طريقك للأمن المعلوماتي

المهندس مسلم العيداني

//////////////////////

/

طريقك للأمن ألمعلوماتي

//////////////////////////

اسم الكتاب :طريقك للأمن ألمعلوماتي

تأليف

مسلم ألعيداني

مطور ومدير مواقع الكترونية

طريقك للأمن ألمعلوماتي

تأليف

مسلم العيداني

المحتويات

تنويه وإخلاء مسؤولية : أقدم لك المعلومات المذكورة في الكتاب لأغراض تعليمية فقط (الاختراق الأخلاقي) ولا أتحمل مسؤولية استعمال أو سوء استغلال معلومات الكتاب في أغراض غير قانونية و أي استخدام غير قانوني يتم على مسؤوليتك الشخصية ..

تعلمت الشر لا للشر لكن لتوقيه

ومن لم يعرف الشر من الناس يقع فيه

كلمة المؤلف :

بدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية

وازدهرت مع بداية الثمانينيات من القرن العشرين وخصوصا عام 1981 مع ظهور أول حاسب شخصي من قبل شركة آي بي أم

التي أوصلت الكمبيوتر إلى حجم
يمكنك من وضعه في منزلك
وتسميته (حاسبا شخصيا) بعد أن
كان حجمه يشغل غرفة كبيرة جدا او
حتى مبان بأكملها ومع الزيادة بعدد
مستخدمين الانترنت ازداد الاختراق
وأساليبه بشكل هائل ادى الى ظهور
مجموعة مختلفة ومميزة من
مستخدمي الحاسب اطلق عليهم ب
"الهاكر" لذا أصبح من المهم فهم
الكيفية والآلية التي يفكر فيها الهاكر
أو طرق اختراقه ومعرفة ما هي
الاهداف التي ادت به للاختراق

لكي نحمي بياناتنا ومعلوماتنا من الاختراق .

طريقك للأمن ألمعلوماتي ...

من هو الـهاكر ؟

الـهاكر عبارة عن مجموعة مبرمجين وأشخاص محترفين

يمكنهم اختراق الأنظمة بطريقة غير قانونية.

تتعدد أهداف اختراقاتهم فمنهم من دفعة حب التعلم وكسب المعلومات او المتعة والشهرة للاختراق..

** سئل احد المجرمين لماذا سطوت على البنك أجاب لان المال موجود هناك المال اليوم هو المعلومات ولقد تعلم الهاكر اليوم مكان وجود المال ويمكنهم سرقة كميات كبيرة وبمخاطرة أقل بكثير من الجرائم التقليدية ..

أنواع الهاكر :


BLACK HAT
GREY HAT
WHITE HAT

1- القبعات البيضاء (White Hats) أو القراصنة الأخلاقيين :

ويعملون في المؤسسات الحكومية وشركات أمن المعلومات ويطلق عليهم ب المحللين الأمنيين (Security analysts)

أو يعملون حتى منفردين
لاكتشاف ثغرات البرامج
والأجهزة والشبكات والبحث عن
المشاكل الأمنية والإبلاغ عنها من
أجل سدها ومنع استغلالها من
قبل المخترقين المجرمين .

وهم لا يستغلون هذه المعلومات من
اجل هدف شخصي فمعظم الشركات
يمتلكون محللين امنين من اجل
حماية أنظمتهم ضد الهجمات
المختلفة .

2-القراصنة المجرمين - القبعات السود(Black Hats)

ويعرفون أيضا باسم كراكر (Cracker) هؤلاء يخترقون أمن الحاسوب من أجل مكاسب شخصية مثل سرقة بيانات بطاقات الائتمان أو البيانات الشخصية من أجل بيعها أو حتى من أجل المتعة الذاتية..

3-أصحاب القبعات الرمادية(Grey hats)

وهم القراصنة الذين يقعون بين الهاكر الأخلاقي والهاكر المجرم فهم

يخترقون أحيانا ويقدمون
المساعدات الأمنية أحيانا أخرى .

**الفرق بين المرأة والكمبيوتر أنه
إذا أخطأ لا يلقي باللوم على الزوج

أنيس منصور (كاتب صحفي
وفيلسوف وأديب مصري)

الاختراق الأخلاقي -------

الهاكر الأخلاقي (ethical hacking)

الهاكر الأخلاقي أو ذو القبعة البيضاء (White Hat-Hacker) اختراق يهدف لزيادة الأمن الالكتروني ويستخدم في

الشركات لتحديد نقاط الضعف والثغرات في شبكاتها وأنظمتها لتقوم باغلاق هذه الثغرات وتطوير أنظمتها لتجنب هجمات الهاكر على النظام لكون منفذ هجوم الهاكر الاخلاقي يستخدم نفس الأدوات التي يستخدمها الهاكر ذو القبعة السوداء (Black Hat-Hacker) ولكن الاختلاف يكمن بكون اختراقة قانوني وشرعي .

توجد العديد من الشهادات ترخص للشخص العمل كمخترق أخلاقي او تمنحة معلومات مهمة كمواطن الضعف في أنظمة الحاسوب

والشبكات التي قد تكون عرضة لعمليات اخترق غير أخلاقية يمكنك الحصول على شهادة الهاكر الاخلاقي Certified (Ethical Hacker) CEH من خلال اجتياز امتحان يتألف من 125 سؤالاً وتكون مدة الامتحان 4 ساعات (2)


Certification Number
C|EH
Certified Ethical Hacker
This is to acknowledge that
has successfully completed all requirements and criteria for
certification through examination administered by EC-Council
Issue Date:
Expiry Date:
ANSI
EC-Council
Sanjay Bavisi, President
SAMPLE

مراحل الاختراق :

المرحلة الأولى/ مرحلة الاستطلاع (Reconnaissance) .

او ما تسمى (المرحلة التحضيرية) وهي مرحلة جمع المعلومات عن الهدف مثل المعلومات الشخصية كالأسماء والعناوين و أرقام الهواتف إلخ ... قبل بدأ عملية الاختراق وكلما جمعت معلومات أكثر عن الهدف كلما كانت عملية الإختراق أسهل و أسرع

وتكون الهندسة الاجتماعية هي الجزء الاهم من هذه المرحلة .

المرحلة الثانية/ مرحلة المسح (Scanning & Enumeration)

وهي تتمثل في عملية المسح أو الفحص التي يقوم بها الهاكر قبل الهجوم على مستوى الشبكة للحصول على معلومات محددة على أساس المعلومات اللي توفرت لديه من عملية الاستطلاع وسبب استخدام المسح لإيجاد ثغرة للبدء بالاختراق

المرحلة الثالثة/ تحقيق الدخول إلى النظام (Gaining Access) .

هذه المرحلة هي مرحلة الاختراق فالمخترق يستغل الثغرات التي وجدها بمرحلة الفحص واستغل هذا الضعف في النظام جيدا في مرحلة الاختراق

المرحلة الرابعة/ تثبيت الاختراق أو مفهوم تامين الوصول والدخول مجددا على النظام (Maintaining Access)

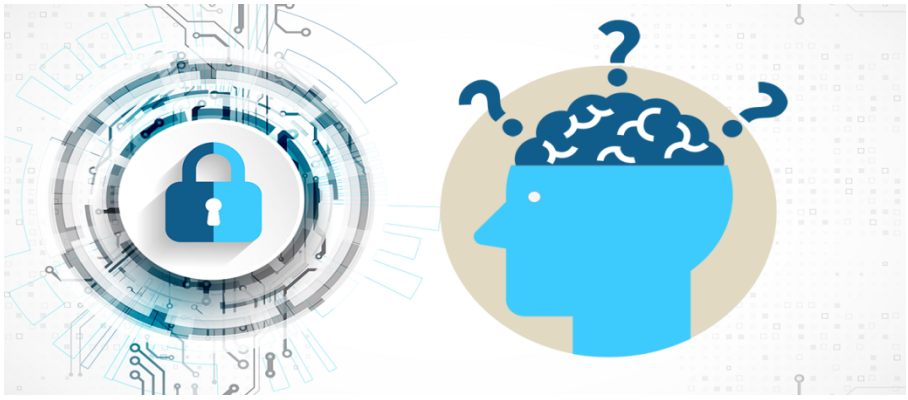
في هذه المرحلة يقوم الهاكر بترك منافذ في النظام المخترق لكي يتمكن من الولوج إليه مرة أخرى وذلك عن طريق زرع برامج خبيثة مثل الأبواب الخلفية # Backdoors أو ال Rootkits أو ال # Trojans و التي تمكنه من رفع و تحميل الملفات و التعامل مع التطبيقات أو المعلومات في النظام المخترق مباشرة كي لا نكرر الخطوات السابقة مستقبلا للعودة إلى النظام

المرحلة الأخيرة/ مسح آثار الإختراق Covering Tracks .

ازالة اثر الاختراق -clearing tracks- هذه هي المرحلة الأخيرة في الاختراق حيث يقوم الهاكر بإزالة جميع الأنشطة التي قام بها على النظام الذي أخترقه بداية من عملية الاستطلاع المباشر وصولا إلى الخروج من الشبكة وذلك ليضمن عدم كشفه من قبل

مسئولي الحماية و ليترك المجال مرة أخرى للولوج في هذا النظام ولكي يبقى على النظام طويلا

الاختراق من خلال الهندسة الاجتماعية ..



تعد من ضمن المراحل الاولى في الاختراق وجمع المعلومات وتستخدم في الحصول على المعلومات الحساسة أو إقناع الضحايا المستهدفة بتنفيذ بعض الإجراءات

التي تساعد على اختراق أنظمتهم والإضرار بها.

مثلاً أن تقوم بإقناعه بأنك أدمن أو مسؤول في شركة جميل ومطلوب منك التحقق او التأكد من الشخص الذي يستخدم الاميل هو له ام قام شخص ما باختراقه واعطاءه رابط صفحة مزوره [Phishing Emails] لدخول منها وتسجيل الاميل والباسوورد الخاص به.

وكما تعرفها الموسوعة الحرة (الهندسة الاجتماعية عبارة عن مجموعة من التقنيات المستخدمة

لجعل الناس يقومون بعمل ما أو يفصحون عن معلومات سرية وشخصية حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة والتي قد يظن الضحية أنها تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو فتاة جميلة على مواقع التواصل الاجتماعي أو ذات عمل يسمح له بطرح هكذا أسئلة دون إثارة الشبهات) ولهذا السبب يصبح من المهم للغاية معرفة أنواع الحيل والخدع المستخدمة في هذا الأمر وكيفية الوقاية منها .

أنواع الاختراق :

للاختراق أنواع وطرق كثيرة ولكن سوف يكون شرحنا مقتصر على الأنواع الثلاث الرئيسية التالية :

1-طريقة إِختراق المواقع والسيرفرات.

من المعروف أن جميع المواقع
مبنية على لغات البرمجة الخاصة
بالشبكة ألعنكبوتيه والانترنت ..
ومن هذه اللغات PHP HTML
JAVA PERL ومع وجود
الثغرات البرمجية في هذه البرامج

والأنظمة المعدة والمبنية عليها المواقع والسير فرات يأتي دور المخترقين في اكتشاف هذه الثغرات كما تسمى وترجمتها لخدمتهم في الوصول الى الملفات الرئيسية ويتم إكتشاف هذه الثغرات الأمنية عن طريق برامج خاصة في البحث عن الثغرات

ومن أهم هذه الثغرات التي يتم إكتشافها

- ثغرات الـ **XSS** وتعتمد على سحب كلمات السر من **ADMIN** الموقع .

- ثغرات الـ SQL وهي قليلة الإستخدام وتعتمد على الأخطاء في قاعدة البيانات في المواقع والسيرفرات والمنتديات .

2-طريقة اختراق الشبكات اللاسلكية :

الشبكات اللاسلكية ببساطة هي الشبكات التي لا تستخدم أي نوع من الكابلات في عملية الاتصال وهي نظام اتصالات للبيانات

data communicating system

تستخدم التردد الراديوي كوسط لاسلكي لعملية الاتصال وتقوم بنقل البيانات عبر الهواء لتريح وتخلص المستخدم من الأسلاك المتعددة والمعقدة فهي تستخدم الأمواج

الكهرومغناطيسية لتبادل البيانات من نقطة الى أخرى

اسم الشبكة (SSID)

تستخدم كل شبكة محلية لاسلكية (WLAN) اسم شبكة فريد لتعريف الشبكة. ويطلق على هذا الاسم معرف مجموعة الخدمات (Service Set Identifier أو SSID اختصاراً). عندما تقوم بإعداد محول WiFi تحدد اسم SSID. إذا أردت التوصيل بشبكة محلية لاسلكية (WLAN) قائمة فيجب عليك استخدام اسم تلك الشبكة إذا قمت بإعداد شبكتك المحلية اللاسلكية الخاصة فيمكنك اختيار أي اسم تريده واستخدامه على كل كمبيوتر ويجوز أن يبلغ طول الاسم 32 حرفاً وأن يضم حروفاً وأرقاماً. يتم تخصيص

SSID أو اسم الشبكة عند نقطة الوصول أو الموجه اللاسلكي.

انواع انظمة التشفير في الشبكات اللاسلكية

نظام التشفير

WEP

Wired Equivalency)
(Protocol

الخصوصية المكافئة للشبكة اللاسلكية

- نظام التشفير

WPA

الدخول المحمي لشبكة الواي فاي (WI-FI Protected Access)

- نظام التشفير WPA2

- اهم طريقة لحماية الشبكة اللاسلكية اختر كلمة مرور تتجاوز ال 15 حرف وقم بتغييرها بصورة دورية
- تفعيل فلتره عنوان ألماك
- استخدام نمط أخفاء SSID

اكتشاف الشبكات اللاسلكية

Vistumbler :

وهو برنامج بحث عن الشبكات اللاسلكية ويمكنة تتبع مسار الاكسس بوينت عن طريق جي بي اس وهو يدعم windows 10 يقوم بإيجاد الأكسس بوينت يقوم بإظهار جميع معلومات الشبكة ك mac address

ومعرف مجموعة الخدمات (Service Set Identifier أو SSID اختصاراً)

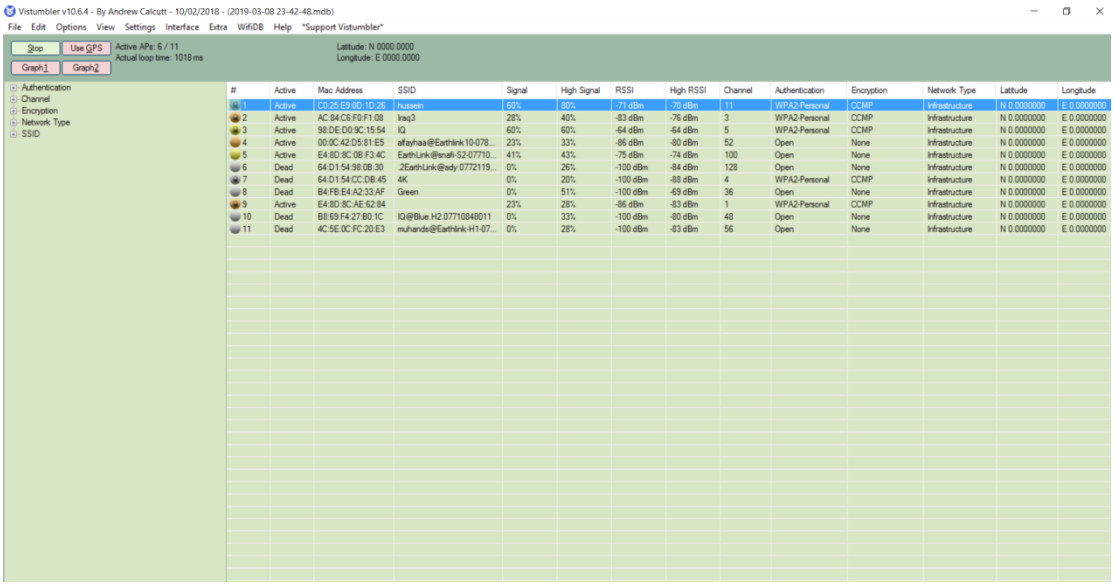
ومدى قوة الاشارة اللاسلكية لشبكة الوايفاي ونزع الحماية المستخدمة

وهو من اهم برامج جمع المعلومات عن الشبكات اللاسلكية ويقوم بمسح للشبكات اللاسلكية القريبة من موقعك

يمكنك تحميله من الموقع الرسمي للبرنامج

https://www.vistumbler.net/

بمجرد اثبيت البرنامج تظهر لك الواجهة الرسومية



في المدرسة يعلمونك الدرس ثم يختبرونك أما الحياة فتختبرك ثم تعلمك الدرس

ما يستطيع الهاكر فعلة حين اختراقك ؟

أصبح مفهوم الاختراق مفهوم متطور جدا لأبعد الحدود حيث أن البرامج الجديدة أصبحت تقدم خدمات كثيرة جدا تكاد لا تنتهي عند ظهور برنامج تلو الأخر ومنها :-

1- بامكانة سحب جميع كلمات السر لديك .

2- تسجيل مباشر لسطح المكتب لجهازك وكذلك يمكنة التقاط صورة لك او تصوير سطح مكتبك.

3- تسجيل مباشر لكل حرف تقوم الضحيه بطباعتها .

4- ايقاف تشغيل الحاسب .

5- العبث بمحتويات الملفات وحذف ونسخ واضافة ملفات جديده .

6- اجراء محادثه مباشره مع الضحية .

9- عمل عملية فورمات لإِحدى اجزاء الهارد دسك .

نظام التشغيل(Operating System)

واختصاره ((OS وهذا النظام يتكون من برمجيات تدير العتاد الخاص بالحاسوب وبرمجيات الحاسوب ويكون حلقة وصل بين المستخدم وعتاد الحاسوب

وهذه المجموعة من البرامج والمكونات الأساسية هي التي تجعل الحاسوب يعمل

ومن دون نظام التشغيل يصبح الحاسوب قطعة خردة لا قيمة له

وكما هو معلوم فان الحاسوب يتكون من أمرين:

(1) العتاد (Hardware)

(2) البرمجيات (Software)

أما العتاد فهو مثل لوحة المفاتيح-الشاشة-وحدة المعالجة المركزية((CPU-الذاكرة (RAM) وغيرها من المكونات المادية.

أما البرمجيات فهي مثل نظام ويندوز و جنو / لينكس والبرامج التي تراها أمامك مثل مايكروسوفت وورد والمواقع الالكترونية ولا يمكن إنشاء هذه البرمجيات إلا باستخدام لغات البرمجة...

أو بتعبير أكثر دقة فأي شيء مادي ملموس يوصف بالعتاد وأي شيء غير ملموس يوصف بالبرمجيات.

أهم 10 نصائح للحماية من الاختراق :

وان كانت النصيحة الأولى يجب إن تكون بتنصيب برنامج حماية من الفيروسات ولكن الفيروسات ليست التهديد الأمني الوحيد على الانترنت... حينما يكون الإنسان الحلقة الأضعف في السلسلة الأمنية يكون من المهم أن تحدث معلوماتك عن حيل وخدع الهندسة الاجتماعية من خلال اشتراكك بالمواقع والمدونات والقنوات المتخصصة في

مجال امن المعلومات لتبقى مطلعا على كل جديد وتطور ثقافتك في مجال امن المعلومات لأن ذلك يعطيك أفضلية تحتاجها لتجنب الوقوع كضحية على الإنترنت .

النصائح التالية تعد من أساسيات الحماية الواجب تعلمها .

1-عدم تنزيل إي برنامج أو العاب من مواقع غير موثوق بها ودائما قم بتنصيبها من مواقعها الأصلية .

2- إنشاء كلمة مرور قوية ومعقدة وقم بتغييرها بصورة دورية لانها تكون قابلة للاختراق وقد يبقيها

الهاكر بدون تغيير لكي يستمر بالتجسس عليك ولا تقم باستخدامها نفسها مع حساب أخر أي تجعلها نفس الكلمة للفيس بوك وللجيميل و باقي الحسابات.

3-لا تدخل إلى أي موقع من رابط تم أرسالة لك (حتى وان كان من صديقك فقد يكون قد تم اخترق حسابه وأرسل المخترق الرابط لك) بل افتح الموقع من المتصفح

4- استخدام VPN

ما هو إل VPN ؟

VPN اختصار لكلمة **Virtual Private Network** وتعني الشبكة الخاصة الافتراضية وهي طريقة لتشفير البيانات وتخطي الرقابة الالكترونية حين استخدام الحاسوب أو الهواتف الذكية و إخفاء الهوية حيث تقوم بتغيير عنوان بروتوكول الإنترنت **(IP Address)** الخاص بجهازك واستبداله بأخر وهمي مما يجعل اتصالك امن بالشبكة و يمنع مواقع الانترنت من معرفة موقعك الجغرافي عند تصفح الانترنت وتحافظ على

خصوصية بياناتك وأمنها من الاختراق والرقابة .

ولكن من مساوئ VPN عند استخدام VPN هويتك تكون معروفة لمقدم خدمة VPN الذي تستخدمه

5- حافظ على المعرفة حول احدث الاختراقات وطرق الوقاية منها.

6- راجع صلاحيات الوصول في هاتفك ولا تمنح صلاحيات الوصول ألا للتطبيقات الموثوقة بعد تحميلها من مصادرها الرسمية .

7-اخذ نسخة احتياطية للنظام

وعمل نسخة احتياطية للمعلومات الهامّة لنتمكن من استعادتها فور تعطلها ,.

8- تشغيل وإعداد خاصية الخطوتين للتحقق من تسجيل الدخول حيث تعطي هذه الخطوة أمان اكبر لحساباتك.

9- تأكد من انك قد حذفت البيانات أو الصور و الفيديوهات من هاتفك أو كمبيوترك قبل بيعة بشكل امن.

10-عدم الاحتفاظ بأية معلومات شخصية داخلَ جهازك كالرسائل الخاصة أو الصور أو الملفات المهمة وغيرها من معلوماتٍ بنكية،

مثل أرقام الحسابات أو البطاقات الائتمانية.

الجرائم الالكترونية :

مع انتقال الناس من العالم الواقعي إلى عالم افتراضي (الفضاء الالكتروني) انتقلت معها الجريمة التقليدية المعروفة وتحولت إلى

جريمة الكترونية تتصف بالتعقيد يرتكبها مجرمون فائقوا الذكاء ومع الزيادة الكبيرة بعدد مستخدمين الانترنت زادت نسبة الجرائم الالكترونية .

فالجرائم الالكترونية أما تستخدم الحاسوب كأداة لها لتنفيذ الاختراق او يكون الحاسوب ضحية لهذا الاختراق وتتكون الجريمة الإلكترونية (cyber crimes) من مقطعين هما

الإلكترونية (cyber)

صفة لأي شيء مرتبط ب الحواسيب أو تكنولوجيا المعلومات(

Information (Technology) .

و # الجريمة ((crime

أما الجريمة فهي"فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا" (3)

بعض تسميات الجرائم الإلكترونية :

1- جرائم الإنترنت

Computer Crime

2-جرائم التقنية العالية.-Hi-tech Crime

3-الجريمة السايبرية Cyber Crime

خصائص الجرائم الإلكترونية :

1-سرعة تنفيذ الجرائم الالكترونية فهي لا تتطلب بتنفيذها وقت كبير بمجرد ضغطة على لوحة المفاتيح من أي جهاز كمبيوتر تمكن المجرم

من نقل الاف الدولارات من مكان لاخر.

2- عابرة للحدود : يتم التنفيذ لهذه الجريمة عن بعد فهي بذلك لا تعترف بالجغرافيا و هدمت بذلك مبدأ الإقليمية فلا حاجة لوجود الجاني في مكان الجريمة فكل ما يحتاجه الجاني اتصال عن بعد ووصول إلى بيانات أو معلومات ثم الاستيلاء عليها .

4- صعوبة الكشف عن مرتكب الجريمة الالكترونية : من الصعوبة أثبات هذه الجرائم واكتشاف الآثار الناجمة عنها إلا بأساليب أمنية وتقنية عالية بسبب افتقاد وجود

الآثـار التقليديـة للجريمـة (بصـمة اليد - شـواهد ماديـة - تخريـب) مما يصعب على المحققين تعقب المتهمين و إجراء تحقيق وجمع الأدلة الرقمية بإتباع الإجراءات التقليدية للتحقيق: كالمعاينة – التفتيش - الضبط .... خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية مرتكبيها أشخاص مرتفعي الذكاء تتوفر فيهم أدوات المعرفة التقنية ببساطة هم أشخاص متمكنين ومختصين في مجال الحاسوب مما يسبب خسائر للمجتمع ككل علي

المستويات الاقتصادية والاجتماعية والثقافية والأمنية .

5-جرائم ناعمة لا تترك آثار مادية ملموسة بل كل ما تتركه آثار رقمية ذات جهد أقل من الجرائم التقليدية.

القوانين الخاصة بالجرائم الإلكترونية :

1-الأردن

قانون الجرائم الإلكترونية في الأردن والذي تم نشره في الجريدة الرسمية رقم 5343 للعام 2015

2-الإمارات

*القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة الجرائم الإلكترونية .

*القانون الاتحادي رقم (12) لسنة 2016 بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات - وزارة العدل

*إرشادات استخدام الإنترنت - الهيئة العامة لتنظيم قطاع الاتصالات

*فئات المحتوى المحظور - الهيئة العامة لتنظيم قطاع الاتصالات

*قانون نشر وتبادل البيانات في إمارة دبي

*القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية

*إدارة النفاذ إلى الإنترنت - الهيئة العامة لتنظيم قطاع الاتصالات

*الخطة الإستراتيجية للحكومة الإلكترونية الاتحادية

***قرار وزاري رقم (1) لسنة 2008 بشأن إصدار لائحة مزودي خدمات التصديق**

3-البحرين

قانون جرائم تقنية المعلومات رقم (60) لسنة 2014

4-السويد

قانون البيانات الشخصية رقم (204 :1998)

5-فلسطين

قرار بقانون رقم (16) لسنة 2017م بشأن الجرائم الإلكترونية

6- سوريا

*القانون رقم 9 لعام 2018 القاضي بإحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات.

*قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم / 17/ لعام 2012

7- السعودية

*نظام التعاملات الإلكترونية

*نظام مكافحة جرائم المعلوماتية

8- الجزائر

ورغبة منها في مكافحة فعالة للجريمة المعلوماتية، تبنت الجزائر أساليب جديدة للتحري، من خلال: تعديل قانون العقوبات بموجب القانون رقم 06-22 بتاريخ 20 ديسمبر 2006 عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية

للمعطيات. وفي 2009 أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 05 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

احد الجرائم الالكترونية :

بيتر سكالي (Peter Scully)
البالغ من العمر 52 سنة ولد في
استراليا عام 1963 كان يمتلك
موقع في ألدارك ويب يستخدم نظام
ادفع للمشاهدة

وهو موقع لعرض تعذيب الأطفال
القصر و التحرش بهم جنسيا

في عام 2011 هرب بيتر من
استراليا إلى الفلبين حيث تم اتهامه
بأنه يمتلك اكبر شبكة في ألدارك
ويب (الانترنت المظلم) لتصوير

الأطفال القصر إثناء تعذيبه لهم و التحرش بهم جنسيا

في شهر فبراير من عام (2015) تم إلقاء القبض عليه في مدينة مالايبالاي (Malaybalay) في الفلبين بعدما اكتشف محققون بقايا مراهقة فلبينية في إل 17 من عمرها تم دفنها أسفل المنزل الذي كان يعيش فيه تم توجيه له التهم بالقتل لفتاة تبلغ من العمر 12 عاما و أخرى الفلبينية صاحبة إل 17 عاما و تهمتي التعذيب وخمس حالات اغتصاب تم تصنيف جرائم

بيتر على أنها من أبشع الجرائم التي مرت بالتاريخ (5).

خسائر الاقتصاد العالمي الناجمة عن القرصنة الالكترونية :

الخسائر الناجمة عن قرصنة

الانترنت وصلت إلى مبالغ ضخمة جدا تفوق ما وصلت إلية الجرائم التقليدية وتزداد سنويا بنسبة كبيرة تصل إلى الضعف وقد بلغت هذه الخسائر مليارات الدولارات حسب الإحصائيات والتقارير الصادرة من شركات ومعاهد متخصصة وهذه الخسائر سببها انتقال معظم النشاط التجاري والاقتصادي إلى شبكة الانترنت وكذلك الانتشار الكبير لأجهزة الحاسوب والموبايل على مستوى العالم ووفقا لتقرير صادر عن مركز الدراسات الإستراتيجية والدولية (CSIS) في واشنطن بالتعاون مع شركة مكافي (McAfee) لبرامج الأمن

ألمعلوماتي فإن الاقتصاد العالمي يخسر سنوياً نحو 600 مليار دولار بزيادة في تكلفة خسائر الهجمات السيبرانية من 445 مليار دولار في العام 2014 إلى 600 مليار في 2017 (4)

المصادر

-1

https://www.statista.com/statistics/2180

89/global-market-share-of-windows-7/

-2

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

-3

الأستاذ الدكتور محمود نجيب حسني شرح قانون العقوبات - القسم العام الطبعة السادسة دار النهضة العربية القاهرة 1989 ، ص 40

-4

http://www.cityam.com/281006/cybercrime-costs-global-economy-600bn

-5

http://www.abc.net.au/news/2018-06-14/australian-peter-scully-convicted-in-philippines/9868958