الاختراق الإلكتروني في الفضاء السيبراني و أفضل الطرق للحماية منه

الباحث : أوراغ كريم

باحث دكتوراه فلسفة في إدارة الأمن السيبراني – الجزائر

aouragh.karim@yahoo.com

الملخص:

نظراً لانتشار الشبكات الحاسوبية واعتماد المؤسسات العامة والخاصة على كفاءتها وجودة عملها، فإن أي توقف لها أو تخريب فيها قد يؤدي إلى خسائر عظيمة وتعطيل لخدمات المواطنين، وبانتشار القراصنة والأخطار وإساءة الاستخدام، أصبح التحدي الأساسي في يومنا هذا في مجال أمن الشبكات هو مواكبة جميع أنماط التهديدات التي هي في مرحلة تطور وتزايد مستمر بشكل يومي وذلك من أجل تأمين الحل الأفضل لحماية أي منظومة . هنالك العديد من آليات الحماية التقليدية ، لكن هذه الحلول لا تؤمن كشف الهجومات الجديدة ، لذلك نحن بحاجة إلى حلول أكثر فعالية. في هذا المقال نقوم بدارسة الاختراق الالكتروني في الفضاء السيبراني و أفضل الطرق للحماية منه.

الكلمات المفتاحية: الاختراق الالكتروني، السيبراني، أمن الشبكات.

Abstract:

Due to the protection of computer networks and the reliance of public institutions on their efficiency and quality of work ، any interruption or vandalism may lead to great losses and disrupt citizens services، with the spread of hackers، dangers and misuse the main challenge today in the field of network security has become keeping up with all types of threats that are in order to provide the best solution to protect any system ، there are many traditional protection mechanisms، but these solutions don’t ensure the detection of new attacks، so we need more effective solution. in this article، we study the electronic penetration in cyberspace and the best ways to be protected from it.

Key words: hacking، electronic، cyberspace، security، networks.

1. مقدمة:

بالرغم من المزايا التي تحققت ولا تزال تتحقق كل يوم بفضل التطور الهائل في المجال الالكتروني على جميع الأصعدة في شتى مجالات الحياة المعاصرة، لدرجة حتى أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الحاسب الآلي بالدور الأول حيث أصبح العلم قرية صغيرة تربطها شبكات المعلومات[1].

و في هذا العصر اعتمدت المؤسسات في تسيير أعمالها على تقنية المعلومات التي أثبتت أنها تسهم في إنجاز الأعمال بسرعة عالية وبدقة متناهية.وحيث أن البيانات والمعلومات تخزن في مخازن معلومات مربوطة مع حاسبات المؤسسة من خلال شبكة الاتصال وغالبا ما تكون متاحة عبر شبكة الانترنت تسهيلا لإجراءات العمل واختصارا للوقت.

ولهذا تطورت طرق معالجة البيانات للتوافق مع بيئة الحاسبات من طرق يدوية إلى طرق آلية منتجة نظم سير العمل الإلكترونية لتصل إلى مفهوم الحكومة الإلكترونية، وبذلك نجد أن تقنية المعلومات قد ساهمت في تسهيل الأعمال الطبية والهندسية والصناعية والمصرفية وأنظمة المكتبات وأعمال المؤسسات التعليمية بل إنها أصبحت سلاحا في المؤسسات العسكرية يستخدم في الأعمال الحربية.

إن هذه الشبكات تحتاج إلى حماية تضمن سلامة محتوياتها واستمرارية عملها .حيث وصل الأمر إلى أن الأعمال تتوقف في المؤسسات إذا تعطلت شبكات معلوماتها كشركات الطيران والشركات الكبيرة المنتشرة حول العالم بل إن التوقف القصير لتلك الشبكات يكبد أصحابها أو المستفيدون منها خسائر فادحة، وإن التوقف القصير لشبكات المعلومات الحكومية والوطنية يؤدي إلى تعطيل أعمالها مما ينعكس على انخفاض مستوى الخدمات المقدمة للمواطنين وإرباك في مؤسسات الدولة ذات العلاقة بالشبكات المتعطلة .وتوقف شبكات المؤسسات التجارية يسبب خسائر مالية كبيرة قد تؤدي في كثير من الأحيان إلى الإفلاس، وغدت جودة الأعمال ونجاحها يعتمدان على جودة وأداء شبكات الاتصال واستمرارية عمل قواعد البيانات.

أصبحت قضية أمن الشبكات تمثل حجر الأساس في بناء أي منظومة شبكية مهما كان حجمها وذلك بسبب تزايد وتنوع التهديدات الجديدة كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، والتي نجدها دائما في حالة من التطور والتقدم السريع، ولمواجهة هذه التهديدات نحتاج إلى حلول أمنية متطورة والتي لم تعد متوفرة عبر طرق الحماية التقليدية، مما شكل تحدي أساسي في تأمين الحماية اللازمة لأي منظومة شبكية.

إشكالية البحث:

من خلال ما سبق تتضح الإشكالية الرئيسية للبحث وهي:

ماهي الآليات و الاحتياطات الحديثة التي يجب اتخاذها للحماية من الاختراق الالكتروني؟

وتندرج ضمن هذه الإشكالية الرئيسية مجموعة من الأسئلة الفرعية تتمثل أساسا في:

- ماهي الأشياء التي تساعد على الاختراق الالكتروني؟
- ما هي التهديدات الرئيسة للشبكات؟
- ما هي الطرق المستخدمة لاختراق الحسابات؟

أهمية البحث:

تأتي أهمية هذه الورقة البحثية الموسومة ب "**الاختراق الإلكتروني في الفضاء السيبراني و أفضل الطرق للحماية منه**" من أهمية موضوع الفضاء السيبراني الافتراضي ومختلف الهجمات السيبرانية التي يتلقاها الفضاء الالكتروني والتي أصبحت اليوم المهدد الأول لأمن المعلومات، خاصة وان جل المجتمعات الحديثة أصبحت تعتمد بشكل متنامي على التكنولوجيات مما باتت القرصنة الالكترونية تهدد أمن الإنسان.

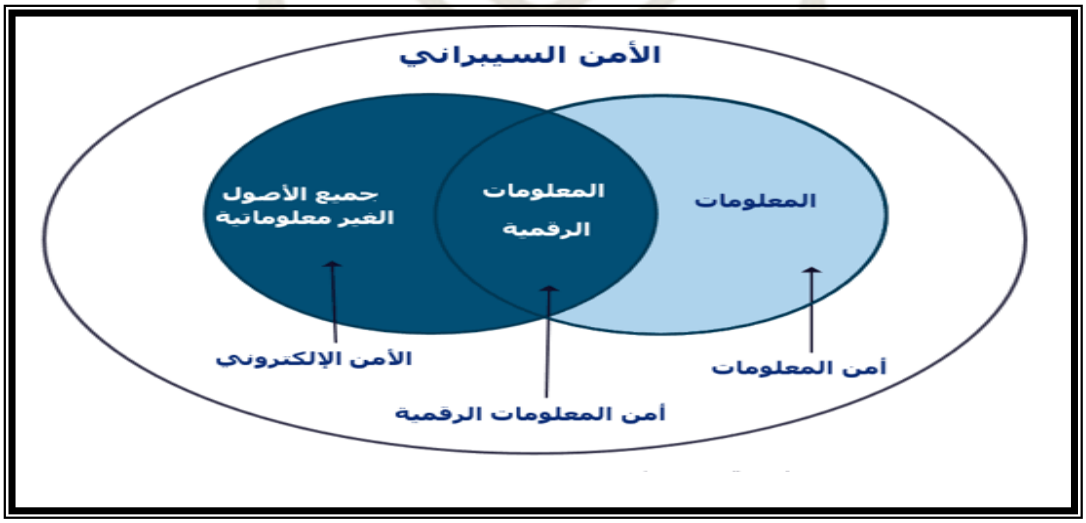
أهداف البحث:

- التعرف على الإختراق الإلكتروني في الفضاء السيبراني.
- التعرف على الهجمات الرئيسة.
- التعرف على برامج التجسس.
- التعرف على الاحتياطات الحديثة التي يجب اتخاذها للحماية من الاختراق.

2. الفضاء السيبراني

الفضاء السيبراني مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنيت وكم هائل من البيانات والمعلومات والأجهزة، كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[2]، وهناك من يرى أنه البعد الخامس للحرب، وهذا التعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الأخرى. كما عرَفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) "على أنه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية [3] "، وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري، والذي يعد جزءا أساسيا في فهم الفضاء السيبراني.كما يمكن الاعتماد على تعريف الاتحاد الدولي للاتصالات الذي يصف الفضاء السيبراني" بأنه المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي : أجهزة الكمبيوتر ، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدموا كل هذه العناصر[4] ".

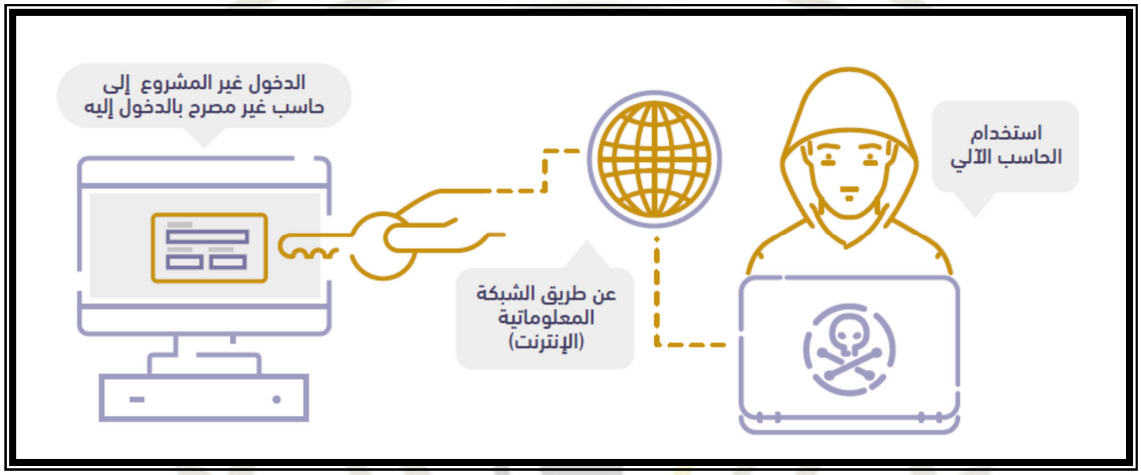
وعليه يمكننا القول بأن: الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين وتجدر الإشارة إلى أن مسألة تحديد مفهوم" الفضاء السيبراني"، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.



الشكل 1: مكونات الفضاء السيبراني.

1.2. اختراق الشبكات (Hacking):

هو محاولة الدخول إلى جهاز عضو في شبكة حاسب آلي من قبل شخص غير مصرح له بالدخول إلى ذلك الجهاز أو تلك الشبكة وذلك بغرض الإطلاع أو السرقة البيانات و المعلومات أو التخريب أو التعطيل أو زرع الفيروسات أو تدميرها.



الشكل2: الاختراق الإلكتروني.

2.2. تعريف الهاكرز " Hackers " :

أطلقت هذه الكلمة أول ما أطلقت في الستينيات لتشير إلي المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودراية حيث أنهم كانوا يقدمون حلولا لمشاكل البرمجة بشكل تطوعي في الغالب [5]. وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت بقصد الانتقام أو الابتزاز.

3. التهديدات الرئيسة للشبكات (Primary Network Threats):

1.3. تهديدات غير منظمة:

تتضمن بشكل رئيس أفراد غير متوقعين يستخدمون أدوات قرصنة سهلة تتوفر على شبكة الانترنت في مواقع كثيرة كأدوات كسر كلمات المرور (password crackers) والنصوص المغلفة (shell scripts)، مع أن التهديدات غير المنظمة يمكن أن تحصل عند تشغيل أدوات القرصنة السهلة فإنها تظل مصدر خطر يمكن أن يؤذي الشبكة المعتدى عليها بأضرار خطيرة تزيد بازدياد مهارة هؤلاء الأفراد وقوة الأدوات المستخدمة. فعند اختراق موقع منظمة ما على الانترنت يكون ركن السلامة أحد أركان الحماية الأمنية غير محققاً، وحتى لو كان الموقع المخترق محمياً من الشبكات الخارجية بجدار حماية فعال فإن مصداقية المنظمة تنخفض لدى الأطراف الأخرى ويعدّون ذلك الموقع بيئة غير آمنة وبالتالي تتأثر أعمال المنظمة سلباً، ويكون الأثر أكثر سلبية إذا كان الموقع خاص بجهات وطنية دفاعية متصلة بقواعد بيانات عسكرية أو أمنية.

2.3. تهديدات منظمة:

تأتي من قراصنة مندفعين بشدة يحفزهم التنافس التقني، يعرفون ثغرات نظم التشغيل ويمكنهم فهم النصوص البرمجية والشفرات واستغلالها. يفهمون ويطورون ويستخدمون تقنيات القرصنة المعقدة في اختراق مواقع الشركات والمؤسسات غير المحمية عن جهل وقلة خبرة. هذه المجموعة من القراصنة غالباً ما تكون متورطة في معظم قضايا الاحتيال والسرقة التي يتم إخبار الجهات الأمنية عنها.

3.3. الهجمات الرئيسة:

بوجود العديد من نقاط الضعف تكون الشبكة معرضة للكثير من الهجمات ويتوفر ثلاثة أنواع رئيسة من الهجمات هي الاستطلاع والتنصت ورفض الخدمة.

أ. الاستطلاع (Reconnaissance):

يقصد بالاستطلاع هنا جمع المعلومات بدون إذن أو تخويل، بقصد استكشاف شبكة منظمة ما ورسم مخططها ومعرفة الخدمات المستخدمة فيها واستنتاج نقاط ضعفها، وقد يرِد مصطلح الاستطلاع أحياناً باسم جمع المعلومات،

وفي معظم الحالات تقود هذه العملية إلى تمكين الوصول غير المرخص ومن ثم تنفيذ هجمة رفض الخدمة. ويتم ذلك غالبا على مرحلتين بالشكل التالي:

المرحلة الأولى: يقوم القرصان الماكر بتنفيذ أوامر متعددة لكشف العناوين النشطة كالأمر (ping) بمسح جميع مكونات شبكة الضحية، ونتيجة هذه المرحلة تسجيل قائمة بالعناوين تدل كل منها على جهاز يقوم بخدمة أو مجموعة من الخدمات.

المرحلة الثانية: يستخدم القرصان أداة لمسح المنافذ ليستنتج المنافذ المفتوحة والخدمات العاملة في العناوين المستنتجة في المرحلة الأولى. ونتيجة هذه المرحلة تكون تحديد الخدمات والوظائف وبتوفيق العناوين والمنافذ يتوصل القرصان إلى معرفة التطبيقات المستخدمة وأنواعها وأسماء أنظمة التشغيل وإصداراتها التي تشغل حاسبات الشبكة الضحية. واعتماداً على هذه النتائج يقرر القرصان فيما إذا كانت نقاط الضعف قابلة للاستغلال أم لا. والاستطلاع يشبه تصرف السارق حينما يستكشف المبنى المراد سرقته فيدور حوله باحثاً عن نافذة مفتوحة أو نافذة سهلة الفتح أو باب مفتوح أو باب خلفي سهل الفتح أو نقطة ضعف في نظام الأقفال وغير ذلك.

ويستخدِم القرصان على سبيل المثال أداة (NSLOOKUP) و أداة (WHOIS) لتحديد عناوين بروتوكولات الانترنت المسجلة للمنظمة الضحية. ثم يستخدم أداة (PING) ليقرر أية عناوين قيد التشغيل.

ب. التنصت (Eavesdropping)**:**

يُعرف التنصت بعبارات شائعة مثل استطلاع الشبكات واكتشاف الحُزم. يمكن أن يستخدم التنصت لاكتشاف الهجمات على الشبكات. ومن الأمثلة على البيانات القابلة للتأثر بالتنصت النسخة الأولى من بروتوكول (SNMP) الذي يرسل نص التعريف (Community string) بالنص الواضح غير المشفر، ويستطيع القرصان الماكر تشغيل أدوات تنصت على بروتوكول (SNMP) وجمع معلومات قيّمة عن معدات الشبكة وطرق إعداد كل منها. ومن البروتوكولات التي تقبل التصنت بروتوكول (TCP/IP) حيث يتم مراقبة الحُزم والتقاط كلمات المرور وأسماء المستخدمين عند مرورها بالشبكة وبيانات بطاقات الائتمان والبيانات الشخصية وكثير من البيانات المختلفة التي تقود لتسهيل الوصول إلى الشبكة الضحية ودخول أجهزة الخادم المتوفرة فيها.

والأدوات المستخدمة لتنفيذ التصنت تتضمن برامج تحليل الشبكات وبروتوكولاتها بالإضافة إلى أدوات التقاط الحُزم على شبكات الحاسب.

أما الطرق المستخدمة للحماية من هجمات التصنت فتتلخص بإصدار سياسة تقود إلى منع استخدام بروتوكولات قابلة للاختراق من قبل هجمات التنصت، واستخدام تشفير يتوافق مع متطلبات الحماية في المنظمة بحيث لا يُنقِص كفاءة موارد النظام أو رِضا المستفيدين.

ج. هجمة رفض الخدمة:

يتم في هذا النوع من الهجمات إرسال عدد كبير من الحزم من الشبكة الخارجية (عادة الانترنت) إلى الشبكة الداخلية (عادة خادم الويب) مما يؤدي إلى إيقاف خدمة الويب وبالتالي عدم استطاعة المستفيدين من تصفح موقع المنظمة المستهدفة، وغالباً ما يتم إرسال تلك الحزم من عدد كبير من الحاسبات من مواقع جغرافية مختلفة لتضييع مصدر الهجوم.

الشكل3: بعض إحصائيات الهجمات الالكترونية لعام 2020.

4.3. برامج التجسس [6]:

يستطيع الهاكر الدخول إلى جهاز الضحية عن طريق أستخدام بعض البرامج التي تساعده على الأختراق و من أشهرها:

1. **Web Cracker 4**
2. **Net Buster**
3. **Net Bus Haxporg**
4. **Net Bus 1.7**
5. **Girl Friend**
6. **BusScong**
7. **BO Client and Server**
8. **Hackers Utility**

ويوجد بعض البرامج الحديثة لا تُرى من قبل برامج الحماية من الفيروسات مثل:

1. **BEAST**
2. **CIA122b**
3. **OptixPro**
4. **NOVA**

4. النتائج:

ان البحث و الدارسة التي سباق استعراضها تشير إلى أن للاختراق مخاطر عديدة :

1- إتلاف المعلومات أو تعديلها: ويقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنيت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد آو خرائط سرية.

2- التجسس على الشبكات: ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، والهدف منه الحصول على معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلبا على مهام الخصم.

3- تدمير المعلومات: ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه" تهديد لسلامة المحتوى "ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

4- تهديد أمن وسلامة الدولة.

5- انتهاك حقوق التأليف.

الشكل4 يوضح تأثير الهجمات الالكترونية لعام 2020.

5. نقاش:

وفيما يلي نستعرض أهم الاحتياطات الحديثة التي يجب اتخاذها للحماية من الاختراق:

1- استخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي.

2- التأكد من تحديث Anti-Virus كل أسبوع على الأقل (شركة نورتون تطرح تحديث كل يوم أو يومين) .

3- التأكد أن وضع Anti-Virus جيد.

4- لا تظل مدة طويلة متصل بالشبكة بحيث لو قام بالدخول عليك أحد لن يستطيع أن يخرب في جهازك.

5- لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاماً وصوراً لا أخلاقية لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع.

6- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا.

7- عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (Win.exe) أو أن تكون ملفات من ذوي الامتدادين مثل (MBM.pif.jpg) أو (bat. أو dll.أو com.) وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبب الأذى والمشاكل لك.

8- عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية.

9- قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري.

10- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق.

11- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.

12- لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره.

13- قم بمسح cookies أول بأول من جهازك هي عبارة عن ملفات يرسلها الموقع لمتصفحك و هي عبارة عن ملف مكتوب لا يستطيع أي موقع قراءته غير هذا الموقع و قد يكون به كلمات سر موقع أو اشتراك، وهي مزعجه في بعض الأحيان حيث أنها تسجل كل المواقع التي دخلتها و كل الصفحات التي شاهدتها و مدة مشاهدة كل صفحه ويمكن مسح الكوكيز عن طريق الذهاب المجلد الخاص بها و حذف الملفات التي به C:\WINDOWS\Cookies و حذف الملفات التي توجد داخل هذا المجلد أو من قائمة Start نختار Run ونكتب فيها Cookies ثم OK ستظهر نافذة نمحو كل ما فيها.

14- لا تخزن كلمات المرور أو كلمات سر على جهازك مثل كلمة المرور لاشتراكك في الانترنت أو البريد الكتروني.

15- إذا لاحظت حدوث أي شيء غريب مثل خلل في أي برامج أو خروج و دخول السي دي افصل الاتصال بالانترنت فورا و تأكد من نظافة الجهاز.

16- لا تدخل بريدك أو أيّ من معلوماتك الخاصة من مقاهي الانترنت نهائيا فهناك برامج تعمل بشكل مخفي تحفظ جميع النماذج التي تقوم بتعبئتها دون أن تشعر.

17- غيّر كلمات مرورك بين فترة وأخرى وينصح أن تكون الكلمة مكونة من حروف وأرقام كثيرة يصعب تخمينها، لأن هناك برامج تقوم بتجريب الآلاف من كلمات المرور وتعمل مسح على مدار الساعة فيدخل المخترق اسم المستخدم للبرنامج ويطلب منه تخمين كلمة المرور، فإذا كانت كلمة المرور سهلة مثل هذه 12105 فسوف يحصل عليها في وقت قياسي، ولكن إذا كانت كلمة المرور صعبة مثل gfhym38*ui#j9?@%$*87 فسوف يكون من الصعب جدا أن يكتشفها البرنامج بالتخمين وتزداد الصعوبة أكثر إذا أضيف في كلمة المرور أحرف أخرى باللغة العربية في المواقع التي تسمح بذلك.

18- لا تستخدم كلمة مرور موحّدة بل اجعل كلمة مرور بريدك تختلف عن معرفك بالساحة وأيضا تختلف عن معرفك في المنتديات الأخرى ولو استطعت أن تجعل لكل منتدى أو بريد كلمة مرور مختلفة فافعل، وضع جدولا لكلمات المرور على مكتبك وليس في جهازك.

19- احذر من مواقع الكراكات والمواقع غير الموثوقة ففيها برامج يتم تحميلها في الخلفية أثناء تصفح الموقع وهي تتحدّث بشكل مستمر وأحيانا تفشل برامج Anti-Virus في مقاومتها أو القضاء عليها ، وكذلك عند تركيب كراك لبرنامج فكثير من هذه الكراكات يحتوي على باتش يمكن أن يكون عند تشغيله ثغرة خطيرة في جهازك.

20- للعلم مواقع المراسلة التي ظهرت مؤخرا وشارك فيها كثير من الأعضاء من السهل جدا جدا للعاملين بتلك المواقع الاطلاع على محتويات الرسائل الموجودة بها، ولذا إذا استخدمتها فكن على حذر فالرسائل الواردة إليك والمرسلة منك عن طريقها مكشوفة بنسبة 100% .

21- على أسوأ الاحتمالات لا تترك بيانات أو ملفات أو مستندات خاصة بك في بريدك الالكتروني بل بادر بمسحها أو الاحتفاظ بها في جهازك وأيضا يفضّل أن تحفظ ملفاتك الشخصية الخاصة والتي لا ترغب أن يطّلع عليها أحد في فلاش ديسك أو هارديسك خارجي وتقوم بفصلها عند الاتصال بالانترنت.

22- "ما يقوله Google صحيح" فإذا قمت بعمل بحث على موقع ووجدت Google يحذرك من هذا الموقع لا تدخل على هذا الموقع لأنه قد يضر بجهازك فقد يحتوى على برمجيات خبيثة وسوف تنزل على جهازك من دون أن تشعر وسوف تكون بذلك ضحية لأي هاكر.

23- انصح كل عضو أن يكون له ثلاثة ايميلات واحد منها مخصص للشبكة و يفضل أن يكون على الجي ميل حتى لا يستخدم في الماسينجرات و أيميل أخر للماسينجر و أيميل للمراسلات الخاصة حتى أن تم سرقة باسورد أيميل الماسينجر لا يكون هناك ضرر معين و أن يكون الايميل المخصص للشبكة بأي اسم غير اسمك الحقيقي.

24- جميع الأجهزة المتصلة بالشبكة عرضة للإصابة بالفيروسات في حالة مشاركة الملفات فيما بينها أو في حالة مشاركة الاتصال بالإنترنت بينها. لذلك يجب تعطيل وظيفة تبادل الملفات والطابعات وتفعيل الدخول إلى الجهاز بكلمة سر حتى يتم تجنب المخاطر إلى حد كبير.

25- المتصفح الذى تقوم بأستخدامه سواء Internet Explorer أو Fire Fox أو غيره .... لابد أن يكون أحدث نسخة موجودة.

26- تفريغ قائمة my recent document لأنها أول ما يلهث إليه لص المعلومات هو آخر ملفات تعاملت معها مؤخراً وما بها من معلومات فيبحث عنها على القائمة سالفة الذكر.

6. الاستنتاجات:

أصبح الإنترنت يستخدم ويعتمد عليه بشكل هائل وبما يحمله من ملايين الإتصالات، أصبح يشكل تهديد جدي لسلامة البيانات التي تنساب في الشبكات إن معرفة سُبل حماية خصوصية معلوماتك وأجهزتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع، والذي يلحق الضرر بك مادياً أو معنوياً

7. المراجع:

[1] الفيروز آبادي، القاموس المحيط ، مؤسسة الرسالة دار الريان للتراث، (بيروت، 1987 ط2) ص1219.

[2] عباس بدران، الحروب الالكترونية :الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية، بيروت، 2010، ص4.

[3] Olivier KEMPF، Introduction à la Cyberstratégie، Paris، Economica، 2012، P 9.

[4] The International Télécommunication Union، ITU Toolkit for CybercrimeLégislation، Geneva، 2010، P 12.

[5] https://www.alarabimag.com/download/1982-pdf

[6] https://books-library.online/file