ANHRI

س و ج
عن أمانك الرقمي

بداية

بالطبع، انت مهموم بأمانك الرقمي وحساباتك على الكمبيوتر والموبايل ، وكلمات المرور.
في هذه الورقة المبسطة ، نقدم لك بعض النصائح والارشادات لتزيد من أمانك الرقمي وتزيد من صعوبة قرصنتها وتقلل من التهديدات باختراقها.

النصيحة الأهم :

أفضل شيء يمكنك فعله لتحسين أمانك الرقمي والحفاظ على خصوصيتك هو تغيير عاداتك في استخدام الشبكة العنكبوتية.

وهنا سنوضح لك بشكل مبسط إزاي تكون في أمان.

س: إزاي تعمل باسورد ؟

كل الناس عموما بتنسي كلمه المرور وعشان كدة معظم الناس بتعمل باسورد عبارة عن ارقام مكررة او تاريخ ميلاد او رقم الهاتف ودا اكبر غلط لآنه يعرض نفسه للاختراق من قبل مخترقين ممكن يسرق الحساب الخاص بيك يسرق الواي فاي يفتح تليفونك يطلع علي اسرارك وخد بالك ممكن جدا إنه لو عرف الباس ورد الخاص بشبكة الإنترنت ممكن يبقي موجود معاك ويسحب كل المعلومات من جهازك واي جهاز موجود علي شبكة الواي فاي .

الباسورد

تاكد بوجود احرف كبييره و صغيره و ارقام و رموز دخل كلمه المرور حتى يصعب على المخترق تخمين كلمه المرور

وعشان كدة يستحسن إنك تخفي شبكة الواي فاي نهائي مثلا .

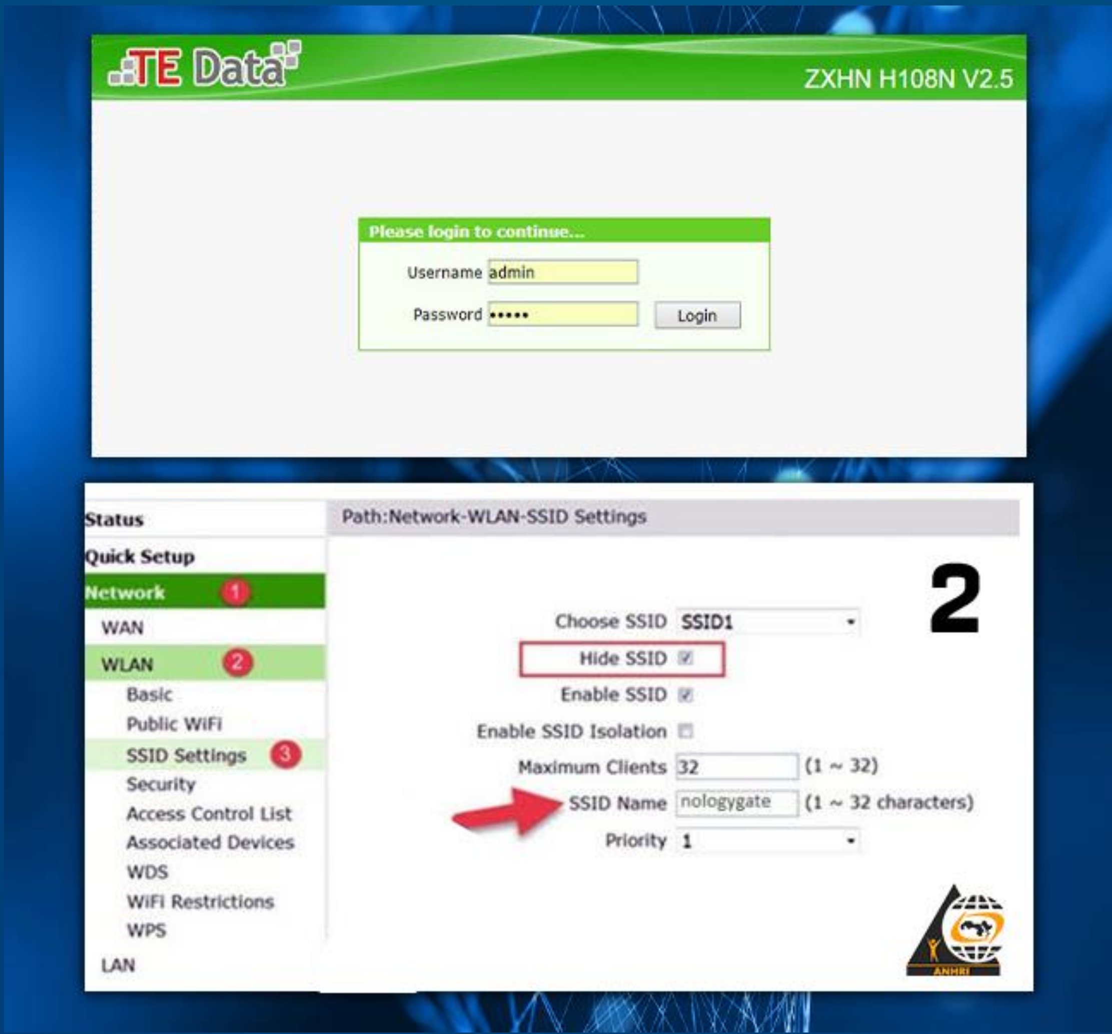
س: إزاي تخفي شبكة الواي فاي؟

هتفتح اي نوع من انواع المتصفح جوجل كروم او فاير فوكس او غيرة

هتكتب في مكان العنوان

عنوان الروتر الخاص بك مثل (192.168.1.1) او حسب نوع الروتر الخاص بك

و بعد متفتح صفحه الروتر تكتب اسم المستخدم و كلمه المرور الخاصه بك و اذا كانت اول مره تدخل على صفحه الروتر بتلاقى اسم المستخددم و كلمه المرور خلف الروتر
اتبع التعليمات بدقة



س: هل تعلم ان ملفاتك موجودة علي الهاتف او علي الهارد بعد المسح او عمل فورمات لأي جهاز؟

يوجد عده طرق استعاده البيانات المحذوفه من على الهاتف او من على الهرد دسك بعد عمل فورمات له و لكن ليس هذه النقطه الاتى نشرحها الان
الطريقه الصحيحه لمسح الملفات بلا عوده هى الادوات المتاحه التى يمكنها كتابه بيانات وهميه عشوائيه فوق البيانات الموجوده على جهازك و هذه يضمن ان تصبح ملفاتك الشخصيه المحذوفه غير قابله للاسترجع تماما و للقيام بذالك يمكنك استخدام تطبييق مثل (Shreddit - Data Eraser)

س: يعني ايه اختروق للاجهزة؟

يعني في ناس متطفلة كتير عايشين وسطنا عندهم هواية وجنون حب الاستطلاع والتطفل علي الغير والتصنت عليهم ، وفي برامج كثيرة بإمكانها تسرق الصور الخاص بيك وممكن تأخذ اي معلومات من جهازك أو موبايلك ، وتفتح الكام والمايك

س: طيب ازاي اكون امن وسط كل ده ؟

ج: اول حاجة زي ما قولنا إن الباس ورد لازم يتم تأمينه حتي يصعب تخمينه من قبل المخترقين.

- ولما تروح اي مكان لا تشحن هاتفك مثلا في لاب توب خاص باي حد تكون واخد الشاحن معاك عشان احتمال كبير يكون الشخص صاحب الجهاز صاحب هوس الاطلاع ويكون حاطط برامج علي جهازه لسرقة الاشياء الخاصة بمجرد توصيل اليو اس بي للشحن.
- لا تفتح الموقع دائما في الموبيل الا عند الضرورة فقط
- اي حد بعتلك رابط اوعي تدخل عليه ،، ليه ؟
- هبسطلك الامر الرابط اللي بتدخل عليه ده ممكن يكون عبارة عن فيرس يدمر نقط الامان لما تدوس عليه وينقل كل حركة بتعملها للمخترق وهنوضح دا فيما بعد ،، تابع

وفي برنامج اسمه key logger بيسجل جميع ضربات المفاتيح التي تقوم بها علي الكي بورد

س: ما هو vpn للتصفح الآمن؟

كلمة VPN اختصار لجملة Virtual Private Network، وتعني " شبكة خاصة افتراضية ، ووظيفتها إنشاء اتصال آمن بينك وبين الإنترنت، مما يزودك بطبقة إضافية من الخصوصية وإخفاء الهوية. وهو يختلف كثيرا عن استخدام البروكسي ، وأكثر أمانا.
وفي كذا برنامج سهل التعامل معها علي الهاتف منها

ExpressVPN

Opera Free VPN

طبعا سهل تحميل البرامج دي من جوجل ومن ابل استور وتشغيلها باتباع الخطوات في منتهي السهولة.
وممكن تشوف الفيديو ده هيساعدك في تحميل VPN
https://www.facebook.com/146770222053055/videos/1353689898123706

س: وكيف احمي الايميل؟

لحماية الايميل ، ممكن تستخدم خدمة بريد إلكتروني مشفرة مثل بروتون ميل
https://mail.protonmail.com/login
هو مزود خدمة بريد إلكتروني تم تطويره في العام 2013 في سويسرا. ويتميز "بروتون ميل" بتصميمه الذي يتيح للمستخدمين المجهولية والأمان التام وذلك عبر عدد من الميزات:

1- التشفير بين طرفين (End to End Encryption): والذي يتيح تشفير الرسائل والملفات قبل إرسالها من جهاز المستخدم.
2- لا يتطلب وجود رقم هاتف، أو أي بريد إلكتروني إضافي لإنشاء الحساب.
3- عبر اعطائك مساحة صغيرة "نصف جيجا فقط" كحساب مجاني ، فهو يجعلك ، اويجبرك على مسح الايميلات القديمة كل فترة ، واذا كنت عايز مساحة اكبر ، لازم تدفع.

س: وماذا عن اختراق حساب الفيسبوك؟

كلمة اختراق حساب فيس بوك الالاف من الناس بتدور عليها محاولة منهم لايجاد وسيلة لاختراق حسابات مستخدمين اخرين " لو كانوا هاكرز" او لتأمين حساباتهم " كمستخدمين عاديين".

- سنحاول تبسيط الامر بلغة وأمثلة بسيطة :

سنطرح عليكم بعض وسائل الامان لكي نبين لكم الطرق التي يستعملها الهاكراو المخترقين لسرقة الحسابات الشخصية و على اي برامج يعتمدون .

1- اختراق حساب الفيس بوك. عن طريق الصفحات المزورة :

يمكن للهاكر اختراق حسابك الخاص على موقع فيسبوك عن طريق صفحات مزورة إما من إنشاءه الخاص أو عن طريق العديد من المواقع التي تقدم هذا النوع من الخدمات ، و هذا ما يعرف في مجال الاختراق بالتصعيد Phishing .

و تكون عملية الاختراق ناجحة عندما يضغط الضحية على هذا الرابط الخبيث الذي يوجهه إلى صفحة شبيهة تماما بصفحة الدخول إلى فيسبوك ومن ثم يطلب منه إدخال اسم المستخدم وكلمة السر و الضغط على زر الدخول ، وعندما تتم هذه الخطوة يكون الهاكر قد حصل على معلومات دخولك الشخصية و يتمكن عبرها من السيطرة على حسابك .

لذلك لا تفتح اي روابط يرسلها اليك اي شخص غريب عنك ، وتأكد ان الصفحة التي فتحت هي فيس بوك فعلا.

2- اختراق حساب الفيس بوك عن طريق الكوكيز :

الكوكيز عبارة عن ملفات نصية صغيرة يمكن إرسالها وتسجيلها على الحاسوب الخاص بك بواسطة مواقع الويب التي تقوم بزيارتها، ثم يعاد إرسالها إلى نفس المواقع عند زيارتك لها مرة أخرى. ... وقد تحتوي أيضًا على رمز معرّف فريد يتيح تتبع أنشطة التصفح داخل موقع الويب، لأغراض إحصائية أو إعلانية.

3- اختراق حساب الفيس بوك عن طريق ال **Key logger** :

برامج ال Key logger هي برامج تقوم بتسجيل جميع ضربات المفاتيح التي تقوم بها على الكيبورد وهي في الأصل برامج عادية لا تضر بالنظام ، ولكن يأتي دور الهاكر هنا ، في دمج هذا البرنامج مع صورة أو مقطع ملتيميديا أو برنامج تنفيذي يكون امتداده عادة " exe " مستعملا في ذلك الهندسة الاجتماعية لدفعك للضغط عليه أو تحميله و تثبيته على الجهاز .

و عندما تقع في هذه الحيلة فإن ال Key logger سيقوم بأرسال جميع ضربات المفاتيح التي قمت بها على ايميل الهاكر الذي أعده مسبقا و بذلك سيتعرف على معلومات دخولك إلى الفيس بوك بالإضافة إلى العديد من المعلومات الأخرى .

4- اختراق حساب الفيس بوك عن طريق ال **Access token**

يعتبر ال Access token بمثابة كلمة السر الثانية لحسابك على فيسبوك وهو عبارة عن رابط مخصص يمكن الحصول عليه من خلال تطبيقات الفيس بوك Facebook apps ، و عندما يقع هذا الكود بين أيدي الهاكر فإنه يصبح لديه جميع صلاحيات حسابك و يتحكم به تحكما كليا .

و لقد انتشرت في فترة سابقة العديد من التطبيقات مثل " اعرف من زار بروفاليك ، أكتب اسمك على قارورة كوكا كولا ، ضع صورتك مع الاسد ، اخترق أي حساب فيسبوك ،،،الخ"
و غيرها من العناوين المغرية ، التي ما هي إلا وسيلة قد يستعملها الهاكر لاختراق حسابك و معرفة معلوماتك الشخصية

س: ليه مهم تغير نظام التشغيل الخاص بك؟

على الأغلب فإنّ معظمنا يستخدم نظام التشغيل Windows من شركة مايكروسوفت، هناك أنظمة أخرى مثل Mac OS X من شركة Apple ونظام Linux وتوزيعاته المختلفة التي يطوّرها مطورون من شتّى أنحاء العالم. لا يوجد شيء آمن 100% ولا يمكن اختراقه، كلّ هذه الأنظمة قابلة للاختراق لكن فقط قد تزداد الصعوبة، ونحن ننصحك بالانتقال إلى نظام Linux فهو الأكثر أمانًا من بينها.

استخدم متصفح **Tor**

هذه النصيحة مفيدة إذا كنت لا تريد لحكومة أو متلصص أو فضولي أن تقوم بتعقّبك، مشروع Tor هو مشروع للتصفح الآمن والخفي وهو مجاني ومفتوح المصدر تمامًا، يعمل Tor عبر تمرير الاتصال الخاصّ بك عبر اتصال مشفّر وعبر عدّة حواسيب لمستخدمين آخرين حول العالم، مما يجعل الحكومات ومزوّد خدمة الإنترنت غير قادرًا على تعقّبك أو معرفة البيانات التي تقوم بإرسالها.
متاح هنا :

https://tb-manual.torproject.org/

استخدم إضافات وبرامج الأمان والخصوصية

يوجد العشرات من الإضافات (**add-ons**) لمتصفّحات الويب الشهيرة مثل فيرفكس وجوجل كروم (لا ننصحك باستخدام جوجل كروم، إنّه يمتلك مزايا مخفية لالتقاط الصوت والبيانات الخاصّة بك، كما أنّه مغلق المصدر، كما أنّه يرسل العديد من البيانات إلى خواديم شركة جوجل بصورة دورية) من أجل الحماية والخصوصية.
هذه هي أهمّ الإضافات التي ننصح بها:
HTTPS Everywhere: هذه الإضافة هي واحدة من أهمّ الإضافات التي يجب عليك تثبيتها، تقوم هذه الإضافة باستخدام بروتوكول **HTTPS** على المواقع التي تزورها متى ما كان ذلك ممكنًا، هناك نوعان من الاتصال: **http** و**https**،،،، ال **https** هو الأضمن ، وهو يعني أنّ الاتصال بينك وبين الموقع هو اتصال مشفّر ولن يتمكّن مزوّد الخدمة أو شخصٌ ما بمعرفة البيانات التي يتم إرسالها بينك وبين الموقع، ووظيفة هذه الإضافة هي استخدام هذا البروتوكول متى ما أمكن ذلك.
AdBlock Plus: تقوم هذه الإضافة بحجب الإعلانات والنوافذ المنبثقة التي قد تظهر لك أثناء تصفّحك، وهي إضافة شهيرة جدًا، قد تقول: وما علاقة حظر الإعلانات بالأمان والخصوصية؟ عليك أن تعلم أنّ جميع الشركات الإعلانية تقريبًا تقوم بتعقّبك وتعقّب حركاتك والمواقع التي تزورها لتقوم بتخصيص الإعلانات لك، فهي لن تظهر لك إعلانات باللغة الفرنسية في حال كنتَ من مصر، بل ستظهر لك إعلانات باللغة العربية من معلنين مصريين، ولذلك فإنّ تثبيت إضافة لمنع هذه الإعلانات يساعد بشكلٍ هائل على الحفاظ على خصوصيتك وإبقاء هويتك مجهولة.
Ghostery: مهمّة هذه الإضافة هي حجب المواقع والخدمات والسكربتات التي تقوم بتتبّعك ومحاولة جمع معلومات عن هويتك تلقائيًا، العديد من المواقع التي تزورها تقوم بمحاولة تشغيل سكربتات **Scripts** (شفرات برمجية يتم تنفيذها على متصفحك) لتقوم بتتبعك وأخذ معلومات عنك، وظيفة هذه الإضافة هي حجب هذه السكربتات والمواقع والخدمات تلقائيًا، ويمكنك التحكم في خياراتها إن أردت.
WOT: باختصار شديد تقوم هذه الإضافة بإخبارك عن المواقع المشبوهة والتي تحتوي على برمجيات خبيثة وتقوم بإخبارك كذلك عن المواقع الآمنة، تعتبر هذه الإضافة مفيدة أثناء تصفّحك لمواقع مجهولة لأوّل مرّة.
طبعًا هناك العديد من الأدوات الأخرى التي يمكنك استخدامها للحماية من الفيروسات والبرمجيات الخبيثة (على نظام ويندوز)، هناك العديد من الخيارات التي يمكنك استخدامها لاختيار برنامج مضاد الفيروسات الخاصّ بك، ولكننا ننصحك بـ **Bitdefender** أو **Avira** أو **KasperSky** ، هذه البرامج هي البرامج الأنجح وفق اختبارات الأمان والأداء التي تمّ إجراءها على العديد من مواقع اختبارات الحماية الشهيرة.
يمكنك كذلك استخدام أدوات مخصصة لإزالة البرمجيات الخبيثة (**Malware**) مثل **Malicious Software Removal Tool** من شركة مايكروسوفت و**Spybot**.