزتنا، وكما نعتني باختيار مفتاح محكم لمنزلنا أو خزانة أموالنا يجب أخذ الاحتياطات اللازمة لتكون كلمة سرنا قوية تتميز بتشفير عال ووثوقية تامة، بحيث يصعب سرقتها واستخدامها في فتح حساباتنا أو انتحال شخصيتنا.

أ. كيف يتمكن القراصنة من كشف كلمة السر الخاصة بنا؟

يستعمل القراصنة عدة طرق منها استخدام برامج التنبؤ بكلمات السر، والتي تجرّب بسرعة فائقة عدد كبير من الاحتمالات بالدقيقة الواحدة لمعرفة كلمة السر بعد تزويدها ببعض المعلومات حول صاحب الحساب والتي من الممكن الوصول إليها بسهولة من خلال وسائل التواصل الاجتماعية وغيرها.

بالإضافة إلى العديد من طرق الاحتيال أو التجسس التي تمكنهم من الوصول لكلمة السر. وفي حال توفر الوعي الكافي والحماية لدى المستخدم يبقى الخيار الوحيد المتاح للقراصنة هو عبر التنبؤ الذي قد يكون سهلاً فيما لو لم نقم باختيار كلمة السر بشكل صحيح.

ب. نقاط مهمة عند اختيار كلمة السر:

1- أن تكون طويلة بحدود 14 حرفًا على الأقل، إذ يسهل اختراق كلمات السر القصيرة بواسطة البرامج التي تحدثنا عنها في الفقرة السابقة.
2- أن تكون معقدة أي تحتوي على حروف كبيرة وصغيرة وأرقام ورموز، وهو الأمر الذي يزيد صعوبة اختراقها.
3- أن تكون عشوائية لا تستخدم أنماط معتادة مثل: 1234 أو QWEASD.
4- أن لا تحتوي على أية معلومات عن الهوية الشخصية مثل تاريخ أو مكان الميلاد أو أرقام هواتف أو حتى معلومات متعلقة بصاحب الحساب مثل طعامه المفضل أو المدينة التي يقطنها.
5- أن تكون كلمة سر يمكن تذكرها دون الحاجة لكتابتها على ورقة أو ملف يسهل فتحه، كتخزين كلمة السر في ملف إكسل، مثال: Ig3GaM20bFmf وهي اختصارات لعبارة بالإنكليزية: I got 3 gifts at my 20th birthday from my friends
6- أن تكون كلمة سر فريدة لا تُستخدم نفسها لأكثر من حساب وذلك لتقليص حجم الضرر الذي قد يحدث في حال اكتشافها.
7- تغيير كلمة السر بشكل دوري "كل ثلاثة شهور فترة جيدة".
8- التعرّف على كيفية استعادة كلمة السر أثناء إنشاء الحساب، إذ تستخدم مواقع عدة أدوات لاستعادة كلمة السر، وهنا يجب الحرص على أن تكون عملية الاستعادة آمنة، ففي حال استخدام سؤال لاستعادة كلمة السر يجب أن تنطبق على جوابه نقاط اختيار كلمة السر نفسها.
9- عدم كتابة كلمة السر على أجهزة عامة أو أجهزة الأصدقاء، إذ تقوم برامج رصد لوحة المفاتيح بتسجيل أي كلمة يتم طباعتها على الحاسوب، ويصبح بالإمكان سحب كلمات السر بسهولة.
10- استخدام برنامج آمن لإدارة كلمات السر مما يساعد على اختيار كلمات سر قوية دون الحاجة لحفظها جميعًا مثل برنامج KeePass.

ج. ما هو برنامج كيباس KeePass ؟

برنامج مجاني مفتوح المصدر يعمل على جميع أنظمة ويندوز وماكنتوش، كما يتوفر منه نسخ للأجهزة الذكية iphone، ipad، Android، BlackBerry، يهدف إلى إدارة وإنشاء كلمات مرور الحسابات الخاصة بك ضمن قاعدة بيانات الكترونية، محمية برقم سري.

يتيح هذا البرنامج حفظ عدد كبير من الحسابات متضمنة كلمة السر واسم المستخدم لكل حساب، كما يقترح كلمات سر صعبة تتكون من أحرف ورموز وأرقام من خلال مولّد كلمات السر الذي يحتويه، بالإضافة إلى أنه ينظم الحسابات وكلمات السر الخاصة بها ضمن مجموعات، على سبيل المثال: مجموعة حسابات الشبكات الاجتماعية، مجموعة حسابات البريد الإلكتروني.

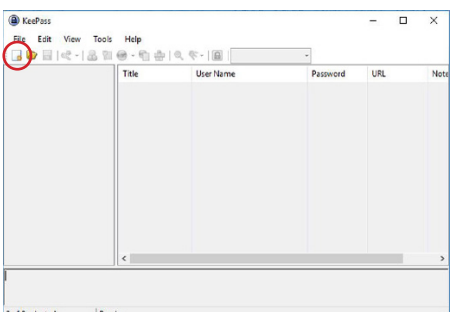
ميزات أخرى للبرنامج:

- سهولة الاستخدام إذ أن البرنامج بسيط وواضح ويمكن حمل نسخة منه بسهولة دون الحاجة إلى تنصيب، فهو متوفر بنسخة محمولة Por-table.
- إمكانية نقل ملف الحسابات وكلمات السر على فلاشة أو على قرص مضغوط أو حفظها على التخزين السحابي لاستخدامها على أجهزة أخرى.
- إمكانية تصدير الحسابات وكلمات السر إلى العديد من الصيغ مثل TXT، HTML، XML، CVS.
- إمكانية استيراد الحسابات وكلمات السر من عدة أنواع من الملفات.
- إمكانية البحث ضمن البرنامج عن حساب معين.
- البرنامج متوفر بثلاثين لغة.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي: https://keepass.info/download.html

طريقة الاستخدام

1. بعد تحميل البرنامج قم بعملية التثبيت على جهازك، عند فتح البرنامج للمرة الأولى ستظهر لك الواجهة الرئيسية للبرنامج
2. إضغط على الأيقونة المشار إليها في الصورة أسفله ليتم إنشاء قاعدة البيانات ومن بعدها اضغط على OK



3. ثم ستظهر نافذة تطلب منك اختيار اسم ومسار حفظ قاعدة البيانات
4. بعدها ستظهر لك نافذة تطلب منك إنشاء كلمة مرور لقاعدة البيانات
   أ. في خانة Master password اكتب الرقم السري الرئيسي
   ب. أعد كتابته في خانة Repeat password سيظهر لك مدى قوة الكلمة الرئيسية بجانب quality-ed Estimat

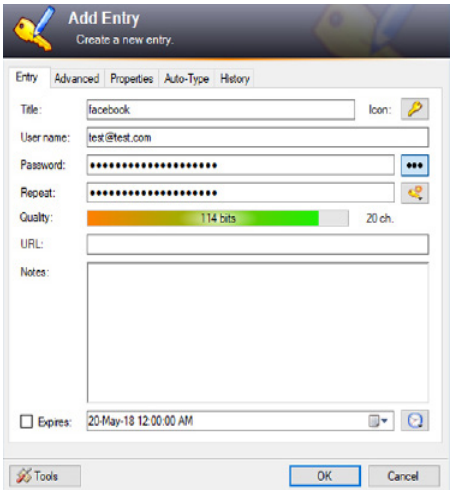
بعد الإنشاء ستظهر لك نافذة تطلب منك وضع إعدادات اضافية لقاعدة البيانات مثل

أ. الاسم في خانة Database name

ب. الوصف في خانة Database description

ج. اسم مستخدم افتراضي في خانة for new entries Default user name

لإضافة كلمات سر للقاعدة اضغط في القائمة على زر الفأرة الأيمن ثم إضغط على زر Add Entry



ستظهر لك هذه النافذة للبدء بادخال البيانات

1. في خانة Title أكتب عنوان الحساب مثل الفيس بوك
2. في خانة Username اكتب اسم المستخدم او الايميل
3. في خانة Password اكتب الرقم السري
4. في خانة Repaet أعد إدخال الرقم السري
5. في خانة URL اكتب عنوان صفحة تسجيل الدخول أو رابط الموقع الرئيسي.
6. في خانة NoteS يمكنك كتابة ملاحظات حول الحساب
7. من خانة Expires يمكنك وضع مدة صلاحية لكلمة السر والبرنامج سيذكرك بانتهائها لتقوم بحذفها أو تغييرها

يمكنك نسخ اسم الحساب أو كلمة المرور بالضغط عليهما في الصفحة الرئيسية للبرنامج

د. وسائل أمان إضافية:

تعتمد وسائل التواصل الحديثة على طرق مختلفة لتسجيل الدخول، أغلبها يطلب إضافة اسم المستخدم وكلمة السر مثل: البريد الإلكتروني جيميل، وموقعي فيس بوك وتويتر وغيرهما.، وبعضها الآخر يطلب تسجيل رقم الهاتف فقط مثل: واتساب وتيليغرام وغيرهما من الوسائل المشابهة.

ولكن كيف يمكننا أن نزيد من أمان حساباتنا في حال فقدان كلمة السر أو سرقتها؟

توفر أغلب وسائل التواصل الاجتماعي خيارات أمان إضافية، وبالتالي فنحن لا نعتمد فقط على كلمة السر لحماية حساباتنا.

ومن أهم هذه الوسائل التي يتوجب علينا استخدامها هي استخدام بريد بديل، والتحقق بخطوتين.

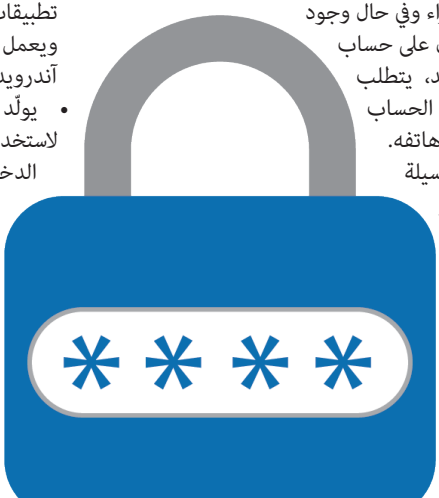
- استخدام بريد بديل: إن إضافة بريد إلكتروني بديل عند إنشاء الحساب يرفع من مستوى الأمان، وهو ما يؤمن عند محاولة أي مخترق تسجيل الدخول على الحساب من جهاز آخر، وصول رسالة تحذيرية على بريد المستخدم البديل تمكّنه من تأمين حسابه، وتغيير كلمة السر إن اقتضى الأمر ذلك.
- التحقق بخطوتين: هي من الخاصيات التي تندرج ضمن طرق تعزيز حماية حسابات المستخدم، إذ أنها تطلب التأكيد من خلال وسيلة مختلفة على أن عملية تسجيل الدخول تتم عبر صاحب الحساب، فبعد إدخال كلمة السر يحتاج المستخدم إلى رمز إضافي قد يكون عبر الهاتف او باستخدام برنامج مولد الرموز من غوغل، الأمر الذي يساهم في تحصين الحساب.

تُقلل خاصية التحقق بخطوتين كثيرًا من انتحال هوية المستخدم، والدخول غير المُصرّح به إلى معلوماته الحساسة والاستيلاء عليها. وقد باتت كافة وسائل التواصل الاجتماعي تستخدم ميزة التحقق بخطوتين، والتي يمكن تفعيلها من خلال عدة طرق منها :

1- الرسائل النصية "SMS".
2ـ تطبيق إنشاء الرموز.
3ـ رموز الاسترداد.

استخدام الرسائل النصية:

تعتبر أسهل طريقة من طرق تفعيل التحقق بخطوتين وأكثرها انتشارًا، وتتم عبر ربط حساب المستخدم برقم هاتفه، وبناءً على هذا الإجراء وفي حال وجود أي محاولة لتسجيل الدخول على حساب المستخدم من جهاز جديد، يتطلب ذلك تأكيد أنه صاحب الحساب باستخدام الرمز المُرسل إلى هاتفه. تظهر نقاط ضعف هذه الوسيلة في حال فقدان الهاتف، أو عند التواجد في بلدان تعمد حكوماتها إلى اعتراض الرسائل النصية دون إذن أصحابها، أو إلى استخدام أرقام هواتفهم، وإعادة ضبط كلمة السر الخاصة بهم.



تطبيق مولد الرموز من غوغل:

- يقوم هذا التطبيق بتوليد رموز تحقق مؤقتة للدخول إلى الحساب، وهو يعتبر أحد أهم تطبيقات إنشاء الرموز مفتوحة المصدر، ويعمل على أجهزة الهواتف الذكية ذات أنظمة آندرويد وآيفون وبلاك بيري.
- يولّد هذا التطبيق رموز أمان عشوائية لاستخدامها أثناء الحاجة للتحقق من أن تسجيل الدخول يتم من قبل صاحب الحساب عند محاولة الدخول من جهاز جديد غير معروف.
- يتميز هذا التطبيق بمستوى أعلى من الأمان مقارنة بخاصية الرسائل النصية، فهو بعيد عن وصول الحكومات، أو مشغلي الهاتف المحمول، أو أي جهة أخرى قادرة على اعتراض الرسائل النصية، كما يمكن الاستفادة منه حتى أثناء عدم توفر الاتصال بالإنترنت.

- تدعم عدد كبير من الشركات خاصية استخدام التحقق عبر أداة إنشاء رموز، ومن بينها شركتي جوجل ومايكروسوفت بكافة خدماتهما، إضافة إلى العديد من وسائل التواصل الاجتماعي.

رموز الاسترداد:

قد يتعذر الوصول لوسائل الأمان السابقة كونها مرتبطة بجهاز الهاتف، أما في حال فقدان الهاتف لأي سبب من الأسباب، فيمكننا الاعتماد على رموز الاسترداد.
وهي عبارة عن عشرة رموز يمكن الحصول عليها من إعدادات أمان الحساب، ليتم نسخها أو طباعتها وحفظها في مكان آمن، ويمكن استخدام هذه الرموز في حال فقدان الهاتف لمرة واحدة فقط بهدف الوصول للحساب، وعندها يمكننا الحصول على رموز جديدة لحالات الطوارئ المشابهة لاحقًا.

وسائل أمان إضافية خاصة ببعض الشركات:

تُقدّم بعض الشركات وسائل أمان إضافية مختلفة، على سبيل المثال تقدم شركة "فيس بوك" ميزة اختيار جهات اتصال موثوقة، بحيث يمكن اختيار من ثلاثة إلى خمسة أشخاص نثق بهم، وعند تعذر الوصول إلى الحساب، يتمكن صاحبه من استعادته بمساعدة الحسابات الموثوقة، إذ ترسل الشركة رمز لكل شخص مختلف عن الآخر، وبتجميع هذه الرموز سيحصل صاحب الحساب على الرمز الكامل للوصول لحسابه من جديد.

> "تفقدوا إعدادات الأمان لكل حساب تستخدمونه، وتأكدوا من أنكم قد فعّلتم على الأقل وسيلتي أمان إضافيتين، فمن شأن ذلك أن يعزّز من أمان حساباتكم"

الفصل الثامن: عمل الإنترنت ومزود الخدمة

يتزايد مستخدموا الإنترنت يومًا بعد يوم مع دخول هذه التكنولوجيا تفاصيل حياتهم اليومية وعملهم إلى درجة صعوبة تخيلهم العيش بدونها، وإلى جانب سهولة استخدام شبكة الإنترنت يُطلق أصحاب الاختصاص أجهزة جديدة تُسهّل الاندماج مع الإنترنت تتطور ميزاتها بسرعة فائقة. ولكن تبقى ماهية هذه الشبكة وطريقة عملها شيء مبهم بالنسبة للكثيرين مما قد يضعهم في مهبّ مخاطر عديدة تفرضها قوانين هذا العالم الخفي.
من القارات إلى المحيطات وحتى الفضاء يمتد عمل شبكة الإنترنت، فما هي آلية عملها؟

أ. البنية التحتية:

تتكون شبكة الإنترنت من مجموعة من الأجهزة التي تدعمها كالراوتر والمخدّم وأبراج الهواتف الخلوية والأقمار الاصطناعية وأجهزة الراديو والهواتف الذكية. بالإضافة لخطوط النقل التي قد تكون ألياف ضوئية وأسلاك تحمل البيانات إلى حواسيبنا، أو إشارات لاسلكية من الأقمار الاصطناعية أو أبراج الجيل الرابع. ولكي تكتمل العملية تحتاج الشبكة لعنصر البروتوكول وهو عبارة عن مجموعة موحدة من القوانين تتبعها جميع الأجهزة الموصولة بالإنترنت توفر لها الطريقة واللغة المشتركة لنقل البيانات بين بعضها البعض.

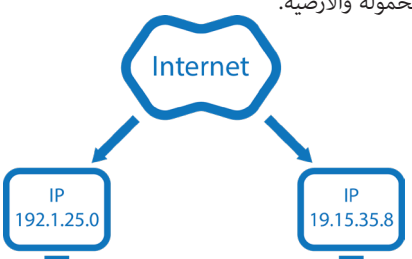
- يستجيب نظام الإنترنت بطريقة مرنة مع كل تغيير يحصل حول العالم كإنضمام أجهزة أو مغادرتها.
- إن تقديم خدمة الإنترنت يتجاوز قدرات أي مزود خدمة إنترنت واحد في أي مكان في العالم.
- تعمل الألياف الضوئية على نقل كم هائل من البيانات ولتقوم بهذه العملية يلزمها طاقة.
- يوجد كابلات احتياطية في البحر لضمان استمرار تدفق المعلومات في حال تعرض أي كابل لمشكلة ما.
- الكابلات وموصلات الطاقة الخاصة بها معدة بشكل يضمن عدم الحاجة لصيانتها لمدة 25 عاماً.

ب. مزود خدمة الإنترنت ISP (Internet Servise Provider):

يتمثل بالشركات التي تكون صلة الوصل بين مستخدمي الإنترنت والشبكة العالمية.

تقدم هذه الشركات خدمة الاتصال بالإنترنت بالإضافة لخدمات أخرى متعلقة بها مثل خدمات البريد الإلكتروني واستضافة المواقع والتخزين السحابي وتسجيل أسماء النطاق وغيرها..

وهي عادة ما تكون شركات ربحية خاصة مختصة بتقديم خدمات الاتصالات بشكل عام بما في ذلك للهواتف المحمولة والأرضية.



ج. كيف يراقبنا مزود خدمة الإنترنت؟

يمر عبر مزود خدمة الإنترنت كل ما نتبادله من طلبات وبيانات مع شبكة الإنترنت من صفحات وعناوين، مما يمكّنه ببساطة من قراءة كافة البيانات التي نرسلها ونستقبلها، وبالتالي تتبعنا ومراقبتنا، والاحتفاظ بسجلات تصفُّح كل مستخدم وتحليلها بهدف استنباط معلومات عنه قد تتعلق باهتماماته وعاداته وغيرها..وذلك إلى جانب قدرته على منع المستخدم من الوصول إلى صفحة أو خدمة ما على الإنترنت.

تحجب مزودات خدمة الإنترنت في معظم الدول الديكتاتورية مواقع ذات طبيعة سياسية أو توعوية.كما أنها لا تحترم خصوصية المستخدمين وتمنع عنهم كل ما يمكّنهم من التواصل وتبادل وجهات النظر بعيدًا عن رقابة الأجهزة الأمنية.

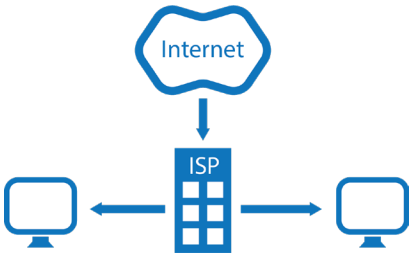
د. عناوين الإنترنت الـ IP (Internet Protocol):

نظراً لأن الإنترنت هي شبكة عالمية من أجهزة الكمبيوتر يتعيّن أن يكون لكل جهاز متصل بالإنترنت عنوان فريد يميزه عن غيره من الأجهزة، مهمته تحديد عنوان الجهاز

ليتمكن من التواصل مع الأجهزة الأخرى في هذه الشبكة الواسعة، إذ يتم إجراء الاتصالات من خلاله واستقبالها عليه.

وتعتمد عناوين الإنترنت نفس مبدأ رقم الهاتف:
رمز البلد، رمز المدينة، رمز المنطقة، الرقم الشخصي
وتأخذ شكل: nnn.nnn.nnn.nnn
حيث يجب أن يكون nnn رقم من 0 إلى 552
مثال: 0.0.0.271

- إذا قمت بالاتصال بالإنترنت من خلال مزود خدمة الإنترنت (ISP) فعادة ما يتم تعيين عنوان IP مؤقت لمدة جلسة الاتصال الخاصة بك.
- إذا قمت بالاتصال بالإنترنت من شبكة اتصال محلية (LAN) فقد يكون لجهاز الكمبيوتر الخاص بك عنوان IP دائم أو قد يحصل على عنوان مؤقت من خادم (DHCP) بروتوكول التكوين الديناميكي للمضيف.



هـ. خادم اسم النطاق DNS:

نظرًا لأنه يتعذّر على مستخدم شبكة الإنترنت حفظ رقم الـ IP لكل موقع يريد زيارته، تمّ رفد الشبكة بمترجم (DNS) يعمل على تحويل هذه الأرقام إلى عناوين (أحرف)، وهو يوفّر بذلك طريقة سهلة للتعامل مع عناوين الإنترنت والاتصال بها.
مثال: عندما نريد الدخول إلى موقع "غوغل" نكتب: google.comوعندها يعرف خادم DNS أننا نقصد 401.531.58.902 فيحولنا إليه.

وعندما نريد الدخول إلى موقع "ويكيبيديا" نكتب: wikipedia.org فيحولنا إلى عنوان الموقع 602.131.241.702.
وعند كتابة أرقام الـ IP السابقة عوضًا عن أسماء المواقع سنحصل على النتائج نفسها.

- يعتمد خادم DNS في عمله على تخزين المعلومات المتعلقة بأسماء النطاقات الموجودة في قاعدة بيانات شبكة الإنترنت، وربط هذه البيانات والعناوين بأسماء النطاقات المرتبطة.
- لا يحتوي خادم DNS على قاعدة البيانات بالكامل بل على مجموعة فرعية فيها، وعندما يرسل المستخدم طلبًا من أجل الحصول على المعلومات ولا تتوفر ضمن خادم SND يقوم الخادم بإعادة توجيه الطلب إلى خادم SND آخر لتنفيذه.

و. الشبكات العامة:

1. تعريف الشبكات:

هي ربط جهازين أو أكثر مع بعضهم البعض بهدف تبادل المعلومات. تحتاج الشبكات للقيام بمهمتها إلى ثلاثة مكونات هي: وحدة الإرسال، وحدة الاستقبال، وسط الاتصال الذي قد يكون خط هاتفي أو كابل اتصال من نوع معين أو اتصال لاسلكي.

2. تعريف الشبكة العامة:

هي شبكة يمكن لأي شخص الاتصال بها.
أفضل مثال على الشبكات العامة وأوسعها هي شبكة الإنترنت والتي تعتبر أكبر شبكة على الأرض.
ومن الأمثلة البسيطة والمنتشرة بكثرة هي الشبكات المفتوحة للاستخدام العام في المقاهي والمطارات والحدائق.

3. تعريف الشبكة الخاصة:

هي أي شبكة يتم تقييد الوصول إليها لاعتبارات معينة، مثل الشبكات في المنازل أو الشركات.

عند الاتصال بالإنترنت عبر شبكة WIFI عامة وفي حال عدم وجود أي كلمة مرور من المهم الانتباه، لأن ذلك يعني أن الشبكة غير مشفرة نهائيًا وغير آمنة، ومن الأفضل استخدام اتصال مشفر للضرورة والذي توفره خدمة VPN التي ستؤمن تشفير كل النشاطات عبر الإنترنت وبالتالي منع أي شخص من الاطلاع على بياناتكم.
أما عند استخدام كلمة مرور فمن المهم الانتباه لأن تكون نوعية التشفير آمنة، إذ أن بعض أنواع التشفير القديمة مثل WEP لم تعد آمنة ويمكن اختراقها، ومن الأفضل أن يكون نوع التشفير WPA2.

- قد يتمكن القائمون على الشبكات العامة أو المخترقون من مراقبة جميع المعلومات غير المشفرة التي يتم تبادلها عبر الإنترنت بما في ذلك الرسائل الإلكترونية، فضلًا عن أن بعض الحكومات التي لا تحترم الخصوصية تعمد إلى مراقبة النقاط العمومية التي تؤمن الإنترنت.
- تظهر مشاكل أمنية أخرى عند استخدام الحواسيب العامة المتاحة في مقاهي الإنترنت، والتي قد تحتوي على برمجيات خبيثة منصّبة مسبقًا كالبرامج التي تعمل على تسجيل ضربات المفاتيح والتي بإمكانها مراقبة كلمات السر التي سيتم إدخالها، أو تلك التي تقوم بأخذ لقطات للشاشة تلقائيًا، أو برامج مراقبة حركة تبادل المعلومات عبر الإنترنت. وفي هذه الحالات يكون الاحتراز الذي يجب اتخاذه هو استخدام حاسوبكم الخاص أو حاسوب شخص تثقون به، فلا شيء يمكنه أن يحميكم من هذه البرامج.

الفصل التاسع: التشفير:

يدخل التشفير ضمن إطار علم التعمية، ويُطلق على عملية تحويل المعلومات من شكلها المقروء أو الواضح إلى شكل لا يمكن معه قراءتها أو معاينتها إلا للمُصرّح لهم بذلك.
عُرف علم التشفير منذ القدم حيث استُخدم في المجالين الحربي والعسكري، ويذكر التاريخ أنّ الفراعنة هم أوّل من قام بعملية تشفير للتراسل بين قطاعات الجيش وذلك في عام 2000 قبل الميلاد، كما استخدمه الصينيون لنقل

الرسائل أثناء الحروب، وكذلك كان للعرب محاولات في هذا المجال، أما الرومان فقد كانوا أفضل من استخدمه قديمًا وعُرف تشفير الرسائل الموجهة لقادة الحرب آنذاك بإسم "تشفير قيصر" نسبةً إلى الإمبراطور الروماني يوليوس قيصر.

إذًا فلتشفير المعلومات قيمة جوهرية في الحفاظ على الأمن الرقمي للمستخدمين وحماية سرية معلوماتهم وخصوصيتها، إذ أنه يتيح إخفاء محتوى الرسائل المتبادلة بين شخصين عن أي شخص ثالث قد يعترضها، كما أنه في حال وقوع الملفات المشفّرة بالخطأ في أيدي أشخاص غير مصرّح لهم قراءتها فسيبقى محتوى الرسائل غير مقروء بالنسبة لهم.

يُقابل علم التشفير علم آخر قائم بحد ذاته يعمل على كسر التشفير وخرق الاتصالات الآمنة، يستخدمه معترضو البيانات المشفّرة للتعرّف على محتوى هذه البيانات.

هذا الأمر دفع مطورو البرامج إلى تحديث وسائل التشفير على نحوٍ مستدام ومتسارع لتوفير وسائل تشفير أكثر جودة، ما دفع أيضًا القائمون على كسر التشفير لرفع مستوى وسائلهم المتبعة.

كل ذلك أدّى إلى خلق حالة من المطاردة المستمرة بين هذين العلمين، في محاولة من كل طرف التفوق على الطرف الآخر.

قد يكون التشفير قويًا أو ضعيفًا، وتُقاس قوة التشفير بمدى صعوبة كشفه مع الوقت، وتوفر الأدوات اللازمة لذلك من عدمها

أ. أنواع التشفير:

1ـ التشفير المتماثل Cryptography Symmetric:

يُطلق عليه أيضًا التشفير التقليدي، يتم من خلاله استخدام نفس المفتاح للتشفير وفك التشفير، لذلك يكون من المهم اعتماد طريقة آمنة لنقل المفتاح بين المرسل والمستلم، إذ يمكن للشخص الذي يملك المفتاح فك التشفير وقراءة محتوى الملفات أو الرسائل.

2ـ التشفير الغير المتماثل Cryptography Asymmetric:

يُطلق عليه أيضًا تشفير المفتاح العام، وهو يعتمد على مبدأ زوج المفاتيح، أي يتم استخدام مفتاحين مختلفين في عمليتي التشفير وفك التشفير.

يُعرف المفتاح الأول بالمفتاح العمومي وهو يستخدم لتشفير الرسائل، أما الآخر فيُعرف بالمفتاح الخاص ويُستخدم لفك تشفير الرسائل.

في هذه العملية يتم إرسال المفتاح العام لجميع المستخدمين، أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد.

ب. الاتصال المشفّر Encrypted connection:

- يوفّر تشفير البيانات أثناء نقلها من جهاز إلى آخر عبر الإنترنت أو الاتصال اللاسلكي حماية فعّالة من اعتراض الاتصال من قبل طرف ثالث.
- يُعتبر من الممارسات الجيدة أيضًا استخدام الاتصال المشفّر عند إرسال أي بيانات عبر شبكة اتصال لاسلكية مثل WIFI، أو عندما تمر البيانات عبر شبكة غير موثوق بها.
- يمكننا نقل بيانات مشفّرة عبر اتصال غير آمن نع بقاء بياناتنا آمنة، على سبيل المثال: إرسال مرفق مشفّر ضمن رسالة بريد إلكتروني.
- إن استخدام طرق الاتصال الآمنة مثل تأمين طبقة النقل TLS أو شبكة خاصة ظاهرية VPN سيضمن عدم فهم محتوى الاتصال في حال تمّ اعتراضه، وذلك شريطة أن يتم تنفيذ الطريقة بشكل صحيح.
- من المهم التذكير أنه بدون استخدام تقنية تشفير للبيانات نفسها في مكان التخزين، من الممكن نقلها عبر اتصال مشفّر بشكل آمن، وهنا سيتم تشفير البيانات أثناء النقل فقط، وسيتم تخزينها لدى المستلم بنفس الشكل السابق كما كانت قبل الإرسال أي بدون تشفير.

ج. الشبكة الخاصة الافتراضية VPN:

وهي خدمة تؤمّن تشفير تنقلات المستخدمين عبر الإنترنت وحماية هويتهم الإلكترونية، وذلك من خلال إنشاء نفق وهمي بين جهاز المستخدم ومزود خدمة الشبكة، تتم من خلاله جميع الاتصالات الخاصة بالمستخدم، مما يعني عدم القدرة على فهمها من قبل أي طرف ثالث يحاول اعتراضها، وهو ما يجعل قراءة هذه المعلومات المشفّرة أمرًا مستحيلًا.

توفّر هذه الخدمة:

- اتصال آمن بالإنترنت: خاصة في حال استخدام شبكة WIFI عمومية.
- خصوصية كاملة عبر الإنترنت: بحيث تضمن أن تكون البيانات مشفّرة وعنوان بروتوكول الإنترنت (IP) محمي.
- مشاهدة المحتوى بطريقة آمنة: يجعل استخدام الشبكة عنوان بروتوكول الإنترنت الخاص بالمستخدم يبدو وكأنه موجود فعليًا في مكان آخر مما يساعده على الدخول إلى مواقع الويب المحظورة ويحافظ على بقاء بياناته الخاصة آمنة في الوقت نفسه.

يوجد العديد من الحالات التي يكون فيها استخدام شبكة خاصة افتراضية ضرورة وأمرًا جديًا:

استخدام شبكة WIFI عمومية:
تؤمن الخدمة ضمان تصفح آمن للإنترنت بدون الخوف من سرقة كلمات المرور أو الملفات أو الصور الخاصة، وذلك في الوقت الذي يكون فيه استخدام الشبكات العمومية محفوفًا بالمخاطر.

في حالات السفر:
تكون بعض المواقع محجوبة في بعض البلدان بفعل حكوماتها، على سبيل المثال: تحجب الحكومة في الصين بعض المواقع من ضمنها موقع فيس بوك، توفر هذه الخدمة الدخول الآمن لكافة المواقع المحجوبة، وذلك بتغيير عنوان بروتوكول الإنترنت الخاص بالمستخدم ليبدو وكأنه يتصفح الإنترنت من مكان مختلف.

تفادي المراقبة الحكومية:
يمنح استخدام شبكة خاصة افتراضية موثوقة ولا تحتفظ

بالسجلات درجة عالية من الخصوصية، كونها تحمي من التعقّب، ومن سطوة المراقبة الحكومية.

الرغبة في حماية الرسائل الحساسة:
والتي قد يضطر إلى إرسالها الصحفيون والباحثون والنشطاء السياسيون، خاصة في البلدان التي لا توفر حرية الرأي والتعبير.

د. أنماط تشفير البيانات:

برنامج VeraCrypt:

هو برنامج مجاني مفتوح المصدر، يسمح لك بتعمية ملفاتك، وهو نُسخة مُحدّثة من مشروع تروكربت المتوقف. يتوفر ڤيراكربت لأنظمة مايكروسوفت ويندوز، ماك، أو لينكس. كما يُعالج الثغرات الأمنية المُكتشفة في تروكربت.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي:

https://www.veracrypt.fr/en/Downloads.html

بداية يجب عليك أن تعلم أنه باستخدامك لـ فيراكربت ستتمكن من إنشاء نوعين من المجلدات المعمية:

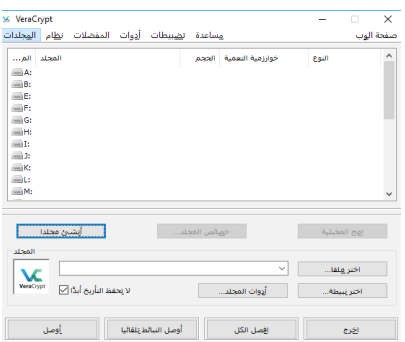
1. المجلدات العادية: تتطلب كلمة مرور واحدة.
2. المجلدات المخفية: تحتوي مجلدين أحدهما ظاهري وآخر مخفي وبالتالي تتطلب كلمتي مرور.

من الممكن استخدام المجلدات المخفية لفتح مجلد مموّه تحتفظ فيه بملفات خاصة لكن ميزة المجلدات المخفية تمكنك من اتباع استراتيجية للكشف عن المجلد الظاهري في حال اضطررت لذلك تحت الضغط، مما يبقي على القسم المخفي آمن وبذلك يمكن الاحتفاظ بالملفات الحساسة داخل المجلد المخفي فيما يتم حفظ بيانات عادية ضمن القسم الظاهري.

1. المجلدات العادية:

عند فتح البرنامج ستظهر لك الواجهة الرئيسية للبرنامج، حينها اضغط على (أنشئ مجلدًا) للبدء بالعملية. بعدها قم باختيار نوع المجلد الذي تريد إنشاءه.

اختر اسم وموقع المجلد الذي ترغب بإنشائه، ستظهر لك نافذة خيارات التعمية، والتي يمكنك من خلالها تحديد خوارزمية التعمية التي تريدها، مع العلم بأن الخيارات المسبقة في البرنامج هي الأفضل ولا حاجة للتعديل عليها.

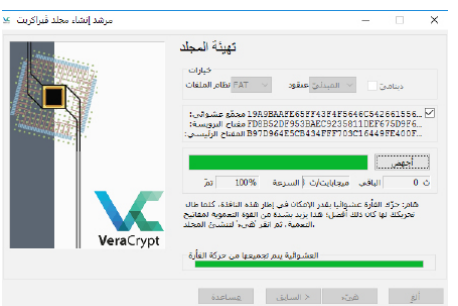


قم باختيار حجم المجلد المُعمى الذي ترغب بإنشائه معتمداً على الحجم المتوقع للملفات التي تود تعميتها.

اختر كلمة مرور للمجلد في الخانة الأولى وأعد كتابتها بشكل متطابق في الخانة الثانية.

يفضل هنا الاستعانة باحد برامج إدارة كلمات المرور لإنشاء كلمة مرور قوية.

الخطوة التالية هي اختيار نوع نظام الملفات، الخيارات المعدة مسبقاً من البرنامج مناسبة، خاصة أن نظام FAT مناسب لجميع الحالات وأنظمة التشغيل

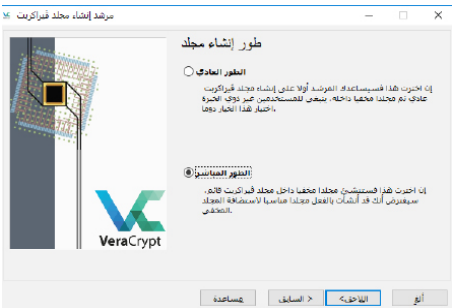


يجب تحريك مؤشر الفأرة لتوليد رموز المجمع العشوائي إلى أن يتم ملئ الشريط بالكامل باللون الأخضر مما يزيد من قوة التعمية.
بعد انتهاء عملية التهيئة ستظهر لك نافذة تُعلمك بأنه تم إنشاء المجلد بنجاح، بعدها ستتمكن من الخروج أو إنشاء مجلد آخر

2ـ المجلدات المخفية:

سيتم اتّباع نفس الخطوات الأولية لإنشاء الملف العادي إلى أن نصل إلى اختيار نوع المجلد حيث سنختار الآن مجلد مخفي.
عند اختيارنا لمجلد مخفي، ستظهر سنجد أن هناك طريقتين لإنشاء مجلد مخفي:

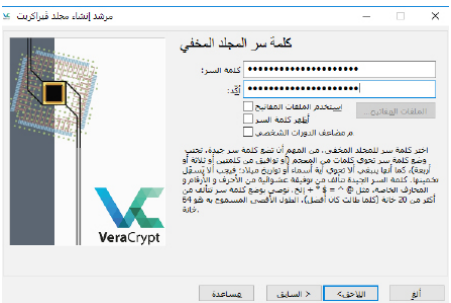
- الطور العادي: وهو عملية إنشاء مجلد عادي ومجلد مخفي جديد غير موجود مسبقًا.
- الطور المُباشر: وهو عملية إنشاء مجلد مخفي لمجلد عادي موجود مسبقاً.



عملية الإنشاء تعتمد على نفس الخطوات الأولية وهي اختيار اسم ومكان المجلد، بعدها ستظهر لك نافذة تطلب منك إدخال كلمة مرور مجلد فيراكربت العادي/ الخارجي الموجود الذي أنشأته مسبقًا.

ستبدأ بعدها بالتحضير لعملية إضافة المجلد المخفي إليه وتحديد خيارات تعمية المجلد وحجمه كما في عملية إنشاء مجلد فيراكريبت عادي، إلى أن تصل إلى عملية

وضع كلمة المرور لمجلد فيراكريبت المخفي على أن تكون مختلفة عن التي اخترتها للمجلد العادي، ولاتنسَ استخدام برنامج إدارة كلمات المرور.



بعد إدخال كلمة المرور ستكون الخطوة الآن عملية تهيئة مجلد فيراكربت المخفي، بعدها سيعرض البرنامج رسالة تُعلمك بانتهاء عملية إنشاء المجلد.

يمكنك الآن تخزين ملفاتك في المجلد المخفي ولن تكون ظاهرة حتى لمن يملك كلمة مرور المجلد العادي.

ولفتح مجلد معمى تم إنشاؤه من خلال فيراكريبت قم بفتح النافذة الرئيسية للبرنامج ثم اختر أي حرف محرك أقراص من الأقراص الظاهرة لديك، ثم اضغط على (اختيار ملف) لتحديد الملف المعمي الذي تود فتحه، ثم اضغط على (أوصل).

بعدها قم بإدخال كلمة مرور لمجلد فيرا كريبت العادي أو المخفي ثم الضغط على زر (موافق)

بعد إدخال كلمة المرور سيقوم فيراكربت بتوصيل المجلد المعمى كقرص تخزين على الجهاز

يمكنك الآن الدخول إلى المجلد المعمي من خلال الضغط مرتين على حرف القرص الذي سبق واخترته لمجلدك لتقوم بإضافة الملفات التي تود تعميتها أو التعديل على الملفات المخزنة سابقاً

بعد الانتهاء من عملك قم بفصل مجلد فيراكربت حتى لا يتمكن أي أحد من استخدامه، من خلال اختيار حرف القرص من قائمة الأقراص الظاهرة في نافذة فيراكربت الرئيسيّة واضغط على زر (أفصل).

من الممكن أيضاً استخدام البرنامج لتعمية أقراص تخزين ثابتة أو قابلة للإزالة الخطوات مشابهة لما سبق في عملية انشاء مجلد عادي أو مخفي لكن في هذه الحالة يتم اختيار قرص كامل موصول بالجهاز، وقد تتطلب عملية تعمية القرص وقت بحسب حجم القرص.

ملاحظة: عند توصيل اقراص مشفرة باستخدام برنامج فيراكربت ستظهر كأنها اقراص معطوبة وقد يطلب منا نظام التشغيل تهيئتها مما قد يتسبب بفقدان كافة المعلومات المخزنة بداخله بشكل نهائي، إلا أن هذا الأمر يزيد من قوة الحماية لعدم الوصول للمعلومات المخزنة بداخله من أشخاص غير مصرح لهم.

تشفير الرسائل:

يعتبر تشفير الرسائل أمرًا في غاية الأهمية في الحالات التي يتم فيها نقل رسائل حساسة، قد يشكل تبادلها مصدرًا كبيرًا للخطر على ناقليها، خاصةً في الدول التي تقمع الحريات، الأمر الذي قد يكلّفهم حياتهم.

إنّ إرسال الرسائل الإلكترونية العادية أمر غير محمي، إذ يمكن الوصول إليها واختراقها وسرقة المعلومات التي تحتويها، سواء من قبل قراصنة الإنترنت، أو من قبل الشركة التي توفّر هذه الخدمة، أو قد تقوم بذلك الحكومات.

يوجد العديد من البرامج التي تعمل على تشفير رسائل البريد الإلكتروني، الأمر الذي يقي من مخاطر كشف مضمونها أو حتى معرفة صيغة مرفقاتها الحقيقية.

- يمكن أن يوفر البريد الإلكتروني المشفّر القدرة على تشفير جسم ومرفقات الرسائل الإلكترونية، وكمثال على ذلك تستخدم معايير OpenPGP و S-MIME على نطاق واسع طرق التشفير التي تمّ تنفيذها من قبل مجموعة من منتجات البرمجيات الحرة والتجارية.
- يستخدم البريد الإلكتروني المشفّر نوع تشفير غير متماثل، ويتطلّب من المستخدم إنشاء زوج مفاتيح قبل أن يتمكن من إرسال بريد إلكتروني مشفّر، ويجب على المستخدمين أيضًا تبادل المفاتيح العامة قبل إرسال بريد إلكتروني مشفّر بينهم، فيما يبقى المفتاح الخاص سرّيًا.
- يمكن أن يتسبب تكوين البريد الإلكتروني المشفّر داخل بيئة شركة في حدوث مشاكل، وذلك نظرًا لأن المحتوى والمرفقات ستكون مشفّرة وربّما يتمّ حظرها بشكل نشط بواسطة برنامج المسح.
- كما يمكن أن يكون هناك أيضًا مشكلات في التوافق مع أنظمة معالجة البريد الإلكتروني التلقائية، أو إدارة عدة مفاتيح خاصة بين العديد من الموظفين، على سبيل المثال ، صندوق بريد مشترك في support@example.com
- وقد يكون من الصعب أيضًا على بعض الأفراد تثبيت برامج متوافقة وإنشاء أزواج مفاتيح وتقدير ضرورة إدارة المفاتيح، فضلًا عن أنّ فقدان المفتاح الخاص قد يؤدي إلى عدم فك تشفير رسائل البريد الإلكتروني المستلمة التي تمّ تشفيرها باستخدام المفتاح العام المرتبط.
- من الضروري وجود سياسة تحكّم في البريد الإلكتروني المشفّر، لدى وحدات تحكّم البيانات في المؤسسة، بما في ذلك الإرشادات التي تُمكّن الموظفين من فهم متى يتوجّب عليهم استخدام الرسائل المشفّرة أو عدم استخدامها.على سبيل المثال: قد يتضمّن دليل المؤسسة إشارة إلى أنه يتوجّب عند إرسال أي بريد إلكتروني يحتوي على بيانات شخصية حساسة (إما في النص أو كمرفق) أن يكون مشفّرًا.
- من الممكن إرسال ملف مشفّر عبر البريد الإلكتروني ضمن المرفقات، إذ يتم تشفير الملف من خلال برنامج على جهاز المرسل ومن ثم تحميله كملف مرفق إلى البريد الإلكتروني.

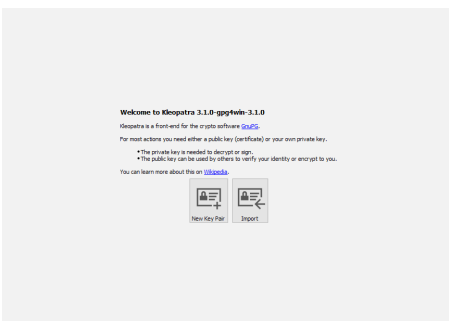
- لتحقيق الحد الأقصى من الضمانات التي يمكن تقديمها عن طريق استخدام المرفقات المشفرة، في حال استخدام التشفير المتماثل يجب توصيل المفتاح عبر قناة اتصال منفصلة، كأن يتمّ الكشف عن كلمة المرور عبر وسيلة اتصال آمنة مختلفة عن البريد المستخدم في إرسال المرفقات المشفرة.

برنامج kleopatra:

برنامج مجاني مفتوح المصدر يعتمد على أداة GpgPG الأساسية للتشفير وهو مخصص لأنظمة ويندوز، يمكن استخدام برامج مناسبة لأنظمة تشغيل مختلفة تعمل بنفس الأسلوب تماماً وجميعها تعتمد أداة GpgPG، وهو برنامج تشفير للملفات ورسائل البريد الإلكتروني.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي:
HTTPS://WWW.GPG4WIN.ORG/GET-GPG4WIN.HTML

بعد تحميل البرنامج قم بعملية التثبيت على جهازك، بعد التثبيت نفتح مدير الشهادات kleopatra ، عند فتح البرنامج للمرة الأولى ستظهر لك الواجهة الرئيسية للبرنامج
اضغط New Key Pair في حال أردت إنشاء زوج مفاتيح جديدة و Import في حال أردت استيراد مفتاح عام أو مفاتيحك الخاصة الموجود مسبقًا.



عند إنشاء زوج مفاتيح جديدة ستظهر لك الواجهة أدناه لإدخال اسم وبريد الإلكتروني (اختيارية وليست ضرورية ليعمل المفاتيح بشكل صحيح ويمكن فقط اختيار أي اسم والمتابعة).

بعدها ستظهر لك نافذة تطلب منك إنشاء كلمة مرور.
بعدها ستظهر لك الشاشة التي توضح انه تم إنشاء زوج المفاتيح بنجاح مع خيارات لإنشاء نسخة احتياطية و ارسال المفتاح العام عبر البريد الإلكتروني، بالإضافة لإمكانية رفع المفتاح العام لمستودع مفاتيح عامة متاح للجميع على الانترنت ولا ننصح برفع المفتاح العام قبل انشاء شهادة ابطال، بعد رفع المفتاح العام لا يمكن حذفه من المستودع على السيرفر ومن الممكن حينها استخدام شهادة الابطال.

تعتمد طريقة التشفير هذه على زوج مفاتيح، مفتاح عام ومفتاح خاص، ويجب على كلا الطرفين الراغبين في استخدام هذا النمط من التشفير للمراسلات معرفة كيفية استخدام هذه الطريقة.

- المفتاح العام: يمكننا ارساله لأي شخص يرغب في مراسلتنا بشكل آمن ومشفر، وبالتالي سيتمكن الاخرين من تشفير رسالة مخصصة لنا باستخدام المفتاح العام، ولا يمكن معرفة محتواها إلا من صاحب المفتاح العام الذي يملك المفتاح الخاص لفك التشفير.
- المفتاح الخاص: هو المفتاح الشخصي لفك تشفير الرسائل التي تم إعدادها باستخدام المفتاح العام، يجب الاحتفاظ به بشكل آمن وعدم تبادله مع أي طرف آخر.

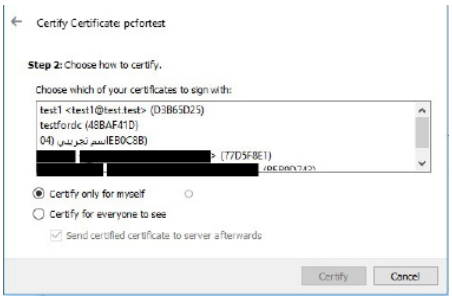
بعد إنشاء زوج المفاتيح يمكننا تصدير المفتاح العام وارساله ليتمكن الطرف الثاني من إنشاء رسالة مشفرة باستخدام المفتاح العام الخاص بنا.
حدد المفتاح الذي قمت بإنشاءه ثم اضغط على Export ثم حدد مكان حفظ الملف على جهاز الكومبيوتر، الآن يمكن ارسال الملف الذي قمنا بتصديره للطرف الثاني عبر البريد الإلكتروني أو بأي وسيلة ارسال مناسبة.

لإرسال رسالة مشفرة إلى طرف آخر يجب أن يكون لدينا المفتاح العام الخاص بالطرف الآخر، بعد الحصول على المفتاح العام نقوم بعملية الاستيراد من خلال الضغط على زر Import، ثم نحدد موقع المفتاح العام الذي نرغب في استيراده.

اثناء عملية الاستيراد من ملف بتنسيق SMC وهو التنسيق الأساسي أثناء التصدير ستظهر النافذة التالية:
يجب تحديد المفتاح وتحديد أنكم قمتم بالتأكد من رمز البصمة (هذا الرمز للتأكد من أن المفتاح الذي نقوم باستيراده هو فعلاً المفتاح الصحيح، ويمكن التحقق من ذلك من خلال التواصل المباشر مع صاحب المفتاح بأي وسيلة مناسبة والتأكد من أن الرمز متطابق مع المفتاح العام الذي ارسله لنا)

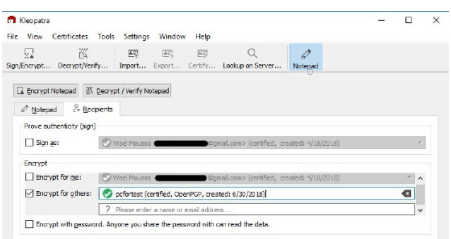
بعد المتابعة تظهر لنا نافذة تمكننا من اختيار المصادقة لنا فقط ويجب استخدام مفتاحنا الخاص للمصادقة وبعدها ادخال كلمة سر المفتاح الخاص بنا.

الخيار الثاني للمصادقة للجميع ومع هذا الخيار يتم ارسال المفتاح العام إلى مستودع المفاتيح على السيرفر مع معلومات انه مصادق من طرفنا.



لا يمكن تجاوز خيار المصادقة الا في حال استيراد المفتاح العام بصيغة نص TXT وعند استيراد المفتاح العام بهذه الطريقة لن يكون خيار المصادقة إلزامي.
الآن لإنشاء رسالة مشفرة، اضغط على زر Notepad لتظهر لك نافذة فيها مكان مخصص لكتابة الرسالة المطلوب تشفيرها.

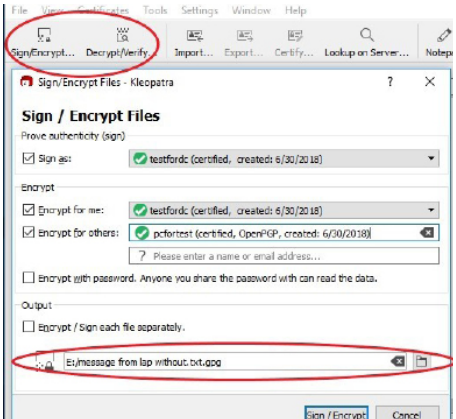
بعد الانتهاء من الكتابة يجب أن نحدد الأشخاص المستلمين من خلال الزر Recipients.
هنا يجب علينا تحديد المفتاح العام للشخص الذي نرغب في ارسال رسالة مشفرة له، كما يمكننا أن ندخل عدة مستلمين في وقت واحد، ويمكن تحديد توقيع الرسالة لمعرفة المرسل ويمكن تجاوز هذا الخيار، ويوجد أيضاً خيار تشفير الرسالة لي.
بعد تحديد المستلمين يمكن الآن الضغط على زر توقيع وتشفير الرسالة Sign / Encrypt Notepad



في حال قمنا بتحديد توقيع الرسالة او تشفيرها باستخدام المصادقة مع مفتاحنا الخاص سيطلب التأكيد بإدخال العبارة السرية، وفي حال لم نستخدم هذا الخيار سيتم تشفير الرسالة فوراً دون المصادقة.

الآن يمكن نسخ الرموز وإرسالها مباشرة عبر أي وسيلة الى الشخص المطلوب، في حال كنتم ستقومون بالإرسال عبر البريد الإلكتروني ننصح بنسخ الرموز إلى ملف TXT وارفاقه في الرسالة.

لفك تشفير رسالة يمكن الضغط على زر Notepad ولصق الرموز في مساحة الكتابة ثم الضغط على زر التشفير والتحقق Decrypt/Verfiy Notepad، في حال كانت الرسالة مشفرة باستخدام المفتاح العام الخاص بكم، سيطلب ادخال العبارة السرية ليظهر بعدها نص الرسالة ومعلومات حول التوقيع إن كانت الرسالة موقعة.



تشفير الملفات:

جميع الخطوات مشابهة لعملية تشفير الرسالة، الفرق هنا هو تحديد ملف وتشفيره أو فك تشفيره في حال كنت المستلم، وذلك عبر الضغط مباشرة على زر توقيع وتشفير في الأعلى ثم تحديد الملف المطلوب ثم تحديد مكان حفظ الملف بعد تشفيره او فك تشفيره.

يمكن الاستفادة من تشفير الملفات وارسالها بأي وسيلة مناسبة وفقاً لحجم الملف، ومن الممكن تشفير ملفات بأحجام كبيرة.

ملاحظة:

في حال كنتم بحاجة لتبادل المفتاح السري مع شخص تثقون به، فمن الضروري عدم ارسال المفتاح بنفس وسيلة ارسال الرسائل المشفرة بينكم، إذ يمكنك ارسال الرسالة على البريد الاكتروني والمفتاح على الواتساب على سبيل المثال.

الفصل العاشر: تخزين البيانات والنسخ الاحتياطي:

تعد وسائط التخزين من أهم مكونات الحاسوب فلا يمكنك الاحتفاظ بالبيانات على الجهاز إلا من خلالها.
تقسم وسائط التخزين إلى:

- داخلية: تكون مرتبطة في الجهاز واللوحة الأم، مثل: القرص الصلب.
- خارجية: تستخدم عند نقل البيانات من جهاز إلى آخر، مثل: الأقراص الليزرية أو USB. كما يمكن تصنيفها إلى:

1. جهاز تخزين أساسي، مثل ذاكرة الوصول العشوائي RAM.
2. جهاز تخزين ثانوي، مثل محرك الأقراص الثابتة، ويمكن أن يكون قابلًا للإزالة أوداخلي أو خارجي.

ونتج عن التطور التكنولوجي المتسارع في عالم الحاسوب، ظهور وسائط تخزين بسرعات عالية وسعات تخزين هائلة. وتأتي كثرة أنواع وسائط التخزين بسبب التطور والحاجة لإيجاد الأفضل والأسرع والأقل تكلفة مع مساحات تخزين أكبر.
ولكن تبقى وسائط التخزين على اختلاف أنواعها ومواصفاتها وطريقة عملها معرّضة للتلف.

إنّ استخدام أكثر من **70%** من مساحة التخزين على أي نوع من أنواع وسائط التخزين يتسبب في ضعف الأداء ويعرّض أداة التخزين للتلف

أ. التخزين السحابي Cloud Storage:

وهي طريقة لتخزين البيانات تُتيح الاحتفاظ بها على الإنترنت بدل تخزينها على وسائط محلية.

مزايا التخزين السحابي:

- يمكن الوصول إلى البيانات من أي جهاز حاسوب متصل بشبكة الإنترنت، ومن أي مكان، ومن أجهزة متعددة في الوقت نفسه.
- سهولة مشاركة الملفات مع أشخاص محدّدين أو إتاحة البيانات للعامّة.
- تخزين الملفات على شبكة الإنترنت يعني أنّ نسخة منها ستكون محفوظة في حال تعرّض جهاز الحاسوب لأي عطل طارئ.
- تستخدم أنظمة التخزين السحابي استراتيجية لحفظ البيانات في أماكن مختلفة مما يجعلها متاحة وآمنة في حال وقوع كوارث.

عيوب التخزين السحابي:

- يُشكل استخدام التخزين السحابي نقطة ضعف من ناحية الأمن الرقمي نتيجة لوجود الملفات بيد طرف آخر.
- قد تتعرّض البيانات للكشف في حال وجود أي خطأ من الشركة أو إذا تعرض حسابكم للاختراق، لذلك من الأفضل تشفير البيانات الحساسة قبل رفعها على التخزين السحابي، وتؤمّن أغلب الشركات العالمية اتصالًا مشفرًا أثناء تحميل ورفع البيانات.

في حزيران 2011 أسفر خطأ برمجي في مزود التخزين السحابي دروب بوكس Drop Box عن إتاحة جميع المحتويات المخزنة أمام الجميع وذلك لفترة من الزمن.

من الشركات الأكثر انتشارًا في تزويد خدمة التخزين السحابي هي دروب بوكس Dropbox ، غوغل درايف Google Drive، مايكروسوفت ون درايف rosoft One Drive-Mic، أبل آي كلاود Apple ICloud، و تيم درايف Team Drive.

توفر العديد من الشركات العالمية مساحات مجانية للمشتركين: (غوغل **15** جيغا، دروبوكس **2** جيغا، مايكروسوفت ون درايف **5** جيغا ...) مما أدى إلى انتشار التخزين السحابي على نحو واسع في السنوات الأخيرة.

ب. النسخ الاحتياطي Backups:

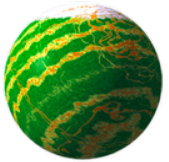
هي عملية إجراء نسخة من الملفات الرقمية المهمة "الشخصية أو ملفات العمل" بغرض حفظها من الضياع، وضمان سلامة المعلومات واستمرارية العمل.
فقد يتعرّض الحاسب الشخصي أو الهاتف المحمول للسرقة، أو لهجوم رقمي خبيث، كما قد تُحذف الملفات عن طريق الخطأ أو بشكل متعمّد من قبل أحد المخربين، فضلًا عن حالات التلف بسبب التعرض للحرائق أو الكوارث الطبيعية.

- تُعتبر عملية النسخ الاحتياطي هامة جدًا لكل من يمتلك ملفات قيمة، وتزداد الحاجة لاستخدامها في ظروف النزاعات والحروب خاصة للعاملين في مجال الصحافة وحقوق الإنسان وغيرها من المهن التي تكون عُرضة للاستهداف والاختراق..
- يمكن إجراء نسخة احتياطية لكلٍّ من: ملفات الفيديو ونظام التشغيل والمستندات والصور المخزّنة محليًا، رسائل البريد الإلكتروني، حسابات التواصل الاجتماعي، المواقع الإلكترونية.

وفقًا لإحصائية موقع "اليوم العالمي للنسخ الاحتياطي" فإن **30**٪ من الأشخاص لا يقومون بالنسخ الاحتياطي، ويضيع **113** هاتفًا جوالاً كل دقيقة، و **29**٪ من الكوارث التقنية سببها خطأ غير مقصود، و **1** من أصل **10** أجهزة كمبيوتر تصاب بالملفات الخبيثة شهريًا.

نقلًا عن موقع سلامتك

برنامج Cobian:



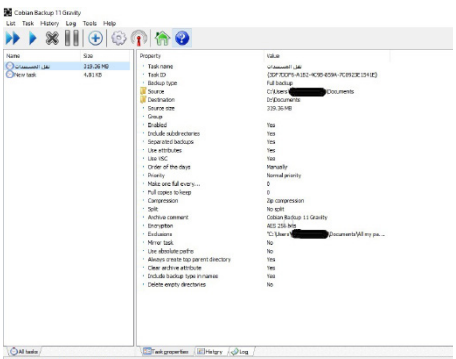
برنامج مجّاني مفتوح المصدر يعمل على جميع أنظمة ويندوز وماكنتوش، يُستخدم لجدولة عمليات النسخ الاحتياطي للملفات المحددة إلى مكان مخصص.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي:

HTTP://WWW.COBIANSOFT.COM/COBIANBACKUP.HTM

بعد تحميل البرنامج قم بعملية التثبيت على جهازك، عند فتح البرنامج يتم تشغيله دون ظهور الواجهة مباشرة، ستجدون ايقونة البرنامج مصغرة في شريط المهام.

عند الضغط على الأيقونة المصغرة تظهر واجهة البرنامج وتحتوي على قسمين، الأول قائمة بأسماء المهام المجدولة بعد انشائها والقسم الثاني يظهر فيه معلومات تفصيلية حول المهمة المحددة



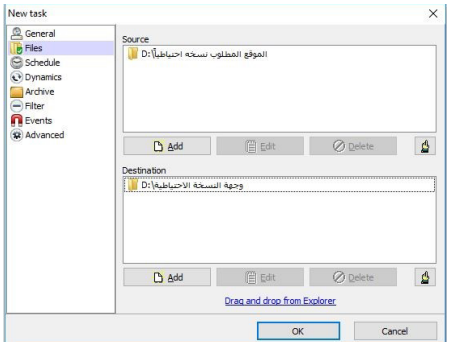
يمكن البرنامج من إدارة عملية النسخ الاحتياطي مع خيارات كثيرة مفيدة، حيث يمكننا انشاء عدة قوائم لتحتوي كل قائمة على مهام متعددة، لإنشاء مهمة جديدة من القائمة Task أو من خلال زر (+) الظاهر في القائمة، علينا اختيار نوع النسخ الاحتياطي المناسب للمهمة المطلوبة:

1. نسخ كامل Full

يقوم هذا الخيار بإنشاء نسخة كاملة في كل مرة يتم فيها تشغيل المهمة حتى للملفات التي لم يتم إجراء أي تغييرات عليها.

2. نسخ تزايدي Incremental

يقوم هذا الخيار عند تشغيله بعد النسخ الاحتياطي لأول مرة بفحص الملفات ونسخ الملفات الجديدة والتي تم التعديل عليها بعد آخر عملية نسخ احتياطي مما يوفر في الوقت والمساحة.



3. نسخ تفاضلي Diffierential

يقوم هذا الخيار بالعمل بشكل مشابه للنسخ التزايدي، لكنه يقوم بفحص الملفات في المصدر ويقارنها مع آخر عملية نسخ احتياطي بالإضافة للنسخة الاحتياطية الكاملة وفي حال اختلاف أي ملف عن الوجهة يقوم فقط بنسخ الملفات التي تم التعديل عليها.

4. Dummy

هذا الخيار لا يقوم بأي عملية نسخ احتياطي، وتم وضعه ليكون فقط بغرض إضافة جدولة مهام كتشغيل أو إيقاف خدمة أو برنامج أو إعادة تشغيل جهاز الكمبيوتر. القائمة في اليسار للتنقل بين الخيارات، Files لتحديد مصدر المعلومات المطلوب نسخها والوجهة، Sch-edule للجدولة الزمنية، Dynamics لتحديد الأولوية في المعالجة وعدد النسخ الاحتياطية بحسب نوعها، وبقية الخيارات إضافية قد تكون مفيدة للبعض لكنها غير إلزامية لإنشاء مهمة نسخ احتياطي.

الفصل الحادي عشر: استعادة وحذف البيانات:

أ. استعادة البيانات:

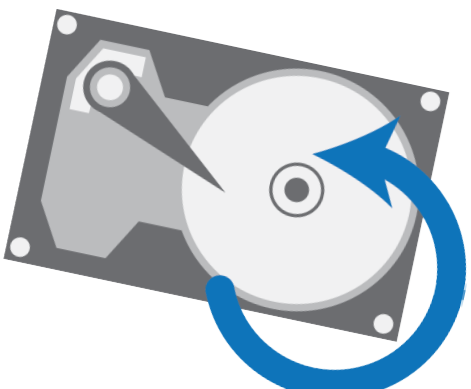
يعتقد كثيرون أنّ الملفات التي يتم حذفها من الحاسب الشخصي أو الهاتف الذكي لا يمكن الوصول إليها مجددًا، وبالتالي تمّت خسارتها إلى الأبد. لكن في الحقيقة قد نفقد بعض البيانات التي نحتاج إليها لأسباب متعددة، كأن نقوم بحذفها عن طريق الخطأ، ولكن حتى عند اختيار الحذف النهائي من جهاز الحاسب أو تفريغ سلة المحذوفات، فإن ذلك لا يعني أنه قد تم فقدان هذه البيانات بشكل كامل، فعملية الحذف التي تمت هي فقط عملية مسح سجل هذه البيانات من نظام التشغيل. لاستعادة البيانات يجب علينا استخدام برامج مخصصة تقوم بعملية فحص مساحة التخزين ثم سرد كافة البيانات الموجودة فيها والتي لم يعد لها سجلات في نظام التشغيل.

يعتبر تخزين بيانات الحاسب أمرًا معقدًا، ولكن يمكن تقسيمه إلى ثلاث عمليات أساسية:

أولًا: يتم تحويل البيانات إلى أرقام بسيطة يسهل على الحاسب تخزينها، أرقام ثنائية 0 و1.

ثانيًا: يتم تسجيل الأرقام بواسطة جهاز داخل الحاسب.

ثالثًا: يتم تنظيم الأرقام ضمن مساحة التخزين ونقلها إلى التخزين المؤقت لمعالجتها بواسطة البرامج.

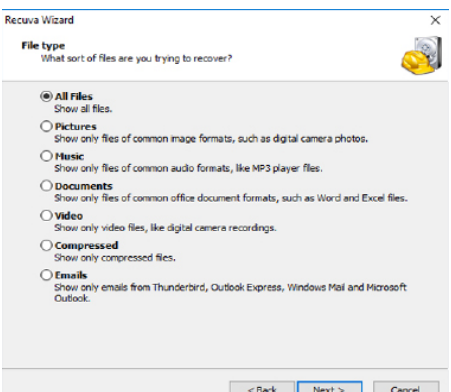


برنامج Recuva:

هو برنامج مجّاني مفتوح المصدر، يعمل على استرجاع الملفات المحذوفة من أي جهاز كمبيوتر، كما يمكن للبرنامج استعادة الملفات المحذوفة من USB ومشغلات MP3 وبطاقات الذاكرة.
يعمل البرنامج على أنظمة ويندوز XP وويندوز7 وويندوز فيستا.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي: HTTPS://WWW.CCLEANER.COM/RECUVA

بعد تحميل البرنامج قم بعملية التثبيت على جهازك، عند فتح البرنامج ستظهر لك الواجهة الرئيسية للبرنامج
بعد الضغط على زر Next ستظهر لك الشاشة أدناه والتي تطلب منك تحديد نوع الملفات التي تريد استعادتها بعدها ستختار مكان البحث أي تحديد المجلد أو القرص الذي تريد البحث فيه، يمكنك اختيار le Deep Scan- Enab من أجل البحث العميق مع العلم ان هذا الخيار قد يتطلب الكثير من الوقت.
عند الانتهاء من البحث قم بتحديد الملفات التي تريد استعادتها واضغط على زر Recover وقم باختيار المجلد الذي تود حفظ الملفات المستعادة فيه.



ب. حذف البيانات:

تشكّل عملية حذف البيانات بشكل نهائي أمرًا في غاية الأهمية على مستوى حماية الأشخاص وأمنهم الرقمي، فقد تتمكن أجهزة الأمن على سبيل المثال من استعادة ملف معيّن كان صاحبه يعتقد أنه قد حذفه نهائيًا. كما ذكرنا سابقًا فإنّ خطوات حذف الملف والتي تتمثل بالضغط على "Delete" وإفراغ سلة المحذوفات بعدها ليست كافية لإزالة الملف نهائيًا من الجهاز، فالملفات المحذوفة تبقى موجودة على القرص الصلب، ويمكن لأي شخص خبير استعادة جزء كبير من هذه الملفات بسهولة وسرعة.

إنّ ما يحصل فعليًا هو أن نظام التشغيل يقوم بحذف الإشارة إلى وجود الملف المحذوف على القرص، أي أنّ الملف سيبقى قابلًا للاستعادة حتى تتمّ الكتابة فوقه.

حتى نتمكّن من حذف ملف معيّن بشكل نهائي غير قابل للاستعادة يجب الاستعانة ببرامج خاصّة تعمل على حذف الملف غير المرئي الموجود على القرص الصلب.

تنبيه:

إن عملية الحذف النهائي بشكل ناجح تتم فقط على وسائل التخزين المغناطيسية ولا تنطبق على الفلاش ميموري أو DSS

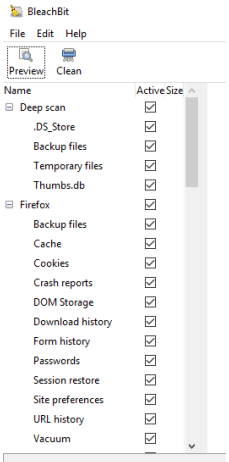
برنامج BleahBit:

برنامج مجّاني مفتوح المصدر، يهدف إلى إزالة الملفات الغير الضرورية من أنظمة تشغيل ويندوز، لنكس، ماك أو إس كالملفات المؤقتة وتاريخ التصفح على الويب وغيرها من مخلّفات تتركها البرامج على حاسوبكم بالإضافة إلى إزالة الملفات بشكل آمن ونهائي.

لتحميل البرنامج من الموقع الرسمي ادخل على الرابط التالي:

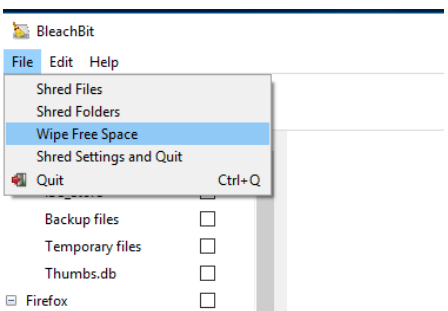
HTTPS://WWW.BLEACHBIT.ORG/DOWNLOAD

بعد تحميل البرنامج قم بعملية التثبيت على جهازك، عند فتح البرنامج للمرة الأولى ستظهر لك الواجهة الرئيسية للبرنامج. قم بإختيار الملفات التي تريد حذفها ثم اضغط على زر Clean المشار أليه في الصورة، بعدها ستبدأ عملية الحذف، تتطلب عملية الحذف بعض الوقت، وعند اختيار Deep scan (البحث العميق) قد تستمر العملية لساعات.



عند الانتهاء من الحذف، ستظهر لك واجهة تعلمك بانتهاء العملية والمساحة التي تمّ فحصها وعدد الملفات المحذوفة ونوعها.

كما يمكنك من خلال الضغط على File اختيار ملفات أو مجلدات محددة من أجل حذفها نهائيًا.
بعد انتهاء العملية سيتمّ حذف المجلد نهائيًا من حاسوبك ولن يستطيع أي أحد استعادته بعد الآن.
أما في حال أردت تنظيف وتعمية المساحة الخالية من الأقراص أو المجلدات فيمكنك استخدام تقنية Wipe Free Space كما هو موضح في الصورة أدناه.



الفصل الثاني عشر: الحماية من الفيروسات:

تُعتبر عملية مكافحة الفيروسات وحماية الحاسوب من البرمجيات الخبيثة وهجمات المخترقين، الخطوة الأهم لتأمين فعّالية وجدوى أي من الأساليب المستخدمة في حماية الخصوصية وزيادة الأمان الرقمي.

والفيروسات هي برمجيات تعمل على اختراق الحاسوب والانتشار داخله بسرعة هائلة، كما يمكنها عدوى الحواسيب الأخرى السليمة، وذلك دون معرفة أو إذن المستخدم، وهي قادرة على تغيير محتويات الملفات الإلكترونية وسرقتها وحتى حذفها نهائيًا، وسمّيت بهذا الاسم لتشابهها الكبير مع الفيروسات الحية التي تتطفّل على الإنسان.

تساعد برامج مكافحة الفيروسات في اكتشاف وإزالة البرمجيات الخبيثة، ووقاية الأجهزة من الإصابة بها.

ينبغي تحديث برنامج مكافحة الفيروسات بشكل دوري حتى يتمكّن من التصدي لأحدث الفيروسات المنتشرة عبر الإنترنت، إذ يقوم العاملون في مجال برمجيات مكافحة الفيروسات بتطوير برمجيات جديدة على الدوام وإجراء تحديثات على برمجيات موجودة، وذلك لمواجهة التحديات المتجددة التي يفرضها مطوروا البرمجيات الخبيثة، والذين يقومون بدورهم بالبحث الدائم عن طرق جديدة لاستغلال ثغرات ضمن أنظمة التشغيل أو خصائص ضمن المتصفحات بهدف الوصول إلى جهاز الضحية.

أ. عوارض الفيروسات والبرمجيات الخبيثة:

يوجد العديد من المؤشرات التي تدل على وجود فيروسات في جهاز الحاسب يمكن ملاحظتها من خلال تصرفّات غريبة تظهر أثناء استخدامه، يكون سببها في الغالب البرمجيات الخبيثة.

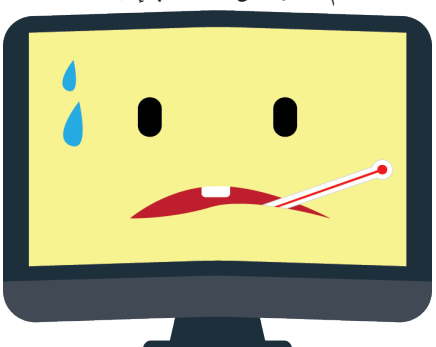
1: العوارض التي تؤثر على برامج الحماية المثبتة:

- يعطيكم البرنامج المضاد للفيروسات إنذارًا بوجود برمجيات قد تكون خبيثة.
- تعمل برمجيات خبيثة تظهر كأنّها برامج حماية بإظهار نوافذ منبثقة تدّعي أنّ جهازكم مصاب بفيروس.
- يتم تعطيل برنامج الحماية بشكل تلقائي ولا يمكنكم إعادة تشغيله.
- تظهر إنذارات متكررة لتثبيت برنامج لتنظيف جهازكم في حين أنّه يحاول تخطّي جدار الحماية.
- اختفاء برنامج الحماية من الجهاز بشكل تام.

2: العوارض التي تؤثر على الإنترنت:

يبدو أن متصفّح الإنترنت يتصرّف بشكل غير طبيعي:

- عدم تجاوب متصفح الإنترنت، أو إغلاقه بشكل تلقائي، أو عدم القدرة على إغلاقه.
- ظهور رسالة تُفيد بأنه لا يمكنكم تحميل الصفحة المطلوبة.
- تغيير الصفحة الرئيسية من المتصفّح بشكل تلقائي.
- يتم فتح صفحات لم تطلبوها.
- فتح العديد من النوافذ المنبثقة على متصفح الإنترنت.
- إضافة أشرطة أدوات بشكل تلقائي في أعلى المتصفّح.
- عدم القدرة على الاتصال بالإنترنت.



3: العوارض التي تؤثر على نظام التشغيل:

قد تُشبه هذه العوارض في بعض الأحيان تلك الناتجة عن عدم توافق بين الأجهزة والبرامج، أو أداء سيّئ لذاكرة الوصول العشوائية، وهي:

- عدم القدرة على فتح البرامج.
- توقّف نظام التشغيل عن العمل بشكل متكرر.
- ظهور برامج جديدة لم تقوموا بتثبيتها.
- اختفاء بعض الملفات أو ظهور تغييرات على بعضها الآخر، كأن يتغير شكل المجلد ليبدو على أنه اختصار للمجلد.
- بطء في الأداء، وتوقف عن الاستجابة لفترات معينة.
- إنذارات غير اعتيادية، كظهور رسالة خطأ تقول إن بعض الملفات ناقصة أو تالفة.
- استهلاك موارد الجهاز رغم عدم استخدام أي برنامج في حينها، كملاحظة انشغال القرص الصلب، أو استخدام الإنترنت في حين أنكم لا تقومون باستخدامه، مما يدل أن الفيروس يقوم بإرسال معلومات.

4: العوارض التي تؤثر على وسائل التواصل الاجتماعي والبريد الالكتروني:

- وصول رسائل بدون عنوان أو موضوع.
- وصول رسائل بريدية لعناوين البريد الإلكتروني المخزّنة لديكم على أنها رسالة مرسلة من بريدكم.
- يبدأ حساب التواصل الاجتماعي بإرسال رسائل للأصدقاء وينشر روابط وصور بشكل تلقائي.

5: عوارض أخرى لحالات تجسس أو عمليات خداع:

- يصلكم إتصال هاتفي يدّعي أنه من قسم الدعم لشركة ما مثل مايكروسوفت أو جوجل أو فيسبوك، علمًا أنّه من غير المرجّح أبداً أن تقوم مثل هذه الشركات بالتواصل مع

عملائها بهذه الطريقة لأي سبب كان.

- تشغيل ضوء الكاميرا رغم عدم استخدامها الأمر الذي يدل على وجود تجسّس.
- قد لا تظهر أيّ من العوارض السابقة على جهاز الحاسب رغم وجود برمجيات خبيثة، إذ بإمكانها التسلّل والاختباء دون إعطاء أي من هذه الإنذارات، حتى أنّ بعضًا منها يقوم بإزالة غيرها من البرمجيات الخبيثة لإخفاء هذه العوارض، لذلك لا يمكن الاستغناء عن برامج مكافحة الفيروسات، والتي تقوم بفحص دوريّ للجهاز من تلقاء نفسها.

ب. ماذا علينا فعله في حال مواجهة العوارض السابقة؟

قد يفشل برنامج مكافحة الفيروسات في بعض الأحيان بإكتشاف برنامج خبيث حديث العهد يكون قد أصاب جهازك، لعدم وصول هذا الفيروس إلى الشركة المطوّرة بعد.

في حالة إصابة جهاز الحاسب الخاص بك ببرنامج خبيث لأي سبب كان، أو في حالة الشك بالإصابة "بعد فتح ملف مشبوه على سبيل المثال"، قم بتنفيذ الخطوات التالية:

1. فصل الجهاز عن الإنترنت لتجنب إرسال أيّ معلومات.
2. إيقاف تشغيل الجهاز في حال عدم معرفتك بما يجب عليك فعله، لأن ذلك يساعد على إيقاف نشاط الفيروس على الحاسب.
3. فحص الجهاز باستخدام أداة حماية، بعد التأكد من الحصول على تحديثات لقاعدة بيانات أداة الحماية.
4. استعادة الحاسب لفترة سابقة باستخدام ميزة System Restore.
5. تغيير كلمات سر وسائل التواصل الاجتماعي والبريد الإلكتروني يساعد في ضمان عدم اختراق الحسابات.

ج. أنواع التهديدات:

تتعرّض نظم المعلومات والنظم الإلكترونية والحواسب وغيرها من الأجهزة لهجمات إلكترونية مفتعلة تسبب لها الضرر وتهدد بيانات المستخدمين، يمكن تصنيفها إلى:

- الفيروسات Viruses
- الديدان Woroms
- حصان طروادة Trojans
- برامج التجسس Spyware
- الخداع Phishing
- النكت / مزح / استخفاف Jokes

الفيروسات Viruses:

الفيروس هو برنامج خارجي يصيب الأجهزة بشكل متعمد، ويعمل على تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر، إما بالإزالة أو التعديل أو التخريب...وذلك بغرض إلحاق الضرر بالحاسب المستهدف أو السيطرة عليه أو سرقة بياناته.

الديدان Woroms:

يستخدم هذا النوع من البرامج الضارة موارد الشبكة للانتشار، وقد سُمّيت بالديدان بسبب ميزتها الغريبة في "للتسلل" من حاسب إلى آخر باستخدام الشبكة أوالبريد الإلكتروني أو أي قناة معلومات أخرى.

تكمن خطورة الديدان باستقلاليتها وعدم اعتمادها على برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع، وتُعتبر سرعة انتشار الديدان عالية جدًا، وهي أسرع من الفيروسات.

تتسلل الديدان إلى جهاز الحاسب، وتحسب عناوين الشبكة الخاصة بأجهزة الحواسب الأخرى وترسل إلى هذه العناوين نسخها، وبالإضافة إلى عناوين الشبكة يتم استخدام بيانات عناوين عملاء البريد أيضًا. علاوةً على ذلك يقوم مثل هذا النوع من البرامج الضارة في بعض الأحيان بإنشاء ملفات العمل على أقراص النظام.

الرسائل الإلكترونية المفخخة هي من أشهر وسائل انتشار الديدان، وعادةً ما تحمل هذه الرسائل عناوين جذابة "كدعوة لمشاهدة صورة أحد المشاهير"، لذلك يجب عدم فتح أي رسالة إلّا بعد التأكد تمامًا من أنها خالية من

الضرر حتى وإن كان مصدرها معروفًا، لأن بعض الديدان تعمل على إرسال نفسها من أي بريد لجميع الايميلات المضافة بدفتر العناوين.

أحصنة طروادة Trojans Horses :

هي برامج متخفية تنفّذ نشاطها على أجهزة الحواسب من دون علم أصحابها، أي أنّها قد تعمل بشكل تلقائي على حذف المعلومات من الأقراص، وتجميد النظام، وسرقة المعلومات الشخصية، أو كلمات السر التي يتم تغييرها واستخدامها كوسيلة للابتزاز..وهنا تكمن خطورتها.
هذا النوع من البرامج الضارة ليس فيروسًا في الفهم التقليدي (أي أنه لا يصيب البرامج أو البيانات الأخرى).
لا تستطيع أحصنة طروادة اختراق الحاسب بنفسها، وتنتشر على أنها برامج "مفيدة" و "ضرورية"، وما يزال الضرر الناجم عنها أعلى من هجوم الفيروسات التقليدي.
سُمّي البرنامج باسم "حصان طروادة" نسبةً للطريقة التي استخدمها اليونانيون في فتح مدينة طروادة (Troy)، والتي عجزوا عن اقتحامها بالطرق التقليدية، فقاموا ببناء مجسّم كبير جدًا على شكل حصان خشبي مُفرّغ من الداخل، ووضعوا بداخله جنود، وتركوه كهدية عند حصون المدينة وانسحبوا منها، فقام أهالي المدينة بإدخال المجسم معتبرينه رمز للانتصار على الأعداء، وعند منتصف الليل خرج الجنود من المجّسم وفتحوا أسوار المدينة للجيش اليوناني الذي قام بالدخول ومن ثم احتلال المدينة.

برامج التجسس Spyware:

هي البرامج التي تسمح بجمع البيانات عن مستخدم معين أو منظّمة معينة، ممن ليسوا على دراية بها، فقد لا تُخمّن حتى وجود برامج تجسس على جهاز الحاسب الخاص بك.
أمّا هدف برامج التجسس فيكون: تتبّع إجراءات المستخدم على الحاسب "مثل رصد مواقع الإنترنت التي يتصفحها"، وجمع معلومات حول محتويات القرص الصلب، وجودة الاتصال، وطريقة الاتصال، وسرعة المودم وما إلى ذلك.

لا يعدّ جمع المعلومات الوظيفة الرئيسية لهذه البرامج، بل إنها تهدّد الأمن أيضًا، ويمكنها تغيير إعدادات الحاسب والتحكّم فيه.

الخداع/التصيّد Phishing :

يتم هذا النوع من التهديد من خلال التواصل عن طريق البريد الإلكتروني أو أي وسيلة تواصل أخرى بهدف الحصول على معلومات مالية أو سرية مهّمة من المستخدم.

أي أنّ التصيّد هو شكل من أشكال الهندسة الاجتماعية، يتميّز بمحاولات للحصول على معلومات حسّاسة بشكل احتيالي، فهو يستهدف كلمات المرور أو تفاصيل بطاقة الائتمان أو غيرها من المعلومات الهامة، من خلال التزييف ومحاولة المهاجم للظهور كشخص جدير بالثقة.

على سبيل المثال يقوم المهاجم بتصميم صفحة خبيثة تشبه صفحة تسجيل الدخول لأحد المواقع الشهيرة "فيس بوك أو جيميل" لكنّها تحمل عنوانًا مختلفًا عن العنوان الأصلي، ثم يقوم المهاجم بتوجيه الضحية إلى الموقع الخبيث سواء عبر رسالة بريد إلكتروني أو رسالة فورية، تحتوي هذه الرسائل على رابط إلى الموقع الزائف حيث يُقترح على المستخدم إدخال رقم بطاقة الائتمان الخاصة به ومعلومات سرية أخرى.

للتحقّق من أنّ الموقع ليس خبيثًا يتوجّب:

1. معاينة شريط عنوان الموقع للتأكد من أنّه العنوان الصحيح للموقع الذي ترغبون تسجيل الدخول فيه.
2. التأكد من أنّ البروتوكول المستخدم في خانة عنوان الموقع هو بروتوكول Https.
3. وجود رمز القفل بجانب العنوان.

النكت/المزاح/استخفاف Jokes:

هي برامج لا تضر بجهاز الحاسب المستهدف بشكل مباشر ولكنها تعرض الرسائل التي ستتسبّب لاحقًا الضرر.

غالبًا ما يحذّر هذا البرنامج المستخدم من خطر غير موجود، كأن يعرض له رسائل حول تهيئة القرص الصلب

(على الرغم من عدم حدوث أي تهيئة)، أو رسائل عن اكتشاف فيروسات في الملفات (والتي تكون غير مصابة) وما إلى ذلك.
يوجد أنواع أخرى يمكن اعتبارها من التهديدات مثل: الدعايات والتي عادة ما تكون مرفقة ضمن البرامج المجانية، والبريد العشوائي.
بعض البرامج الضارة التي تكون مهمّتها توليد برامج ضارّة أخرى على الجهاز المصاب لأغراض مختلفة "مثل تنظيم هجمات منع الخدمة DDOS، التجسس على أجهزة أخرى،" عادةً ما تكون أداة للمخترقين أو لمنشئي الفيروسات.

د. استخدام أدوات الحماية:

1- يتوفر العديد من الأدوات للحماية، بعضها مجّاني وبعضها الآخر يكون مقابل اشتراك مادي.
2- تُعتبر تحديثات برامج الحماية هامّة جدًا إذ بدونها لا يمكن لبرامج الحماية التعرف على الفيروسات الحديثة.
3- يمكن استخدام أحد البرامج المجّانية التالية لفحص الأجهزة المصابة وإزالة الفيروسات:

- Microsoft Malware Remover
- BitDefender Free Edition
- Kaspersky Virus Removal Tool
- Malwarebytes

4- في بعض الحالات يكون من الأسهل والأضمن إعادة تهيئة الحاسب بشكل كامل، ويتوجّب قبل القيام بذلك التأكّد من نسخ البيانات الخاصة إلى جهاز تخزين خارجي، وبعد إتمام عملية تهيئة الحاسب يجب تثبيت أداة حماية وفحص جهاز التخزين الخارجي وذلك للتأكد من أنّ الفيروس لم ينتقل مع البيانات أثناء نقلها.
5- من الممكن فحص الروابط المجهولة قبل فتحها عبر موقع: HTTPS://WWW.VIRUSTOTAL.COM/AR

الفصل الثالث عشر: مواقع الإنترنت:

يُعتبر موقع الإنترنت مركزًا للعديد من الصفحات المختلفة والمرتبطة جميعها والتي يمكن الوصول إليها من خلال الصفحة الرئيسية.

تمّ إطلاق أوّل موقع إنترنت في عام 1991 ويمكننا زيارته والتعرّف عليه من خلال الرابط التالي:
http://nfio.cern.ch/

تعتمد مواقع الإنترنت على صفحات تحتوي لغات ترميز، وهي لغات حاسب تستخدم علامات لتحديد العناصر داخل المستند، وهي قابلة للقراءة من قبل الإنسان، أي أنّ ملفات الترميز تحتوي على كلمات قياسية، ومن أشهر لغات الترميز Markup Language Hypertext "HTML" لغة ترميز النصوص التشعبية.

تتعدّد أنواع مواقع الإنترنت، كما أنّه من الممكن أن يتضمّن موقع الإنترنت الواحد عدّة أنواع في نفس الوقت، فعلى سبيل المثال: يُصنّف موقع "تويتر" على أنّه موقع تواصل إجتماعي كما أنّه يُعتبر في نفس الوقت أحد مواقع التدوين المصغّر Microblog website.

كما يحتوي "غوغل" على العديد من الأنواع من المواقع كالبريد الإلكتروني ومحرك البحث بالإضافة للمنتديات والمدونات وغيرها.

يتمّ إنشاء مواقع الإنترنت وتصميمها بعدّة طرق، ونتيجة التطور في هذا المجال توافرت العديد من البرامج التي تساعد في إنشاء مواقع إنترنت بوقت أسرع وتكاليف أقل، مثل برامج السحب والإسقاط، و برامج إدارة المحتوى، ومنصات إنشاء مواقع الواجهة الأمامية.

كيف تعمل مواقع الانترنت؟

يتمّ حفظ مستندات الموقع وتطبيقاته على خادم إنترنت web server ، وبغضّ النظر عن نوع الموقع وطريقة إنشائه يحتاج الموقع ليعمل إلى مُخدّم ويب، وهو عبارة عن جهاز حاسب مخصّص للاتصال بالإنترنت بشكل دائم، لاستقبال وإرسال وحفظ البيانات، ويختلف عن الحاسب بأنه لا يحتاج لقطع تحكّم مثل لوحة المفاتيح والماوس كما أنه لا يوجد شاشة عرض.

يتمّ تشغيل مخدّم الويب عبر أنظمة تشغيل مخصّصة ومشابهة لأنظمة التشغيل التي نستخدمها على أجهزتنا الشخصية، لكنّها مُعدّة لدعم عمليات خدمات الويب مسبقًا، ومن أهم أنواع أنظمة تشغيل مخدّم الويب:

لينكس وويندوزCentOS من لينكس: مفتوح المصدر مجّاني ولا يستهلك الكثير من موارد الجهاز والمساحة.

ويندوز سيرفر من مايكروسوفت ويندوز: مغلق المصدر وبحاجة لشراء ترخيص، يستهلك موارد من المخدّم بشكل أكبر من نظام لينكس، لذلك تُعتبر استضافات مخدّم ويندوز مكلفة أكثر.

تُماثل المخاطر والتهديدات التي تواجه مخدّم الويب تلك التي تهدّد الأجهزة الشخصية والتي تحدّثنا عنها سابقًا، ولكنّ الاختلاف الوحيد يكمن في طريقة عمل مستخدم مخدّم الويب وإدارته عن بعد.

ما الذي يحصل في الخلفية؟

لكي يعمل موقع الإنترنت بشكل طبيعي أثناء طلبه عبر الإنترنت، يوجد العديد من التطبيقات مهمّتها نقل ومعالجة البيانات مثل:

IIS (Internet Information Servive)

Apache ,NGINX ,Microsoft

كما يتم استخدام برامج قواعد البيانات مثل:

LQSergtsoP ,SQL Server ,PostgreSQL

ولتسهيل عملية استضافة موقع إنترنت عبر مخدّم ويب، يتوفّر عدد كبير من التطبيقات التي تساعد على إدارة الاستضافة مثل: لوحة التحكم CPanel و WHM التي تعمل على مخدمات الويب والمخدمات الظاهرية العاملة بأنظمة تشغيل لينكس، ويمكن من خلالها إدارة التطبيقات وإضافتها والتحكم بها.

وبشكل عام يوجد عدد كبير من التطبيقات على خادم الويب التي تعمل في الخلفية لتشغيل موقع الإنترنت، من الممكن أن يشكل الوصول إلى إحداها خطرًا على موقع الويب ومحتوياته.

ما الذي يجب مراعاته في حماية مواقعنا على الإنترنت؟

يعتمد الكثير من أصحاب المواقع اليوم على أنفسهم في إنشائه نتيجة توفر وسائل عدّة تُسهّل هذه العملية، كإنشاء مدوّنة عبر Blogger، أو منصات إدارة المحتوى مثل ووردبرس ودروبال، أو أحد برامج السحب والإسقاط. يوكل آخرون هذه المهمّة لمطوّري مواقع إنترنت، وذلك لإنشاء مواقع أداؤها أفضل وبتنسيقات ظهور جيدة، بغض النظر عن نوعية الموقع وطريقة إنشائه.

وفي كلتا الحالتين يوجد عدة نقاط مهمة يجب مراعاتها لحماية مواقعنا ومحتوياتها:

- صلاحيات الوصول: لكل تطبيق أو واجهة تحكّم صلاحيات وصول معيّنة تتطلب اسم مستخدم وكلمة سر، كما أن للاستضافة حساب مستخدم يمنحه صلاحيات الوصول لهذه الواجهات والتطبيقات، ومن المهم مراعاة أن تتم عملية إنشاء الحسابات وكلمات السر بشكل آمن، كما من المستحسن استخدام برنامج إدارة كلمات المرور كيباس لإنشاء كلمات مرور قوية ومختلفة.
- التصميم باستخدام أدوات آمنة: كما وضّحنا سابقًا يوجد عدد كبير من الطرق لإنشاء مواقع إنترنت، ومن المهم الأخذ بعين الاعتبار أمن الموقع أثناء اختيار طريقة إنشائه، مثل اختيار منصة إدارة محتوى مفتوحة المصدر وآمنة والحفاظ على التحديثات، أو اختيار أطر عمل تأخذ بعين الاعتبار العوامل الأمنية.
- تهيئة خادم الويب: يجب التأكد من أن

إعدادات خادم الويب تحتوي على خيارات أمان مناسبة، مثل الحدّ من عمليات الوصول لإدارة الخادم الفاشلة، وتعليق عنوان الإنترنت ضمن لائحة الحظر، وتشغيل التصفّح الآمن باستخدام شهادات تشفير HTTPS لخادم الويب والموقع.

- استخدام أدوات فحص وحماية: يتوفّر العديد من أدوات الحماية الخاصة بمخدّم الويب أو منصات إدارة المحتوى، بعضها يعمل على فحص بنية الموقع واكتشاف الأخطاء والثغرات في التصميم ومواطن الضعف التي قد تشكّل تهديد، وبعضها الآخر يمكنه مراقبة الطلبات من العملاء والحدّ من النشاطات المشبوهة، مثل محاولات تسجيل الدخول لمنصّة إدارة المحتوى، أو الحدّ من هجمات منع الخدمة.
- صلاحيات الوصول للمستخدمين: من المهم جدًا في المواقع التي تتطلّب وجود عدّة مستخدمين لإدارة محتوى الموقع، تحديد صلاحيات وصول مناسبة للمستخدمين تضمن منحهم ما يناسب من صلاحيات كافية فقط لإتمام مهمّتهم، دون الحصول على صلاحيات كاملة، مثل التعديل على التصميم وقواعد البيانات وغيرها.
- تطهير البيانات من المتصفّح: يجب عدم الوثوق بالبيانات الواردة من المتصفّح إلى الموقع، ومن المهم التأكّد من أنّه يتمّ فحصها وتطهيرها قبل معالجتها واستخدامها في استعلامات قواعد البيانات أو حفظها أو تمريرها لنظام التشغيل، مثل إتاحة المجال للعملاء بإدخال بيانات أو رفع ملفّات، فقد يتمّ إساءة استخدام هذه الميزات وإدخال نصوص برمجية أو ملفّات مصابة تنجح في التسلل، واستغلال هذه الطرق للوصول إلى الموقع دون الحصول على إذن وتصريح.


سوريون
من أجل
الحقيقة
والعدالة
Syrians
For Truth
& Justice