نصائح مهمه لحمايةنفسك ومعلوماتك على الانترنت

بسم اللَّه الرحمن الرحيم

وبه نستعين

بدون مقدمات

نصائح مهمه لحماية نفسك ومعلوماتك على الانترنت

زوار wasfh / تقنيه وانترنت الكرام سلام اللَّه عليكم ورحمته وبركاته ، أما بعد بما أننا نستخدم الانترنت لتقديم المحتوى لكم ، وكذلك انتم تستخدمون الانترنت للوصول له ولغيره من المحتوى الكثير الموجود على الانترنت ، لذا كان لزاما علينا وعلى كل من يستخدم

الانترنت لتقديم محتوى ما او خدمه معينه ،أن ينشـــىء بموقعه او مدونته قسم خاص بكل مايتعلق بـــالتقنيه والانترنت ،وقد فضلنا أن يكون أول موضوع لنـــا بقســـم تقنيه وانترنت على wasfh أن يكون حول أهم موضـــوع مرتبط باستخدامنا للأنترنت وهو الحمايه ،حيث سنوضح لكم نصائح مهمه وفى ذات الوقت بسيطه تساعدك على حماية نفسك وبياناتك اثناء استخدامك للأنترنت ، حيث على الرغم من بساطة تلك النصـــائح نجـــد ان البعـــض لايقوم بها او لايعرفها من الاساس وبالتـــالى يقـــع فـــى مشكلات عديده.

النصيحه الاولى

احذر شبكات الانترنت الغير مشروعه والعشوائيه

اخى الكريم واختى الكريمه ، أحذروا أحـــذروا مـــن استخدام شبكات الانترنت الغير مشـــروعه والعشـــوائيه على هواتفكم الذكيه والتابلت او اجهزة سطح المكتب او اللابتوب ، ولكن اولاً دعونا نعرف ماهى شبكات الانترنت الغير مشروعه والعشوائيه وعندنا هنا بمصـــر يســـميها

الناس وصلة النت و بعضهما يسميها وصلة حرامى النت ، وتنتشر مثل تلك الشبكات عندنا هنا بمصر بالاحياء الشعبيه وكثير من القرى البسيطه ، حيث يقوم احد الاشخاص بتركيب خط تليفون ارضى سلكى من الشركه المصريه للأتصالات(WEحالياً) ثم الاشتراك بخدمة الانترنت المنزلى ADSL الغير محدوده التابعه لنفس الشركه TEData(WE حالياً) ثم بدون ذكر التفاصيل يقوم باحضار جهاز كمبيوتر واجهزه آخرى لتوزيع الانترنت لمدى ومسافه معينه عن طريق ا لواى فاى او الوصلات السلكيه للآخرين مقابل الحصول منهما على اشتراك شهرى معين يترواح سعره بين 30الى 60جنيه شهرياً فيما بين 2:3دولار تقريباً فى اغلب المناطق عندنا هنا بمصر (وهذا الاشتراك اقل بكثير من سعر الاشتراك الرسمى والشرعى لدى الشركه) ثم يقوم باعطاء المشترك ياسورنيم وباسورد محدده يقوم المشترك بادخاله على ويب باج لتلك الشبكه ومن ثم الدخول على الانترنت من خلال شبكته ، وأغلب من يقومون بعمل مثل تلك الشبكات عندنا بمصر هما من فئة الخارجين على القانون والعاطلين عن العمل ،وللأسف الكثير من الناس

يشتركون بتلك الشبكات ويستخدمون الانترنت من خلالها لأسباب مختلفه منها رخص سعر الاشتراك بها او لعدم توافر خدمةالانترنت المنزلى (عدم وجود كابل أو خدمة تليفون أرضى سلكى) بجوار منازلهم وارتفاع اسعار انترنت الموبايل والـ USB MODEM المقدم من شركات المحمول فى مصر بشكلاً مبالغ فيه ، دون أن يدركوا المخاطر والمشكلات التى قد يتعرضون لها بسبب استخدامهما لتلك الشبكات للأسف ،حيث يرتكب كثير من هؤلاء الاشخاص ممن يقو مون بانشاء وادارة تلك الشبكات(وصلة النت) العديد من الجرائم الالكترونيه ضد المشتركين لديهما بالأضافه لمخالفتهما الصريحه لقانون تنظيم الاتصالات الذى يمنع انشاء مثل تلك الشبكات.

اخطر المشكلات والجرائم الناجمه عن استخدام شبكات الانترنت الغير مشروعه(وصلة النت)

بأختصار شديد يقوم الاشخاص الذين يديرون هذا النوع من الشبكات والوصلات بتحميل وتنصيب برامج معينه منتشره على الانترنت لتوزيع الانترنت وتقسيم السرعات للمشتركين و فصل الانترنت ومراقبة المشتركين والأجهزه الخاصه بهما ومايتصفحونه وتسجيل كل ما

يفعلونه سواء كان المشترك يستخدم الهاتف او غيره من الأجهزه ويستخدمون ايضا طرق وحيال وبرامج خبيثه اخرى لتصفح اجهزة المشتركين بمختلف انواعها سواء كانت هواتف ذكيه او اجهزة كمبيوتر والاطلاع على ماتحتويه من صور وملفات وغيرها من البيانات من خلال جهاز الكمبيوتر الذى يقوم هؤلاء الاشخاص بتشغيل شبكة الانترنت او الوصله من خلاله، ويمكنهم كذلك طبعاً الدخول على حساباتك على مولقع التواصل الاجتماعى الفيسبوك وتويتر ويوتيوب ، وغيرها من المواقع الآخرى او قد يحصل احدهم على الباسورد الذى تدخل به على موقعك وتديره وغيرها من تلك الأمور العبثيه ، ويمكنهم ايضا زرع اياً من برامج التجسس المنتشره على الانترنت بأجهزة المشتركين لديهما الكمبيوتر والتليفون دون علمهما والتى تقوم بفتح الكاميره او الميكروفون دون علم صاحب الجهاز ليقوم من زرع تلك البرامج بمشاهدته من كاميرة جهازه او التنصت عليه من الميكروفون دون ان يدرى الآخر أو التنصت على المكالمات الهاتفيه وتسجيلها، وبالمناسبه أى من هؤلاء الاشخاص يمكنه القيام بمثل تلك الأمور وبمنتهى

السهوله وبدون خبره مسبقه او أدنى معرفه بعلوم الحاسب ، وذلك بسبب انتشار تلك النوعيه من البرامج على الأنترنت حيث كل ما يحتاج اليه هؤلاء هو تحميل مثل ذلك النوع من البرامج ،ومن ثم استخدامها، لكننا لن نذكر لكم كيف يقومون بذلك لأن ذلك يخالف اتفاقية الاستخدام الخاصه بنا ،وما لفت نظرى الى اضرار تلك الشبكات انه حدثت مشكله عندنا هنا بمصر منذ مده بسيطه (بدون ذكر للأماكن اوالاشخاص) حيث قام احد هؤلاء الاشخاص الذين يديرون مثل تلك الشبكات بالدخول على هاتف مشترك بشبكته ثم قام بألاستيلاء على صوره منه لزوجته كانت موجوده على هاتفه ثم قام بالتعديل عليها بالفوتوشوب لتبدو بوضع غير لائق ثم قام بنشر وتوزيع تلك الصوره على الأنترنت بواسطة حساب فيسبوك تابع لأحد الاشخاص من الجيران والاهالى بنفس المنطقه من المشتركين بشبكته ايضا(حساب استولى عليه من احد المشتركين بشبكته بعد حصوله على الباسورد الخاص به) وظل مالك حساب الفيسبوك الاصلى الذى تم من خلاله توزيع الصوره المصطنعه والغير لائقه دون علم بما تم من خلال

حسابه لمده تزيد على يوم كامل لانشغاله بعمل كان يؤديه خارج المدينه وعدم أتصاله بالأنترنت ،وكادت تحدث مشكله كبيره جداً لولا معرفة الاهالى والناس بالمنطقه بمدى سمو اخلاق ذلك الشخص الذى تم نشر وتوزيع تلك الصوره المصطنعه الغير لائقه بواسطة حسابه على الفيسبوك المستولى عليه ومدى التزامه الدينى والاخلاقى بالأضافه لمر كزه الأجتماعى وتدخل الكبار من أهل الجهه والمنطقه حيث كان من الواضح ان هناك طرف آخر قام بهذه الجريمه الدنيئه وحتى لا اطيل عليكم تمت الاستعانه بأحد الفنيين المتخصصين فى تكنولوجيا المعلومات والاتصالات لكشف ومعرفة كيف تمت تلك الجريمه ومن قام بها من خلال فحص هاتف الزوج الذى كانت موجوده به الصورة وطرق اتصاله بالانترنت ثم بعد التأكد من المجرم الاساسى الذى قام بهاتان الجريمتان الاستيلاء على صوره شخصيه من هاتف ونشرها على الانترنت من خلال حساب فيسبوك استولى عليه دون علم صاحبه ،وبعد ذلك تم ابلاغ جهاز الشرطه المختص بجرائم الانترنت والاتصالات والجريمه الالكترونيه والذى قام ايضا بأجرائته من حيث فحص

الهاتف الذى كانت به الصوره وفحص اجهزة صاحب حساب الفيسبوك (المتهم البرىء) التى يمكنها الاتصال بالانترنت ، ظهر ان الفاعل والمجرم الاصلى هو الشخص الذى يدير شبكة الانترنت الغير شرعيه(وصلة النت) بالحى، وللأسف الشديد ذلك النوع من الحوداث والمشكلات منتشر عندنا هنا بمصر وصار معتاد ،وتلك الحادثه تعتبر كمثال لما قد يحدث من مشكلات بسبب الاشتراك بمثل تلك الشبكات وتصفح الانترنت بأجهزتنا بما تحتويه من معلومات واسرار شخصيه خاصه بنا من خلالها ،ويقوم البعض ممن يديرون هذه الشبكات بتنصيب برامج مراقبه وتجسس واحيانا تنصت على المكالمات عبر الانترنت على الهاتف الذكى وعلى مختلف انواع الاجهزه دون علم الضحيه وتتم تلك العمليه غالباً اثناء عملية ادخال الياسورنيم والباسورد على صفحة الويب باج الخاصه بالشبكه(صفحة تسجيل الدخول) ، حيث قد يستفيد بعض المجرمين من الحصول على معلومات معينه مثل ارقام بطاقات الأئتمان ، معرفة المتواجدين بالمنزل واوقات خروجهم عند استهداف او التخطيط لسرقة منزل معين او التخطيط لارتكاب جريمه معينه ، وغيرها من الاسرار التى

لايجب ان يعلمها الا صاحبها ، ويأخوانى وأخــواتى الكــرام يوجد عدة طرق مختلفه تمكنك من حمايــة نفســك وبياناتك يمكنك استخدامها عند قيامك بالاشتراك بمثل تلك الشبكات ، يمكنك معرفتها بالبحث علــى الانــترنت وجوجل ولن نتطرق اليهــا فــى هــذا الموضــوع ،ولكــن نصيحتنا لكم هى كما تقول الامثله الشعبيه الباب الــذى يأتى منه الريح سده واستريح والوقايه خيــر مــن العلاج مليون مره ، ننصحكم بعدم استعمال مثل تلك الشبكات لتصفح الانترنت وبخلاف خدمة الانترنت التى تقــدمها شركات المحمول وفى حال ماكان اســتعمالك للأنــترنت كثيف اشترك بصوره قانونيه عن طريق مزودى خدمــة ADSL ببلدك وان لم تكن متوفره بمنطقتك فيمكنك استعمال الانترنت عبر خدمــة الــ USB MODEM المقدمه من شركات المحمــول علــى الرغــم مــن ســعر الانترنت المرتفع لها ولكنها تبقى وسيله أمنه جــداً فــى مثل تلك الحاله خصوصاً ان كنت تستخدم الانترنت مــن أجل تأدية عمل معين او تقديم خدمه ما او للتجاره .

ملحوظه مهمه

المقصود بشبكات الانترنت الغير مشروعه (وصلة النــت)

هنا الشبكات التى يتم الاشتراك بها مقابل دفع مبلغ

معين من المال ولها صفحة تسجيل دخول ويب باج بأسم

مستخدم وباسورد سواء كانت سلكيه او واى فاى ، وليست

خدمة الانترنت واى فاى المجانيه التى تتيحها بعض

المقاهى او المطاعم او النوادي _الخ لروادها ،لأن الاتصال

بألانترنت من خلال ذلك النوع من الشبكات يكون غالبًا

من خلال الرواتر مباشرة ، وليس عبر جهاز كمبيوتر سيرفر

لتوزيع الانترنت كما فى حال وصله النت مثبت عليه

برامج للتحكم بالشبكه مثل قطع الخدمه وتقسيم

السرعات أو التجسس والمراقبه_ الخ ، و المخاطر هنا

تكون اقل ، ولكنها موجوده ، وعموما ينصح بتصفحها

عبر VPN

النصيحه الثانيه

استخدام مقاهى الانترنت (النت كافيه) بشكلاً آمن

أخوانى الكرام فى حال ما أضطررتم فى وقت ما لاستخدام

مقهى الانترنت لتصفح الويب ، فاحرصواعلى ألا تقوموا

بتصفح او فتح أى من حساباتكم على مواقع التواصل الاجتماعى او غيرها من المواقع المختلفه او القيام بادخال أى بيانات هامه خاص بكم او باعمالكم من خلالها، لماذا؟ لأن جميع مقاهى الانترنت تستخدم برامج مثل

handy cafe و (Easy cafe(tina soft

،وتقوم هذه البرلمج ومثيلاتها بمراقبه وتسجيل الانشطه والتحكم بشكلاً كامل بجميع ألاجهزه الموجوده بالمقهى من خلال جهاز واحد يديره ويتحكم به مدير المقهى،كما ان بعض مديرى هذه المقاهى يقومون بتنصيب برامج Keylogger لتسجيل كل مايتم القيام به من ضغطات على لوحة المفاتيح الكيبورد بشكلاً واضح وتفصيلى فبمجرد قيامك من على الجهاز واطفائه يمكن للشخص الذى يدير المقهى بمنتهى البساطه وبضغطة زر معرفة جميع ما قمت به من نشاط على الانترنت من المواقع التى زرتها وما كتبته من كلمات وباسووردات وغيره وماقد يحدث جراء ذلك لنت تعرفه طبعاً ، وينصح البعض باستعمال لوحة المفاتيح الافتراضيه على الشاشه للكتابه اثناء التواجد بمقهى

الانترنت وعدم الكتابه من خلال الكيبورد مباشرة لتجنب تسجيل الضغطات وانشطاتك على لوحة المفاتيح من خلال برامج الـ keylogger ولكنى أرى ان تلك الخطوه غير كافيه ايضا حيث توجد طرق وبرامج اخرى عديده لتسجيل الشاشه ومراقبة مايقوم به مستخدم مقهى الانترنت ، كما ينصح البعض عند للدخول لمقهى الانترنت واستخدامه بعمل ريستارت(اعادة تشغيل) للجهاز والضغط المستمر على زر F8 عند البدء باعادة التشغيل للدخول للتشغيل بنظام الوضع الآمن Safe mode ثم اختيار وضع safe mode with network ثم الضغط على Enter حيث ان تشغيل جهاز الكمبيوتر العامل بنظام ويندوز بهذا الوضع يمنع عمل الكثير من البرامج مثل التى ذكرناها لكم سابقاً وأمثالها (معظم هذه النوعيه وليس جميعها) ، وينصح ايضا عند ارتياد مقاهى الانترنت أن أمكن باستخدام جهاز اللابتوب الخاص بنا من خلال الولوج للأنترنت مباشرة من خلال الرواتر الرئيسى بالمقهى وليس عبر أى جهاز كمبيوتر آخر بالمقهى منصب عليه برامج لتوزيع الانترنت ويجب أن يكون جهاز اللابتوب الخاص بنا مثبت عليه برنامج جدار

نارى حقيقى ذو فعاليه قوى ومفعل سواء كـــان نظـــام التشغيل الذى يعمل به جهازنا ويندوز أو ماك او لينكس ،هذا بالاضافه لأستخدام خدمة VPN وتصفح الانترنت من خلالها ، وكما ذكرنا لكم ببداية هذا الجـــزء لا ينبغـــى استخدام مقاهى الانترنت لتصفح حساباتنا على مواقـــع وسائل التواصل الاجتماعى او غيرها ، او ادخال اى بيانات هامه خاصه بنا مثل القيام بالتقدم لتنسيق الجامعات او التقديم لأى خدمه حكوميه آخـــرى الكـــترونيه تقـــدمها الدوله أو جهة ما عبر الانترنت ،أو أدارة أى عمل لنا عـــــبر الأنـــترنت، أو اســـتخدام بطاقـــات النقـــود الائتمـــانيه أو مسبقة الدفع ،وهذا يعتبر خطأ كبير يجب الا نقع فيـــه حيث يجعل ذلك البيانات الهامه الخاصه بك والتى ينبغى ان تكون سريه ولا يعلمها ألا صاحبها عرضه لأن تقع بيد العابثين وقد يسبب ذلك بعض المشكلات الكثيره التى نحن فى غنى عنها، وعموماً مقـــاهى الانـــترنت يتـــم ارتيادها فقط من أجـــل اللعـــب أو مشـــاهدة او تحميـــل الافلام او الموسيقى _الخ .

النصيحه الثالثه

أحذر الدخول على مواقع الويب المزيفه

Fake Websites

اولاً لمن لايعرف مواقع الويب المزيفه Fake websites هى مواقع مشابهه للمواقع الحقيقيه بالضبط 100٪ ظاهرياً فقط ماعدا الرابط الموجود فى الشريط العلوى للمتصفح ، ويقوم البعض بعمل مثل تلك المواقع المزيفه بغرض الاستيلاء على حسابات مواقع التواصل الاجتماعى فيسبوك تويتر يوتيوب_ الخ وارقام بطاقات الائتمان وغيرها للأخرين ،ويتم عمل تلك المواقع المزيفه بمنتهى البساطه ببرامج وطرق سهله جداً يعرفها الكثيرين ومنتشره عبر الأنترنت ، فمثلاً يقوم شخص ما باستعمال برنامج مشهور لعمل موقع مزيف يكون هذا الموقع نموذج مزيف للفيسبوك حيث تكون صفحة تسجيل الفيسبوك المزوره هذه نفس شكل صفحة تسجيل الفيسبوك الحقيقيه 100٪ ماعدا الرابط ،وعندما يقوم الضحيه بادخال بياناته كالمعتاد والباسورد يتم ارسالها بذات الوقت وبالتفاصيل للشخص الذى قام بعمل هذا الموقع المزيف ،ونحن هنا وضحنا ذلك على الفيسبوك كمثال ولكن تلك الخدعه يمكن تطبيقها بمنتهى السهوله مع مواقع آخرى مثل مواقع

البيع والشراء ومواقع تقديم الخدمات المختلفه والتى تتطلب ادخال ارقام بطاقات الائتمان والبطاقات مسبقة الدفع .

كيف تتجنب مواقع الويب المزيفه

يمكن تجنب مثل تلك المواقع بسهوله تامه وبدون برامج حمايه،حيث كما ذكرنا لكم سابقاً تكون تلك المواقع المزيفه متطابقه من حيث الشكل الخارجى مع الموقع الاصلى بنسبة 100٪ ، ولكن الاختلاف يكون فى الرابط الذى يظهر فى الشريط العلوى للمتصفح حيث يكون رابط الموقع المزيف يكون اسم الموقع به حرف او رقم او رمز زائد عن الاصلى فعلى سبيل المثال رلبط الفيسبوك الاصلى

https: / /www.facebook.com

اما رابط الموقع المزيف فقد يكون مثلاً

http: / /www.facebook2.com

وبالاضافه لذلك يظهر بجانب رابط الموقع الاصلى بالشريط العلوى للمتصفح رمز قفل مغلق باللون الاخضر، اما فى الموقع المقلد المزيف يكون رمز القفل

هذا غير موجود طبعاً ،و اكثر طريقه شائعه للقيام بهذه الخدعه هى عن طريق ارسال رساله مزيفه على البريد الالكترونى للشخص المستهدف على اساس انها من الفيسبوك او تويتر الخ تطلب منك القيام باجراء معين من خلال الضغط على الرابط الموجود بالرساله واعادة تسجيل الدخول مثلاً حيث يقوم هذا الرابط بتوجيهك للموقع وصفحة تسجيل الدخول المزيفه وبالتالى ارسال البيانات التى قمت بادخالها لمنشىء الموقع المزيف ، لذلك ننصح بالحرص جيداً على فحص الروابط الموجوده برسائل البريد الالكترونى وكذلك التأكد جيداً من مصدر تلك الرسائل قبل اتخاذ أى اجراء او الضغط على اى رلبط موجود بالرساله ،ويوجد العديد من برامج الحمايه التى توفر لك الحمايه من تلك المواقع المزيفه وتمنعك من الدخول عليها بشكلاً تلقائى، ويمكنكم معرفة المزيد عن تلك البرامج وكذلك مواقع الويب المزيفه Fake websites

من خلال البحث عبر الانترنت وجوجل.

ملحوظه

اكثر من يقوم باستخدام تلك الحيله (مواقع الانترنت المزيفه Fake websites)؛ بعض مديرى ومشغلى شبكات الانترنت الغير مشروعه(وصلة النت) ،متى؟ عندما يفشلون فى اختراق او الدخول على جهاز الشخص المستهدف المشترك لديهم ،لأسباب مختلفه ، فيقومون بمراقبة سلوك الشخص المستهدف على الانترنت ، من حيث اكثر المواقع التى يتصفحها ومايهتم به واكثر مايبحث عنه عبر الانترنت ، فلقد حدث على سبيل المثال أن عرف احد هؤلاء الاشخاص أن احد المشتركين بشبكته يتصفح موقع سوق دوت كوم قسم الكمبيوتر واللابتوب بكثره ويبحث عن لابتوب بسعر مناسب ، فقام بعمل صفحه مزيفه طبقا الأصل لموقع سوق دوت كوم بها عرض بيع لابتوب بسعر مناسب ،وصنع تلك الحيله باستخدام برنامج معروف لصنع مواقع الويب المزيفه ،بحيث عندما يقوم الشخص المستهدف (المشترك بشبكته) بالدخول على الانترنت من خلالها فى المره القادمه وطلب موقع سوق دوت كوم للبحث عن طلبه يرسل له تلك الصفحه المزيفه التى بها عرض بيع لابتوب بسعر مناسب فيقوم الضحيه بطلب شرائه من

خلال البطاقة الائتمانيه او المسبقة الدفع ومن ثم ادخال بياناتها ثم سرقتها من طرف صانع الصفحه المزيفه .

النصيحه الرابعه

الحرص على تصفح المواقع الأمنه العامله بنظام https

فى الحقيقه عندنا هنا بمصر أصبح الغالبيه العظمى من الناس لا تتصفح غير الفيسبوك يليه اليوتيوب (وموقع اليوم السابع الذى يعتبر الموقع الاخبارى الاول بمصر من حيث المتابعه لجميع فئات المجتمع) واصبح من النادر جداً ومن الماضى أن تجد من يتصفح غير تلك المواقع وهذا على حد علمى من المحيطين بى، حيث كل من أعرفهم فى مدينتى من الاصدقاء والأهل والاقارب والجيران لا يتصفحون سوى الفيسبوك واليوتيوب فقط ، ومواقع التواصل الاجتماعى تلك الفيسبوك وتويتر وغيرها واليوتيوب هى مواقع أمنه جداً لأنها تعمل بنظام بروتوكول الطبقات الأمنه SSLلتشفير البيانات ، حيث لو نظرت للرابط الخاص بمثل تلك المواقع بالشريط العلوى للمتصفح تجده يبدأ بـ https وبجواره

علامة القفل الاخضر وليس http،والمواقع الالكترونيه التى تبدأ بـ https وبجوارها علامة القفل الاخضر هذا يعنى انها تستخدم نظام تواصل مشفر يقوم بتشفير البيانات المتبادله بين جهازك ان كان كمبيوتر او تليفون او تابلت وبين الخادم النهائى للموقع ،وهذا يعنى ان عملية التواصل مع هذا الموقع أمنه ومشفره، وعندما تتصفح مثل تلك المواقع فأن مزود خدمة الانترنت لن يكون بمقدوره الا ان يعلم الا اسم الموقع الذى تزوره فقط ،ولن يستطيع ان يعرف مضمون الرسائل التى ارسلتها وقراءة الايميل للذى ارسلته او استقبلته او المعلومات التى ادخلتها سواء كانت ارقام بطاقات بنكيه باسوردات الخ ، ولايمكن قراءة المعلومات او الرسائل الا من خلالك ومن خلال الخادم النهائى للموقع للذى تتصفحه بنظام https ،وهذا الامر غير موجود طبعاً فى المواقع التى تبدأ بـ http حيث تكون البيانات من خلالها غير مشفره ويمكن قرائتها والاطلاع عليها ،وننصحكم اخوانى الكرام فى حال ما أردتما تصفح مواقع اخرى غير مواقع التواصل الاجتماعى واليوتيوب ، بأن تكون تلك المواقع بقدر الامكان تبدأ بـ httpsوبجوارها

رمز القفل الاخضر ،ولا تقم بالبيع او الشـــراء او ادخـــال اى بيانات الا بالمواقع التى تبدأ بـــ https حتى لايستولى عليها طرف ثالث وتأكد جيداً من وجـــود علامـــة القفـــل الاخضر بجوار الرابط ، وبالمناسبه يمكنك تنزيـــل اضـــافة https everywhere للمتصفح الذى تستخدمه حيث ستعمل تلك الاضافه علـــى توجيهـــك دائمـــا للمواقـــع العامله بنظام https فقط وعموماً ننصحكم اخوانى الكرام بالحرص جيداً على تصفح المواقع ذات الســـمعه الجيده والمصداقيه والتى تقدم محتوى جـــاد وحقيقـــى يفيدك، ويقدم لك ماتبحث عنه بالفعل ،وتجنب تصفح المواقع التى بها كثير من الاعلانات المزعجـــه والنوافـــذ المنبثقه والروابط المضـــللة، للـــتى تســـتخدم الكلمـــات والعناوين الجذابه المخادعه لتجذب اكبر عدد من الـــزوار لاغراض مختلفه .

النصيحه الخامسه

تحميل وتنصيب البرامج والتطبيقات الأمنه

اكثر من يعانى من مشـــكلة تنصـــيب البرامـــج الخـــبيثه بشكلاً خاطئ مستخدمى الاجهزه العامله بنظام الوينـــدوز

يليه الماك ،وسبب ذلك يعود لسهولة وطريقة تركيب البرامج على الويندوز عكس اللينكس حيث يتم تركيب البرامج بطريقه وشكل مختلف تملماً عن الويندوز ،ونصيحتنا لمستخدمى الويندوز والماك لتجنب تلك المشكله كالتالى:اولاً لا تقم ابداً بتحميل اى برنامج سواء كان مجانى او مدفوع عن طريق المواقع والمنتديات (بالذات العربيه)المشهوره وغيرها من المواقع المشابهه المشبوهه والمضلله، لاتقم بتحميل اى برنامج ألا من الموقع الرسمى الخاص به اومن احد مواقع البرامج الآمنه التى يمكنك معرفتها من خلال البحث على جوجل واحرص على فحص اى برنامج جيداً بواسطة برنامج الحمايه الموجود بجهازك ثم فحصه أونلاين بأى خدمه مجانيه جيده من خدمات فحص واكتشاف البرامج الخبيثه والفيروسات مثل virustotal وتوجد خدمات اخرى مشابهه لها يمكنكم معرفتها من خلال البحث على جوجل ، وبالنسبه لتحميل وتركيب البرامج مفتوحة المصدر على نظام الويندوز والماك برامج GNU مثل برنامج openshot او gimp اوبرنامج vlc اوغيرها من البرامج مفتوحة المصدر لاتقم بتحميل اى نسخه من

تلك البرامج ابداً الا من الموقع الرسمى الخاص بالبرنامج المقصود ، سواء كانت النسخه عاديه او محموله،لأن تلك البرامج المفتوحة المصدر تختلف عن المجانيه والمدفوعه فى أن الاكواد الخاصه بها تكون متاحه للجميع حيث يعمل على تطويرها وتعديلها كثيرين حول العالم وبالتالى قد يأخذ شخص ما اكواد برنامج معين ويقوم بالتعديل عليه واضافة خواص خبيثه عليه مثل التجسس والمراقبه تسجيل لوحة المفاتيح استخراج الباسوردات التحكم بالاجهزه زرع فيروسات الفديه _الخ وغيرها من تلك الامور ونفس الامر ينطبق على انظمة التشغيل مفتوحة المصدر جميع توزيعات لينكس، لذا احرص جيداً على عدم تحميلها الا من موقعها الرسمى ،واتبع نفس الامر مع جميع توزيعات لينكس عند الرغبه بتحميلها وتركيبها بجهازك ،وبالنسبه للتطبيقات الخاصه بالهواتف والاجهزه الذكيه لاتقم بتحميل وتركيب أى تطبيق على جهازك الا من المتجر الرسمى التابع له نظامك سواء كنت تستخدم الاندويد متجره الرسمى google play ، او أبل متجره الرسمى App store ، وقبل تثبيت اى تطبيق ينبغى ان تقوم

بالبحث لمعرفة معلومات دقيقه عنه من حيث مميزاته وعيوبه وما يقدمه عبر الانترنت ومحرك البحث جوجل.

النصيحه السادسه

استخدام نظام تشغيل ذو نسخه اصليه

لا يعانى من تلك المشكله الا مستخدمى اجهزة الكمبيوتر واللابتوب ، حيث تقوم الغالبيه منهما بتنزيل وتنصيب نسخ مهكره ومقلده من انظمة التشغيل المدفوعه الويندوز بكافة اصدارته ،وذلك على الرغم من توافر البدائل المجانيه بالكامل الجميله والقويه التى تضاهى نظام الويندوز بل وتتفوق عليه فى بعض الجوانب، حيث يوجد العديد من توزيعات اللينكس المختلفه التى تلبى كافة احتياجات مستخدمى الكمبيوتر واللابتوب لتنفيذ اعمال كالتصميم بمختلف انواعه والاعمال المكتبيه بمختلف انواعها وتحرير الفيديو وانتاج الرسوم المتحركه والشبكات والبرمجه والأمن والاستخدام العادى والمناسبه والمتجاوبه مع امكانيات جميع الاجهزه الضعيفه والمتوسطه والقويه الحديثه والقديمه ، وعلى الرغم من توافر هذه البدائل المجانيه الرائعه نجد أن

الغالبيه تفضل استخدام النسخ المهكره للويندوز على تلك البدائل لأسباب مختلفه ، واستخدام تلك النسخ المهكره الغير اصليه من الويندوز المنتشره على الانترنت يجعلك عرضه للأختراق واستخدام جهازك بأعمال اخرى غير مشروعه دون علمك عبر الانترنت بسهوله من جانب من قاموا بعمل تلك النسخه الغير اصليه المهكره للويندوز ويعرض جميع بياناتك ومعلوماتك الهامه والسريه للخطر بسهوله ، وبالأضافه لذلك تسبب تلك النسخ الغير اصليه والمهكره للويندوز الكثير من الاعطال والاضرار لجهازك التهنيج والبطء ، كما انها تستهلك موارد الجهاز الهاردوير بكثره وتقصر من عمرها واحيلناً قد تتلفه ، لذلك ننصحكم بشده باستخدام نسخه اصليه ومفعله بشكل قانونى من نظام التشغيل المدفوع ويندوز ،وان لم تكن ترغب بدفع المال وشراء تلك النسخه الاصليه للويندوز ،فألافضل لك ان تستخدم اى توزيعه من لينكس تكون مناسب لأستخداماتك وامكانيات وقدرات جهازك ولكن انتبه جيداً عند قيامك بتنزيل اى توزيعه من نظام لينكس المجانى ان تقوم بتحميل التوزيعه الاصليه ويكون ذلك من موقعها الرسمى على الانترنت

حتى لاتقع لك مشكلات لأنه كما ذكرت لكم سابقاً نظـــام اللينكس نظام مجانى مفتوح المصدر اى يمكن التعـــديل على خواصه من طرف اى مبرمج بالعالم .

النصيحه السابعه

البرامج المقرصنه

لاتقم بتحميل وتركيـــب اى نســـخ مفعلـــه او مقرصـــنه مسبقاً للبرامج المدفوعه وننصحكم كذلك بعدم تفعيل ايه برامج تجريبيه بطـــرق غيـــر قـــانونيه بالكرلكـــات والباتشات ، لأن ما ذكرنه لكم سابقاً بخصوص هذا الأمـــــر فيما يتعلق بأنظمة التشـــغيل الغيـــر اصـــليه نســـخ الويندوز المقرصنه ينطبـــق بالضـــبط علـــى البرامـــج ، وبالمناسبه لا يوجد برنامج مدفوع ألا ويوجد له بـــديل مجانى او مجانى ومفتوح المصدر يضاهيه ويتفوق عليه احيانا كثيره ، وذلك فى كافة انواع البرامج مثل برامـــج التصميم المختلفه و بعض برامـــج المونتـــاج وتحريـــر الفيديو والحمايه وغيرها .

النصيحه الثامنه

تحديث نظام التشغيل والبرامج

ننصحكم بشده بالحرص الدائم على تحديث نظام التشغيل الخاص بكم أيا كان ويندوز، ماك ، لينكس ، اندرويد iOS بشكلاً منتظم من خلال تنزيل وتثبيت التحديثات الدوريه التى تصدر لنظامك ،لما اذا كنت تستخدم ويندوز 10فعملية تحديث النظام تلك ستحدث بشكلاً تلقائى دون اى تدخل منك ، وبالمناسبه لا داعى لأستعمال أى نسخة ويندوز توقف دعمها أو أى نظام تشغيل آخر توقف دعمه ، وبخصوص الويندوز يفضل وينصح بشده عدم أستعمال أى نسخة ويندوز تم أصدارها قبل ويندوز 10 (استخدام أصدارت ويندوز 10 فقط) حيث النسخ السابقه تعتبر أنتهت فعلياً ، وكذلك احرص على تحديث كافة التعريفات الخاصه بالهاردوير الخاصه بجهازك بانتظام مثل تعريف كارت الشاشه كارت الشبكه _ الخ، وكذلك تحديث جميع البرامج للتى تستخدمها على جهازك أيا كانت خصوصاً برامج الحمايه والمتصفحات ،حيث أن تلك التحديثات التى يصدرها منتجى انظمة التشغيل والبرامج ومصنعى الهاردوير تعمل على القضاء على العيوب التى تم اكتشافها لاحقاً بمنتجاتهم ومن ثم القضاء عليها وسد أى ثغرات امنيه

تم اكتشافها بها ،وبالأضافه لذلك القيام بجميـــع تلـــك التحديثات بانتظام يحافظ ويرفع من كفأءة الاجهزه.

النصيحه التاسعه

استعمال برنامج حمايه وجدار نارى قوى

يقترح ويرى بعض المختصين بالأمن الرقمى حول العالم ، بضرورة تثبيت برنامج حمايه قوى ذو سمعه جيده من أجل مزيد من الحمايه، كذلك يقترح البعض بشده مراعاة تثبيت برنامج جدار نارى قوى لمزيد من الحمايه القـــويه والفعاله بأذن اللَّه ويوصون بذلك الأمر تحديـــداً لمستخدمى نظامى التشغيل الويندوز و الماك ،ومن أشهر برامج الحمايه الموجوده حالياً والتى لها اصدارت تعمـــل على انظمة تشغيل مختلفه ، الويندوز ، الاندرويد، الماك، اللينكس

البرامج التاليه:

Comodo Internet Security و Avast و AVG و Avira و Bitdefender و (nod32 eset)لايوجد لـــه نسخه مجانيه تجريبيه فقط ومدفوعه) وغيرها يمكنك معرفتها من خلال البحث عبر جوجـــل ،ومعظـــم النســـخ

المدفوعه من برامج الحمايه يأتى معها برنامج جدار نارى للحمايه ،والنسخ المجانيه من هذه البرامج توفر قدر جيد من الحمايه لا بائس به ،وتوجد حزمة حمايه متكامله تسمى Comodo Internet Security لها نسخه مجانيه و آخرى مدفوعه وهى آحد انظمة الحمايه التى تقدم العديد من المزايا فى مجال الحمايه حيث توفر برنامج جدار نارى وبرنامج فحص ضوئى للفيروسات والبرمجيات الخبيثه ونظام حمايه من التجسس والتسلل للأجهزه ونظام لفلترة مواقع الانترنت التى تزورها وحمايتك من المواقع الضاره وغيرها من خدمات الحمايه وجميع تلك المزايا موجوده فى النسخه المجانيه كما ان النسخه المدفوعه من Comodo Internet Security تحتوى على ميزات اكثر والنسخه المجانيه توفر قدر جيد من الحمايه لاتوفره احياناً بعض البرامج الآخرى المدفوعه او المجانيه التى يتم الترويج والدعايه لها بكثافه على الانترنت لأستخدامها وذلك على حد زعم الشركه المنتجه comodo،واذا كنت من مستخدمى نظام الويندوز فاحرص على عمل boot time scan بأى برنامج حمايه موثوق من وقتاً لأخر حيث فحص

الجهاز بهذه الخاصيه يتيح لبرنامج الحمـــايه اكتشـــاف وتدمير البرامج الخبيثه والفيروسات المختبئه داخل بنية نظام الويندوز نفسه والتى لا يمكن اكتشافها او الوصـــول اليها بطرق الفحص العاديه.

ملحوظه مهمه

جداً لا يجب تثبيت اكثر من برنامج حمـــايه واحـــد علـــى الجهاز واذا تم تثبيت اكثر مـــن برنامـــج حمـــايه واحـــد فسيحدث تضارب بينهما ولن يعمل أيا منهمـــا كمـــا ان نظام التشغيل سيتضرر وقد يتعطل

برامج الجدار النارى

بأختصار شديد لمن لايعرفون ما هو برنامج الجدار النارى ،الجدار النارى برنامج وظيفته أحكام الســيطره ومراقبــة جميع الأنشطه والأتصالات الداخله والخارجه من جهـــازك عبر الأنترنت أو الشبكه ، ومنع الضار منها والتحكم بها من حيث السماح لها أو منعها ، وحماية جهازك وبياناتـــك الموجوده عليه من المتلصيصن ومن يسمهيما البعـــض بالهاكرز او الدخول عليها والتحكم من جانب طرف آخر عبر الانترنت او الشبكه بدون علمك وموافقتك ســـواء كـــان

ذلك الطرف شخص أو برنامج،وللعلم تعتبر برامج الجدار النارى الحقيقيه من أفضل الوسائل المتاحه لحمليه الأجهزه من استغلال نقاط الضعف والثغرات الأمنيه التى يتم أكتشافها فى الأنظمه والبرلمج وللتى يستغلها القراصنه والمالوير (البرمجيات الخبيثه والفيروسات) فى الهجمات وتنفيذ مهامهم ، ويأتى مع بعض أنظمة التشغيل برنامج جدار نارى مثبت بشكل أفتراضى ، مثل نظام الويندوز وبعض توزيعات اللينكس مثل توزيعة linuxmint ،كما يوجد العديد من برامج الجدار النارى الخارجيه والاضافيه التى بها مزيد من الإمكانات والميزات ،بعضها متوافر بشكل مجانى والآخر مدفوع، مثل برنامج FreeFirewall المتوافر لنظام ويندوز وهو مجانى بالكامل وهو الأفضل على الاطلاق بدون منافس حتى كتابة هذا الموضوع ،ويوجد ايضا برامج جدار نارى آخرى منها Comodo Firewall و Zone alarm وغيرها الكثير يمكنك معرفة المزيد منها من خلال البحث على جوجل

ملحوظه

لاينبغى تثبيت اكثر من جدار نارى واحد على اى جهاز

حاسب حتى لايحدث تضارب بينهما وتشنج لنظام التشغيل ، ما عدا برنامج FreeFirewall

لأنه الوحيد الذى به ميزة أمكانية تثبيته بجوار أى برنامج جدار نارى آخر دون أن يحدث ضرر او تضارب بينهما ويمكن كذلك تثبيته بجوار جدار ويندوز النارى الاساسى بدون أى مشاكل ، أما برامج الجدار الآخرى ينبغى أزالة أو ايقاف عمل اى جدار نارى آخر مثبت على الجهازولو كان حتى جدار الويندوز الأساسى.

أفضل برنامج جدار نارى لنظام ويندوز 10

عن تجربه شخصيه أفضل برنامج جدار نارى لنظام الويندوز هو برنامج FreeFirewall الذى تقدمه شركة EVORIM الالمانيه للبرمجيات ، وهو مجانى بالكامل ، وأهم ميزه فيه انه جدار نارى حقيقى حقيقى متكامل بمعنى الكلمه ، عكس برامج الجدار النارى الآخرى الشهيره مثل comodo firewall و zone alarm وغيرها وعيوبها المعروفه مثل عدم أمكانيتها التحكم بكثير من الاتصالات الصادره والوارده عبر الانترنت التى تتم من خلال النظام والتى تقوم بها كثير من البرامج والخدمات

الموجوده على نظام ويندوز 10 (أذا ما فائدة هذا النوع من الجدران الناريه ،وبالتالى لا يعتبر جدارنارى ولا حتى هوائى)، فضلاً عن كونها مزعجه وثقيله وتؤثر على الجهاز وسرعته ، كما أن البعض يراها برامج وهميه لا توفر أى قدر من الحمايه ،وميزتها الوحيده انها تمتلك واجهة مستخدم جميله "شىء مثير للسخريه"، اما برنامج Free Firewall فهو جدار نارى يتيح أمكانية التحكم بكل الاتصالات الداخله والخارجه عبر الانترنت والشبكه فى جهازك بدون أى استثناء ،وكما انه يمنع أى اتصال ضار وارد او صادر من مالوير او فايروس ،يتيح كذلك أمكانية التحكم فى تلك التى تعمل فى الخلفيه بصورة مشروعه ،مثل بعض خدمات الويندوز windows services التى تستنزف أحيانا رصيد اتصالك بالانترنت بشكلاً كبير ومبالغ وباستمرار بدون داعى لأغراض مختلفه ،كجمع البيانات المختلفه وارسالها لخودامها عبر الانترنت ، كما أن بعض البرامج تجمع معلومات وبيانات عن مستخدميها وترسلها لخودامها عبر الأ نترنت ،وتكون تلك معلومات مثلاً عن نوعية الفيديوهات والصور التى تحب مشاهدتها وتحميلها

وكذلك الموسيقى _الخ من مثل تلك الأمور ، بألاضـــافه لخدمة التحديث الأجباريه على ويندوز 10 والتى لاتملـــك أمكانية التحكم بها ، كل تلك الأمـــور تســـتنزف رصـــيد اتصالك بالأنترنت ، ولكن مع برنامـــج Free Firewall لديك أمكانية التحكم بها من خلال ايقافهـــا أو الســـماح لها ، ومن مميزات Free Firewall ايضا حجمه الصغير حيث لا يتجاوز برنامج التثبيت الخاص بنسخته الاخيـــره 35 ميجا بألاضافه لكونه خفيف جداً على النظام لدرجـــة انه يمكنك تثبيته بجوار اى جدار نارى آخـــر بـــدون أى مشكلات ، حيث يعمل بمنتهى السلاسه ،فـــى الحقيقـــه برنامج Free Firewall جدار جدار ممتاز من جميع النواحى (فعلاً صناعه المانيه) .

موقع Free Firewall الرسمى

ما هو افضل برنامج حمايه (مضاد فيروسات) لويندوز 10؟

قبل الاجابه على هذا السؤال لابد أن نعرف أن الفيروسات والمالوير يتم تشفيرها من طرف صانعيها حتى لا تتمكن برامج مكافحة الفيروسات مـــن التعـــرف عليهـــا وعلـــى كيفية عملها ، وبالتالى تكون المعركه هنا بين تشـــفير

الفيروسات والمالوير بأنواعها من طرف صناعها ، ومحاولة فك تشفيرها من طرف برامج الحمايه ومكافحة المالوير والفيروسات للتعرف عليها وأيقاف عملها ، وللعلم برامج مكافحة الفيروسات لا تكتشف الفيروسات والمالوير الحديثه ،أنما تكتشف فقط الفيروسات والمالوير المعرفه فى قاعدة تعريفاتها المحدثه بأستمرار وتحمى منها ،أما الفيروسات والمالوير الجديده فقد تستغرق أسابيع واحياناً أشهر حتى تتعرف عليها ويتم أضافتها لقاعدة بياناتها وتوفير الحمايه منها ، وكمثال على ذلك فيروس الفديه الشهير اريد البكاء i wanna cry الذى هاجم العديد من المؤسسات والشركات الكبرى والأجهزه الشخصيه حول العالم فى عام 2017 ولم تجدى نفعا معه برامج مكافحة الفيروسات المعروفه، أما برامج الجدار النارى الحقيقى مثل Free Firewall ألية عملها تختلف عن برامج الحمايه من ومكافحة الفيروسات كما ذكرنا سابقاً ،حيث تقوم بمراقبة كل الأتصالات للوارده والصادره من جهازك عبر الأنترنت والشبكه والتحكم بها من حيث منعها أو الموافق عليها ومنع اى نشاط مشبوه للأستيلاء على البيانات وأرسالها عبر الانترنت ،وللعلم

استخدام برامج الجدارن الناريه الحقيقيه يساهم بشكلاً فعال فى الحد من أنتشار الفيروسات والمالوير عبر الأنترنت ، وفى رأيي الشخصى افضل برنامج حمايه متاح لويندوز 10 هو برنامج windows Defender والذى يأتى مثبت بشكل افتراضى مع ويندوز 10 ويوصى بالحرص على تحديثه بانتظام ، ووفقا لأراء اكبر الخبراء فى العالم windows Defender هو الافضل والاكفاء للحمايه من الفيروسات والمالوير بمختلف انواعها ومن حيث العمل على بيئة ويندوز 10 ولمزيد من الحمايه نوصى بتثبيت برنامج الجدار النارى Free Firewall .

ملحوظه مهمه جداً

بالنسبه لمستخدمى انظمة اللينكس لا ينبغى تصفح الانترنت واستخدامه الا بعد تنصيب الجدار النارى وتفعيله ، اما بالنسبه لبرامج الحمايه الخاصه بأنظمة اللينكس فيمكنك الاستغناء عنها ان أرادت مع انها توفر

قدر اضافى وزائد من الحمايه مع بنيـــة النظـــام القـــويه أساساً .

النصيحه العاشره

أخيراً نوصيكم بتنظيف السجل (history) لمتصـــفحات الانترنت التى تستخدمونها واختيار خيار التنظيـــف مـــن البدايه واختيار جميع الخيارات ، ونوصيكم ايضابـــتركيب اضافة منع الاعلانات uBlocker ويمكنك تعطيلها على المواقع التى تثق بها، ويمكنكم كذلك تركيب أى اضـــافه من بعض الاضافات المجانيه الآخرى التى تفيـــدكم فـــى الحمايه من المواقع السيئه والفيروسات وتقييم المواقع من حيث كون سمعتها جيده او سيئه، المتـــوافره علـــى متجر اضافات جوجل كروم وفـــايرفوكس ، ويمكنكـــم معرفة المزيد عن تلك الاضافات من خلال البحـــث عـــبر جوجل .

انتباه

الموضوع منشور على موقعنا على الانترنت

wasfh.blogspot.com ويتم تحديثه باستمرار

ليواكب احـــدث المســـتجدات بخصـــوص الحمـــايه علـــى الانترنت والامن الرقمي ، لذا فى حالـــة الاهتمـــام نوصـــى بالاطلاع عليه من حين لأخر عبر موقعنا على الانـــــترنت للبقاء على علم بأحدث المستجدات بهذا الخصوص

رابط الموضوع الأصلى على الانترنت

نصائح مهمه لحماية نفسك ومعلوماتك على الأنترنت

تلك النسخة

الـ pdf خاصه

بموقع

kutub.info

لزيارة موقعنا والتواصل معنا