العدد الاول

صحيفة نصف شهرية تصدر عن مؤسسة الدرع الالكتروني

IT5: MATRIX.ORG

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

فهرس المحتوى

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

افتتاحية العدد

بسم الله المولى الأجلِ سبحانه له الحمدُ في الأولى والآخرة، نستفتحُ بالذي هو خير، رَبَّنَا عَلَيْكَ تَوَكَّلْنَا وَإِلَيْكَ أَنَبْنَا وَإِلَيْكَ الْمَصِيرُ وبعد، فعلى كثرة ما تموج به الساحة التقنية من إصدارات دورية لا نكاد نجد مجلةً تولي عنايتها خالصةً بالجانب الامني التقني ولا نعني المجلات العلمية المتخصصة، فهي ولله الحمدُ كثيرة، ولا المجلات الثقافية التي تتصل بعضُ موضوعاتها بالجانب التطويري وكذلك لا نغفل وجود الكثير من المجلات التقنية التي تعنى بتطوير المهارات وفي كل المجالات ، لكنَّ مقصودنا أن يكون لدينا مجلة تقنية يقرؤها الاخوة والمتخصص على السواء . فيجد كل منهما ما ينفعة ويفيده فيما يخصُّ امنة على الشبكة العنكبوتية وقد خامر النفسَ زمنًا رغبةٌ في سدِّ هذه الثغرة، غير أنَّ ضيق دائرة المتلقين كانت تُقْعِدُ عن عناءِ الأداء، حتى تولد دافع آخرُ ، فبدأ السعيُ في إخراج هذه المجلة، إلا أنَّ ظروفًا حالت دون إخراجها، فبَقِيَتْ لديَّ حبيسةَ الحاسوب، ومضت الأيام والفكرة الأولى تكبر في نفسي، وتلحُّ عليَّ، حتى استخرت الله عز وجل في أن أخرجها للنُّور في صورة مجلة إلكترونية بصيغة PDF مما يتيح لها بإذن الله تعالى انتشارًا أوسع وتفاعلاً أسرع مع الكتاب والقراء الكرام

الدرع الالكتروني

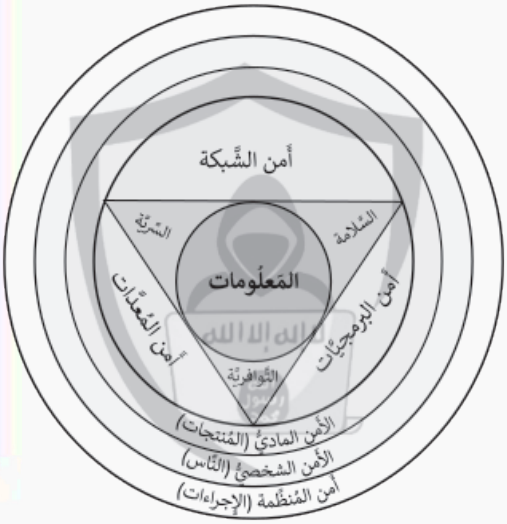
العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

امن المعلومات وحماية الخصوصية

مفهوم امن المعلومات

يمكن تعريف مجال امن المعلومات بكونة فرع من فروع العلوم التقنية الحديثة , وفية يتم حماية المعلومات والبيانات المتداولة سواء على الانترنت او المحفوظة بشكل رقمي في مراكز البيانات من الهجمات الضارة او الوصول الغير مصرح لاي طرف خارجي او التعرض للتخريب المتعمد فيها.

يعد مجال امن المعلومات واحد من اهم المجالات المطلوبة في الوقت الحالي ولا سيما للوظائف التي تتسم بياناتها بالسرية والخصوصية التي ترتقي الى كونها بيانات حساسة للغاية لا يجب تداولها . اذاً يقوم هذا العلم على حماية هذه المعلومات من الضهور وعلى الحفاظ على خصوصيتها ضمن نطاق الاشخاص المسموح لهم فقط



الدرع الالكتروني

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

امن المعلومات وحماية الخصوصية

المبادئ الأساسية لأمن المعلومات

أمن المعلومات مثله مثل أي مجال رقمي ينظمه ويؤسسه بعض من المبادئ الخاصة، هذه المبادئ تساعد على الحفاظ على خصوصية العملاء وأمنهم، بدون أن يمس ذلك بالقواعد الأخلاقية لعملية تبادل المعلومات، وفي الوقت ذاته على سرعة إتاحة المعلومات وتوافرها، لذلك نشأ ما يسمى بالثالوث أو مبادئ أمن المعلومات الثلاثة، وهم كالآتي

اولا : السرية

يقوم مبدأ السرية على الحفاظ على أهم ميزة تم من أجلها إنشاء مجال أمن المعلومات، وهي ضمان وحماية المعلومات الخاصة بالعملاء وعدم السماح للوصول إليها من خلال أي طرف غير مصرح له، وهو بذلك مبدأ تأسيسي ينظم الهدف الأول لخصوصية وأمن المعلومات والذي تعد السرية فيه العماد الأول له.

ثانيا : التكامل والسلامة

يقوم مبدأ التكامل والسلامة على حماية أمن المعلومات من الانتهاك أو التعديل الغير مصرح به، وحتى حالات التخريب الغير متعمدة، إذا من الممكن أن يتسبب عطل ما تقني في تخريب المعلومات المحفوظة أو المتداولة

ثالثا : توافر البيانات

مع الضلع الأخير في ثالوث المبادئ الخاصة بأمن المعلومات، يأتي مبدأ توافر المعلومات كشريطة أساسية لتكامل النظام، حيث يهدف هذا المبدأ إلى جعل البيانات والمعلومات في نوع من التوافر والحيازة المرنة،

الدرع الالكتروني

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

امن المعلومات وحماية الخصوصية

عناصر نظام أمن المعلومات

بالإضافة إلى المبادئ الثلاثة السابقة، يقوم مجال أمن المعلومات في الأساس على ثلاثية أخرى تتكون من ثلاثة عناصر هم

اولا : أمن الشبكات

حتى يتم تداول المعلومات وتخزينها وحفظها بطريقة آمنة للمستخدمين، يجب أن يتم ذلك من خلال شبكة تتسم بالحماية القصوى للبيانات التي تحتويها، لذلك يمثل أمن الشبكات جزء لا يتجزأ من مكونات نظام أمن المعلومات، بل يعد مكونًا رئيسيًا فيه

ثانيا : أمن البرمجيات

أمن البرمجيات هو فرع آخر من فروع أمن المعلومات وهو مكون يركز على صيانة وتصميم أنظمة تقنية تساعد في الحفاظ على خصوصية البيانات وسرعة تداولها وأمنها وهو فرع سريع التطور ويركز بالشكل الرئيسي على علاج الثغرات التي يتم اكتشافها وتطوير الأنظمة لتناسب المتطلبات والهجمات الحديثة كذلك

ثالثا : أمن المعدات

كون مجال أمن المعلومات يركز في الأساس على ثالوث الشبكة والتكنولوجيا والأجهزة المستخدمة، فمن الطبيعي أن يكون فرع أمن المعدات هو المكون الثالث لنظام أمن المعلومات، وفيه يتم التركيز على تطوير الأجهزة والمعدات والتقنيات

امن المعلومات وحماية الخصوصية

مكونات نظام امن المعلومات

أمن المعلومات هو عبارة عن مجال تكنولوجي يتكون من ثلاثيات، فبجانب ثالوث المبادئ وثالوث العناصر الأساسية للنظام، يوجد ثالوث المكونات كذلك، وهي عناصر لا يخلو منها أي نظام أمنى خاص بالمعلومات كالآتي

اولا : الامن المادي

يركز الأمن المادي على اللجوء إلى التدابير اللازمة للحماية المادية لكافة الأصول المستخدمة في تكنولوجيا أمن المعلومات، أي إنه العنصر المسؤول عن حماية المرافق والمعدات والموارد وكذلك الأفراد من التعرض للضرر أو الهجمات أو عمليات الوصول الغير مصرح بها، بهدف حمايتها من التخريب أو الإصابة بأي ضرر يعيق أدائها لوظيفتها الأساسية

ثانيا : الامن الشخصي

يقوم عنصر الامن الشخصي على التثقيف التكنولوجي المطلوب للأفراد المخول لهم الوصول إلى البيانات والأنظمة المستخدمة، إذا يقوم هذا العنصر على تعليم الأفراد أساسيات الأمن المعلوماتي بحيث لا يتعرضون لعمليات الاحتيال السبيراني

ثالثا : أمن المنظمات

يقوم هذا العنصر على توفير كافة الإجراءات وتدابير السلامة والحماية الخاصة بأمن وسرية المعلومات في المنظمات التي يتم استخدامها، بداية من الحفاظ على أنظمة حماية التشغيل والبرامج والتطبيقات

الدرع الالكتروني

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

اساليب الاختراق وطرق التصدي لها

انواع المخترقين

لا يعد الإختراق بشكله العام جريمة يعاقب عليها القانون ، إلا إن تم لغرض الحصول على وصول غير مصرح به الى نظام او شبكة ما ...كما أن ليس كل المخترقين واحد و يصنفون ضمن نفس الخانة . إذ أن هناك ثلاث تصنيفات أساسية خاضعة لمجموعة من المعايير المتفق عليها تعارف الباحثون و العاملون في مجال الأمن المعلوماتي على الأخذ بها في وصف و تصنيف مجموعات الهكرز و هي : هكر القبعات السوداء و القبعات البيضاء و القبعات الرمادية وسنتطرق في هذا العدد الى هذه الانواع بشكل مفصل

اولا : القبعات البيضاء

هاكر القبعة البيضاء هو نفسه الهاكر الأخلاقي الذي لا يملك أي نية في إلحاق الضرر بالأنظمة حيث يقوم بمحاولة إختراقها بغية معرفة .الثغرات الموجودة فيها بهدف التصدي لها هذا النوع من الهاكرز مهم جداً و هناك وظائف كثيرة أمام هؤلاء للعمل فيها

ثانيا : القبعات السوداء

هاكر القبعة السوداء له إسم آخر و هو و هو الشخص الذي (Cracker) كراكر يخترق الأنظمة لأهداف غير قانونية و بدون موافقة من المالك و بدون أي تصريح, فهو يتسلل و ينفذ أجندة خفية منها سرقة ال3بيانات و التهديد بها و قد تتضمن في بعض الأوقات إتلاف النظام قبل خروجه

اساليب الاختراق وطرق التصدي لها

اشهر اساليب الاختراق وطرق التصدي لها

يتصل مفهوم الأمن الإلكتروني بعدد من المفاهيم الإلكترونية الأخرى المتفرعة منه؛ والتي تقوم أيضًا بنفس الوظيفة أو وظيفة مشابهة، مثل: أمن العمليات أو أمن الشبكات أو أمن التطبيقات وما إلى ذلك وأن تهديدات الأمن الإلكتروني أو مايعرف ب أمن المعلومات وإختبار الإختراق تتطور باستمرار مع تقدم التكنولوجيا واستخدام الإنترنت، وفيمايلي بعض أبرز تهديدات الأمن الإلكتروني التي يمكن مواجهتها

اولا : هجوم الرجل في المنتصف

يتم هذا النوع من التهديد عند دخول أحد الأشخاص بين كلاً من المستخدم والشبكة المتصل عليها، وفي الغالب يحدث ذلك في حال استخدام شبكة واي فاي عامة وغير آمنة

فهي من الطرق التي يستخدمها المهاجمون للوصول إلى الجهاز المستهدف عن طريق تثبيت برامج ضارة عليه، ويلي ذلك سرقة بيانات هذا الشخص وإلحاق الضرر به

ثانيا : البرامج الضارة

تعددت البرامج الضارة لتشمل برامج الفدية والابتزاز، برامج التجسس، والفيروسات وغيرها الكثير، مع العلم أن تلك البرامج يتم تفعيلها على الجهاز المستهدف بمجرد ضغط المستخدم على مرفق أو رابط معين يحتوي على أحد تلك البرامج لكن بشكل خفي، وبالتالي يتم تثبيته على الجهاز ويقوم بتعطيل أجزاء منه، ويصبح المستخدم غير قادر على التحكم بالنظام، كما يُمكن عن طريقه الوصول إلى المعلومات السرية الخاصة بالمستخدم

الدرع الالكتروني

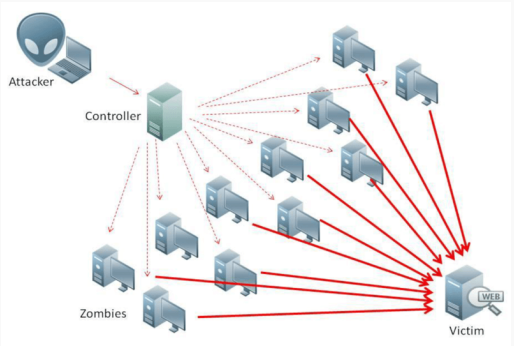
العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

اساليب الاختراق وطرق التصدي لها

ثالثا : التصيد الاحتيالي

يُعد التصيد الاحتيالي واحد من أشكال الهندسة الاجتماعية التي تقوم على خداع المستخدمين ودفعهم إلى الكشف عن بيانات بطاقة الائتمان الخاصة بهم أو بياناتهم الشخصية الهامة، عن طريق رسائل البريد الإلكتروني أو رسائل نصية تخدع المستخدم بأنها مُرسلة من جهات موثوقة

رابعا : الحرمان من الخدمة



يعتبر الحرمان من الخدمة من أنواع التهديدات الإلكترونية التي تتسبب في عدم استجابة جهاز الحاسوب أو الشبكة لطلبات المستخدم، أو من الممكن أن يتم تنفيذها ولكن ببطء شديد

خامسا : هجمات كلمة المرور

في هذا النوع يتمكن المهاجم الإلكتروني من الوصول إلى كلمة المرور الخاصة بالشخص المستهدف عن طريق اختراق قاعدة بيانات كلمات المرور أو التخمين المباشر لها، وبالتالي يتمكن من الوصول إلى معلومات سريّة خاصة بالمستخدم والقيام بسرقتها

الدرع الالكتروني

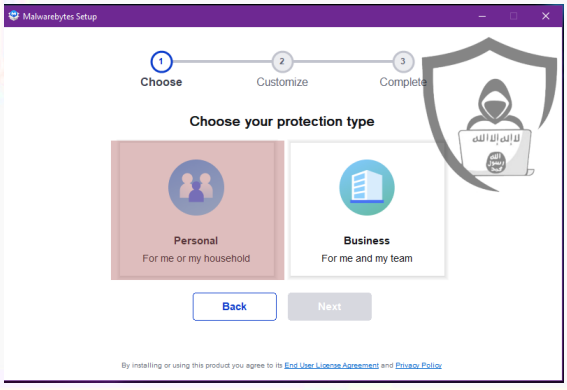
العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

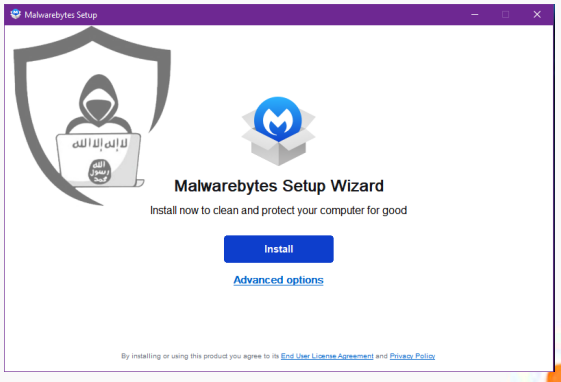
البرامج والاضافات المستخدمة للحماية من الاختراق

موضوع الحماية جدا مهم لكل فرد فهنالك تهديدات كبيرة حيث يوجد قراصنة أعداء الأشخاص الذين يريدون سرقة معلوماتك واستخدام نظامك لتحقيق مكاسبهم الخاصة نظامك يتعرض للهجوم والفيروسات وبرامج التجسس والمتسللين يحاولون سرقة معلوماتك وهويتك وأموالك, أفضل دفاع هو الحفاظ على نظامك نظيفًا ومحميًا سيساعدك هذا الدليل على القيام بذلك هناك عدة برامج تساعدنا في الحفاظ على نظامنا سالم ونظيف ومن اهم هذه البرامج

اولا : برنامج مالوير بايت

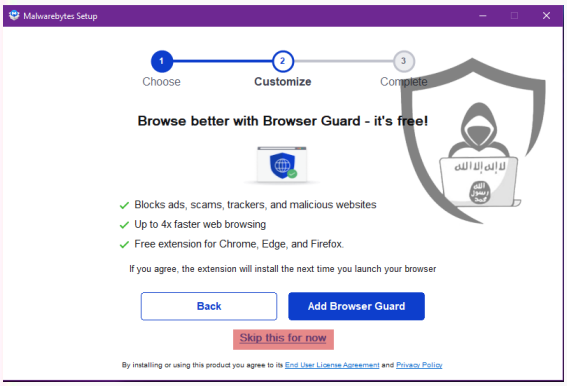
هو تطبيق يحمي جهاز الكمبيوتر الخاص بك من الإصابة بالبرامج الضارة البرامج الضارة هي برامج مصممة لإلحاق الضرر بك أو بجهاز الكمبيوتر الخاص بك ، غالبًا عن طريق سرقة بياناتك أو معلوماتك الخاصة. يحميك تطبيق البحث الموجود على هاتفك تلقائيًا من البرامج الضارة عن طريق فحص محتوى تطبيقات معينة وتحديد ما إذا كانت التطبيقات آمنة أو تشكل خطورة على خصوصيتك. إذا تم تحديد أن التطبيق خطير ، فإن هاتفك يتخذ إجراءات لحماية خصوصيتك وفي ما يلي طريقة تنصيبة بالشكل الصحيح

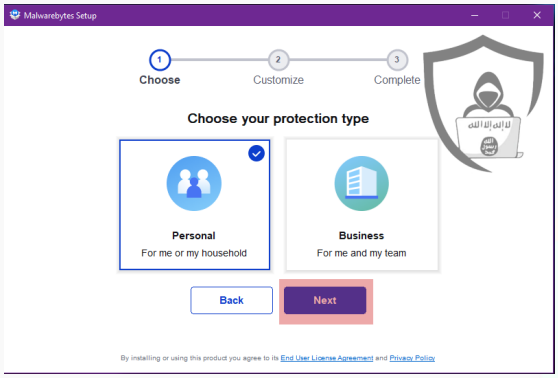


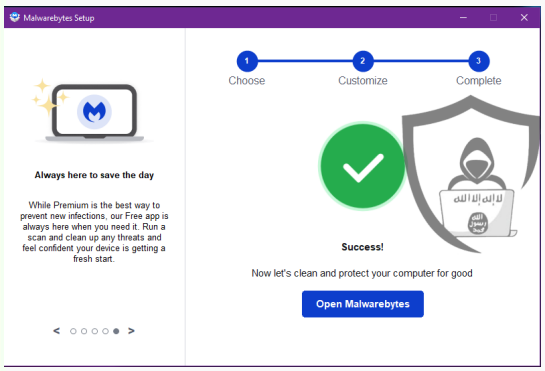


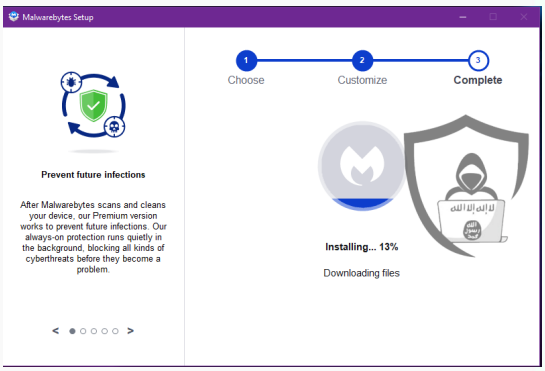
العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

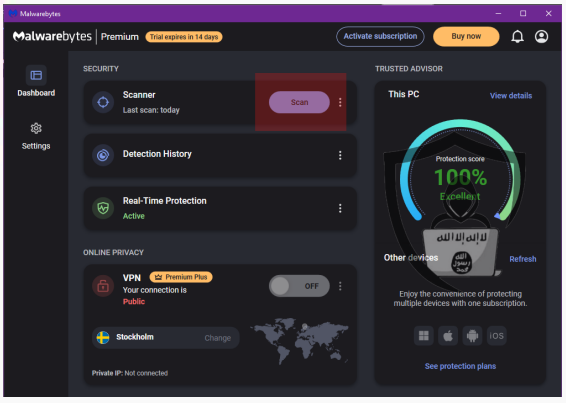
البرامج والاضافات المستخدمة للحماية من الاختراق

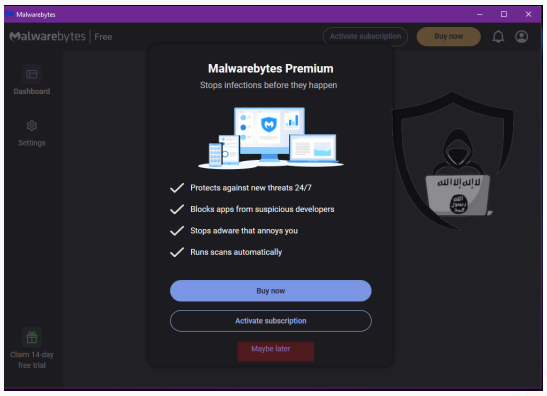












البرامج والاضافات المستخدمة للحماية من الاختراق

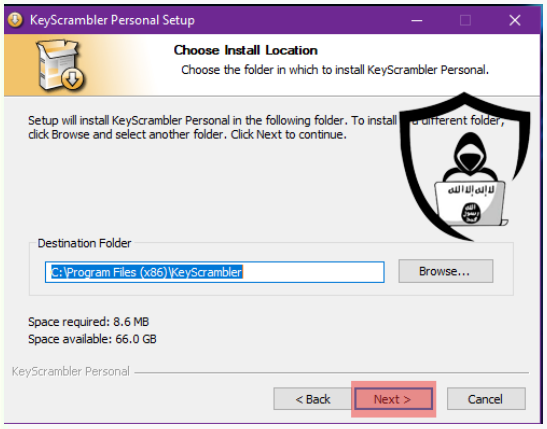
ثانيا : برنامج تشفير لوحة المفاتيح

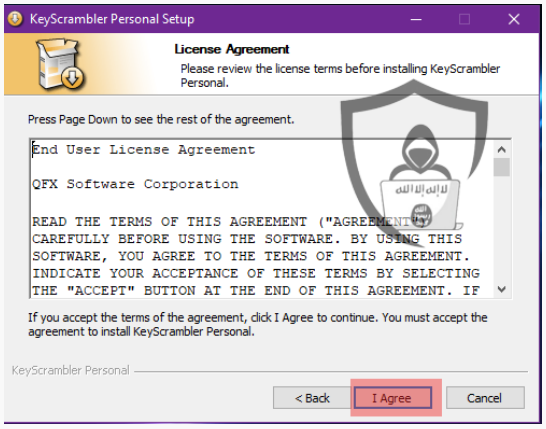
الكيلوجر هو عبارة عن برنامج ينتج سيرفر هذا السيرفر هو عبارة عن فيروسات تروجان يقوم المخترق بأرسال السيرفر الى الضحية وعند فتح الضحية للسيرفر تتم مراقبة كل ضغطة زر تضغطها في الجهاز وبالتالي يستطيع المخترق هنا سرقة جميع كلمات السر من الجهاز وسرقة حسابك المصرفي وكلماتك السرية التي تستخدمها وللحماية من هذه النوع من الاختراق سوف نقوم بشرح برنامج يقوم بتشفير كل حرف يكتب على لوحة المفاتيح تجنبا لهذا النوع من الاختراق اسم البرنامج الذي سنقوم بشرحة

Key S crambler

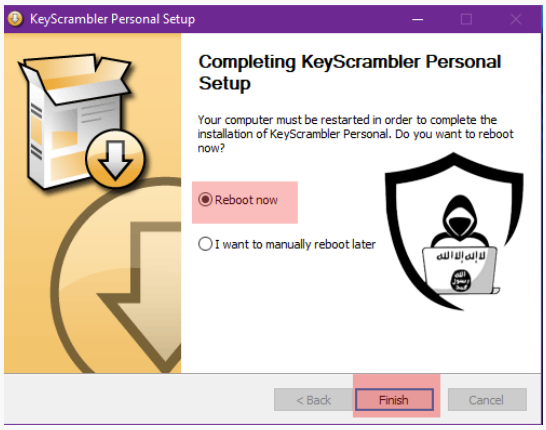
بعدما نقوم بتحميلة من الموقع الرسمي للبرنامج نتبع الخطوات التالية لتنصيبه على الجهاز وكما موضح

البرامج والاضافات المستخدمة للحماية من الاختراق





بعد الضغط على كلمه انهاء سيتم اعادة تشغيل جهاز الحاسوب وسيتم تشغيل البرنامج اليا دون الحاجة الى تشغيلة يدويا وعند كتابة اي جمله سيتم تشفيرها بحيث اذا تم سرقتها من قبل الهاكر ستظهر له جملة مشفر وكما مبين في الصوره التالية



البرامج والاضافات المستخدمة للحماية من الاختراق

نصائح مهمة لزيادة الوعي الامني وتجنبا للوقوع بمصائد المخترقين

يريد الجميع تحقيق الأمن الإلكتروني، ويتم ذلك عن طريق اتباع عدة ممارسات سهلة وبسيطة، ومن كما موضح في المخطط التالي

مدخل الى عالم الشبكات

المنافذ وانواعها واستخداماتها

لمنفذ أو البورت هو عبارة عن بوابات اومنافذ اتصال و قد يعتقد البعض بأنها منافذ مادية في امكانه رؤيتها كمنافذ الطابعة والفأرة ولكنها في واقع الأمر جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة اتصال " اتصال منطقي" يتم عبره ارسال واستقبال البيانات بمعنى اخرهو رقم ملحق بعنوان بروتوكول الإنترنتيستخدم في بعض أشهر بروتوكولات الشبكة بهدف تمييز الخدمات أو البرامج المختلفة .العاملة على ذات جهاز الحاسوب سامحا باستخدام اتصال واحد إلى الشبكة لتقديم أكثر من خدمة فـالمنافذ في ابسط اشكالها هي عبارة عن ممرات تسمح بتبادل المعلومات والبيانات بين شبكة الانترنت وجهاز الكمبيوتر حيث ان الشخص الذي يريد ان يتصل بخدمة شبكة الانترنت لابد وان يستخدم ممر او منفذ للعبور الى هذا العالم الواسع حتى يتم الاتصال والتواصل، ويبلغ عدد المنافذ في الجهاز (65535) منفذ، وكل من هذه المنافذ له وظيفة او خدمة محددة وتستخدم برامج محددة منافذ محددة وعلى سبيل المثال من المعروف ان المنفذ 80 غالبًا ما يكون مخصّصًا لتصفح الإنترنت وفي بعض الأوقات يكون المنفذ رقمه 8080 في شبكات تنتقل المعلومات من منفذ في في الكمبيوتر Portالكمبيوتر المرسل للمعلومة إلى والبرنامج Portالمستقبل للمعلومة حسب رقم الـ الذي يستخدمه هـذا الــمنفذ وكما معلوم فأن كل برنامج له المنفذ معين يعمل عليه في الإتصال وكل المنفذ هو عبارة عـن رقم 16 بت يتألف من صفر حتى 65535وايضا للعلم فأن الـ منافذ تنقـسم إلـى منفذ و منفذ حسب البرنامج الذي يعمل على هذا الـ منفذ

Protocol	Port	Name	Description
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
SSH	tcp/22	Secure Shell	Encrypted console login
SCP	tcp/22	Secure Copy	Relatively simple file copy over SSH
SFTP	tcp/22	Secure File Transfer Protocol	SSH file transfer with file management
Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
DNS	udp/53, tcp/53	Domain Name Services	Convert domain names to IP addresses
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
NetBIOS	udp/137, udp/138	Network Basic Input/Output System	NetBIOS over UDP - Name service, Datagram service
NetBIOS	tcp/139	Network Basic Input/Output System	NetBIOS over TCP - Session service
IMAP	tcp/143	Internet Message Access Protocol	Retrieve and store email
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
TLS/SSL	tcp/443	Transport Layer Security and Secure Sockets Layer	Secure protocols for web browsing
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
FTPS	tcp/990, tcp/989	FTP over SSL	Adds security to FTP with TLS/SSL
ICMP	N/A	Internet Control Message Protocol	Management protocol
IPsec	Various	Internet Protocol Security	Authentication, integrity, confidentiality, and encryption

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

معلومات تقنية عامة

أهم الإختصارات في مجال الأمن السيبراني

MDM - Mobile Device Management
XXS - Cross Site Scripting
XSRF - Cross Site Request Forgery
DRaaS - Disaster Recovery as a Service
DLP - Data Loss Prevention
TCP - Transmission Control Protocol
SNMP - Simple Network Management Protocol
L2TP - Layer 2 Tunneling Protocol
SOC - Security Operations Center
EDR - Endpoint Detection and Response
MDR - Managed Detection and Response
KMS - Key Management Service
TOR - The Onion Router
UEBA - User and Entity Behavior Analytics
UEFI - Unified Extensible Firmware Interface
RFI - Remote File Inclusion
SSID - Service Set Identifier
LAN - Local Area Network
WAN - Wide Area Network
VLAN - Virtual Local Area Network
PGP - Pretty Good Privacy
MiTM - Man in the Middle Attack
CA - Certificate Authority
MAC - Mandatory Access Control
PUA - Potential Unwanted Application
ECDH - Elliptic Curve Deffie-Hellman
BYOD - Bring Your Own Device
GDPR - General Data Protection Regulation
ADFS - Active Directory Federation Service
EPP - Endpoint Protection Platform
UAC - User Account Control
CLI - Command Line Interface
CIA - Confidentiality, Integrity, Availability
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
WAF - Web Application Firewall
PII - Personal Identifiable Information
DoS - Denial of Service
DDoS - Distributed Denial of Service
DNS - Domain Name System
ZTA - Zero Trust Architecture
NAT - Network Address Translation
CTF - Capture the Flag
ACL - Access Control List
CDN - Content Delivery Network
CVE - Common Vulnerabilities and Exposures
RAT - Remote Access Trojan
APT - Advanced Persistent Threat
ATP - Advanced Threat Protection
SSO - Single Sign-on
URL - Uniform Resource Locator
TLS - Transport Layer Security
ARP - Address Resolution Protocol
RDP - Remote Desktop Protocol
FTP - File Transfer Protocol
SFTP - Secure File Transfer Protocol
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
LDAP - Lightweight Directory Access Protocol
MFA - Multi-factor Authentication
IAM - Identity and Access Management
SIEM - Security Information and Event Management
SAM - Security Account Manager

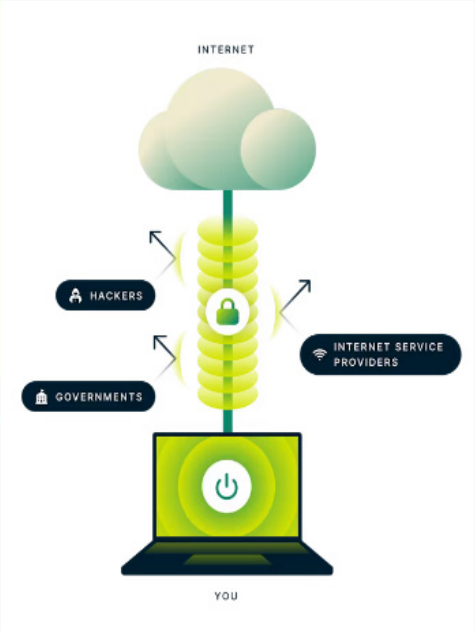
الدرع الالكتروني

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

VPN وحماية الخصوصية

(VPN)

أو الشبكة الخاصة الافتراضية نفق مشفّر آمن بين جهازك والإنترنت. تحميك برامج من التطفل والتدخل في أنشطتك على الإنترنت وجميع أنواع الحظر أو الرقابة على المحتوى الرقمي (الشبكة الخاصة الافتراضية) هو الطريقة الأسهل والأكثر فعالية التي يلجأ إليها مستخدمو الإنترنت للاتصال بالشبكة بكل أمان والحفاظ على خصوصية هوياتهم وبياناتهم الشخصية. خلال الاتصال بخادم في بي ان آمن، توجّه حركة الإنترنت إلى نفق مشفّر يصعب اختراقه أو الاطلاع على بياناته من قبل المتسللين من قراصنة الكمبيوتر والحكومات أو حتى مزودي خدمة الإنترنت



فوائد برنامج (VPN)

اولا : تغيير الموقع الجغرافي

ثانيا : حماية الخصوصية والحياة الخاصة

ثالثا : الأمان على الإنترنت

رابعا : رفع الحظر عن المواقع المحجوبة

متى يجب استخدام برنامج

إذا كنت تعدّ الخصوصية حقا من حقوقك الشخصية يستلزم عليك حمايته، فيجب عليك استخدام في بي ان في كل مرة تتصل فيها بالإنترنت. يعمل تطبيق في بي ان في خلفية جهازك حتى لا يعيق استخدام التطبيقات الأخرى وبث المحتويات وتصفح الإنترنت. وستشعر بالأمان وراحة البال مع العلم أن خصوصيتك محمية دائما

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

VPN وحماية الخصوصية

افضل شبكات VPN لعام 2024

CyberGhost

ExpressVPN

PrivateVPN
Internet Freedom as it should be

privateinternetaccess™

البرامج والاضافات المستخدمة للحماية من الاختراق

NordVPN

IPVANISH

windscribe

Surfshark

الدرع الالكتروني

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

اخر الاخبار التقنية

ثغرة أمنية في واتساب تمكن الحكومات من مراقبة الدردشات

ثغرة أمنية مجهولة بتطبيق واتساب تمكن الحكومات من معرفة من تراسله، وحذر المهندسون في شركة ميتا فيسبوك من أن الدول يمكنها مراقبة الدردشات، وذكر الفريق أنه في شهر مارس/آذار، أصدر فريق أمن واتساب تحذيرا داخليا لزملائه بأنه رغم التشفير القوي للبرنامج، فقد ظل المستخدمون عرضة لشكل خطير من أشكال المراقبة الحكومية. ووفقا لتقييم التهديد الذي لم يُبلغ عنه مسبقا، وحصل عليه الموقع، فإن محتويات المحادثات بين مستخدمي التطبيق البالغ عددهم 2 مليار مستخدم تظل آمنة، لكن الدوائر الحكومية، كما كتب المهندسون، كانت "تتجاوز تشفيرنا" لمعرفة المستخدمين الذين يتواصلون مع بعضهم البعض، وعضوية المجموعات الخاصة، وربما حتى مواقعهم. وحث التقييم على أن يخفف واتساب من الاستغلال المستمر لنقاط الضعف في تحليل حركة المرور التي تمكن الدول من تحديد من يتحدث إلى من. أثار التحذير من التهديد احتمالا مزعجا لدى بعض موظفي ميتا. ومن جانبها قالت كريستينا لونيغرو، المتحدثة باسم ميتا، إن "واتساب ليس له أبواب خلفية وليس لدينا أي دليل على وجود ثغرات في طريقة عمل واتساب

زيادة في عدد الهجمات 130 % السيبرانية خلال الربع الأول من 2024

ارتفع تسجيل الثغرات الأمنية الحرجة 3 مرات عام 2023 مقارنة بالمتوسط السنوي لفترة 2019-2022. وتشير نتائج أبحاث كاسبرسكي إلى أنه وعلى الرغم من حدوث انخفاض طفيف في عدد الثغرات المسجلة في عام 2024، فالمنحى التصاعدي مستمر بسبب الشعبية المتزايدة لأنظمة Linux. عمليات الاستغلال هي برامج مصممة للاستفادة من نقاط الضعف المختلفة في الهجمات السيبرانية. وتكشف أحدث بيانات شبكة كاسبرسكي الأمنية عن زيادة في الهجمات التي تستخدم الثغرات إذ يشير البحث إلى أن الذروة Linux. ضد مستخدمي نظام كانت في الربع الرابع من عام 2023، بينما يستمر الاتجاه العام للنمو في عام 2024، ولو أنه لاقى انخفاضًا طفيفًا في الربع الأول. وفي الفترة من يناير إلى مارس 2024، كانت هناك زيادة بنسبة 130% تقريبًا في الهجمات التي تستهدف مستخدمي نظام Linux باستعمال ثغرات ونقاط ضعف متنوّعة، وذلك مقارنة بالفترة شعبية متزايدة Linux نفسها من العام الماضي. ويكتسب نظام في سوق أنظمة تشغيل الحواسيب المكتبية. فوفقًا لموقع Stat-counter، نمت حصة النظام في السوق، وازداد عدد المستخدمين. ويقول ألكسندر كوليسنيكوف، خبير أمني في كاسبرسكي، عن ذلك: «يفسر هذا الاتجاه بدقة مشهد التهديد المتزايد الذي نشهده وفي المستقبل، من المرجح أن يزداد عدد Linux. لنظام التشغيل عمليات الاستغلال والهجمات بشكل أكبر، مما يؤكد الحاجة الحيوية لتثبيت التحديثات الأمنية والحصول على حل أمني موثوق به». كما أضاف: تكمن أكبر قيمة لمطوري الثغرات في نقاط «.الضعف داخل البرامج التي تمنحهم التحكم في نظام المستخدم وسجلت كاسبرسكي زيادة بنسبة 65% في عدد حالات .الثغرات للثغرات المسجلة عام 2023 وبلغ 1213 ثغرة

العدد الاول صحيفة تقنية نصف شهرية تصدر عن مركز الدرع الالكتروني ذو القعدة 1445

الخاتمة

وفي نهاية العدد الاول من صحيفة الدرع الالكتروني والذي تناول قضية هامة، وتتمثَّل في بعض المبادئ الاساسية للحفاظ على الامان على الشبكة العنكبوتية ، وأوضحنا من خلالها طرق مُجابهة تلك المشكلة، وعلى مستويات عدَّة ولقد حاولنا قدر المستطاع أن نستنهض الهمة، ودافعنا في ذلك تحقيق المواجهة الحاسمة للحد من المخاطر التي يقع فيها بعض الاخوه للحفاظ على امنهم وامانهم على الشبكة ومن خلال ما تم التوصل إليه من نتائج والتي جاءت مُلهبة لمشاعرنا، وزادتنا قوةً وبأسًا وصبرًا، وكانت دافعًا لنا لوضع مقترحات دقيقةلم نكن بذلك مُبتدئين، ولا مُنتهين؛ فهناك الكثيرون من الباحثين الذين يمكنهم تناول ذلك الموضوع بالدراسة، ومحاولة طرح فرضيات واستفسارات مهمةقد تمنحهم أفضلية عنا، وسوف نكون سعداء بذلك، فجميعنا يدًا واحدة في سبيل تخطي السلبيات الحكومات والجهات المعادية للاسلام والمسلمين والتي قد تقف حجر عثرة في سبيل تحقيق الأهداف العامة، حيث سنتناول في الاعداد القادمة سبل اكثر احترافية ليست دفاعية فحسب فسنتناول اساليب الهجوم ايضا لردع كل من يقف امام اهداف الدولة الاسلامية فنحن ما زلنا نقتفي أثر كبار الباحثين، وصلِّ اللهم على سيدنا محمد في الأولين والآخرين، وعدد ما ذكره الذاكرون إلي يوم الدين

مؤسسة الدرع الالكتروني