- **ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن ان تتم في حال عدم توفر عنصر "السرية":**
  - ✓ هي امكانيو الاطلاع على معلومات هامة وحساسة من قبل اي احد اذا تم وضع هذه المعلومات على وسط تخزين خارجي (ذاكرة قلمية مثلا) وهي غير مشفرة.
  - ✓ ومثال اخر هو ارسال مرفق لبريد الكتروني عبر البريد الالكتروني العام (google or hotmail) وهو غير مشفر وبه معلومات هامة جدا. في هذه الحالة، فإن البريد الالكتروني والمرفقات التي معه عرضه للاطلاع عليها من قبل الغير بمن فيهم الشركة المقدمة لخدمة البريد العام.

4- سلامة وتكامل المعلومات (Data Integrity):

- وتعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل او الحذف او الاضافة او اعادة التركيب او اعادة التوجيه وهذا امر مهم جدا لضمان الثقة في المعلومة وانها هي المعلومة الاصلية دون زيادة او نقصان.
- **ومن الامثلة على الخروقات الممكنة لامن المعلومات التي يمكن ان تتم في حال عدم توفر عنصر "سلامة وتكامل المعلومة":**

هي امكانية تعديل الارقام في المعاملات المالية بسهولة دون اي تغيير في معنى الاجراء او الرسالة.فمثلا يمكن تكبير المبلغ بمجرد وضع صفر على يمينه (او تصغيره بإزالة ذلك الصفر). وفي هذه الحالة لا يمكن كشف هذا التغيير اذا لم يتوفر عنصر تكامل وسلامة المعلومة.

5- عدم الانكار:

- وهي الخدمة التي من خلالها يمكن منع وكشف اي شخص او جهة من انكار اي عملية قام بها .
- على سبيل المثال في حالة ارسال رسالة بين طرفين، فإن عدم الانكار يثبت قيام المرسل بإرسالها ويثبت قيام المستقبل باستلامها بحيث لا يمكن لأي منهما انكار ذلك. وتزداد اهمية هذا الاثبات بازدياد اهمية الرسالة نفسها.
- **ومن الامثلة على الخروقات الممكنة لامن المعلومات التي يمكن ان تتم في حال عدم توفر عنصر "عدم الانكار":**

هي امكانية التنصل من مسئولية وثيقة معينة تم توقيعها (تصديقها) الكترونيا من قبل احد الاشخاص. فإذا لم يتوفر عنصر عدم الانكار فلا يمكن اثبات ان هذا الشخص هو من قام بتوقيع هذه الوثيقة.

6- توفر المعلومة (Availability):

- ويقصد بتوفر المعلومة ان تكون قابل للوصول اليها واستخدامها حين الطلب من قبل اي شخص او اي جهة معروفة ومحددة وفي اي وقت (مصرح به).
- ويمكن القول بأن خدمة التوفر هي الخدمة التي تحمي النظام ليبقى متاحاً دائماً (ومن هنا يطلق عليها احياناً "الديمومة").
- **ومن الامثلة على الخوقات الممكنة لأمن المعلومات التي يمكن ان تتم في حال عدم توفر عنصر "توفر المعلومة ":**

امكانية تدمير انظمة المنشأة باستخدام برنامج تدميري (او فيروس تدميري) حديث الانتاج لا يوجد له برامج حماية او تحديثات patches تلغي فاعليته.

ففي هذه الحالة اذا لم تكن هناك انظمة احتياطية يتم استخدامها بدل التي تم تدميرها وتضمن توفر المعلومة فسيكون هناك توقف تام في عمل المنشأة ولو لوقت محدود.

سياسات امن المعلومات:

مقدمة:

تبدا خطة امن المعلومات بانشاء السياسات الامنية (Security Policies) والاجراءات القياسية (Standards) والاجراءات المتخذة (Practices)، من اجل الحصول على معلومات تفصيلية مطبوعة عن كل واحد منها والتي تكون في مجموعها خطة تفصيلية لامن المعلومات.

ماهية السياسات الامنية:

- هي الطريقة او الخطوات المكتوبة التي تحدد كيفية اداء الاعمال ذات العلاقة بأمن المعلومات وكيف تتم معالجة اي حدث يخص المعلومة وكيف يتم استخدام التقنية المتوفرة لمعالجة ذلك.
- وتعتبر السياسة الامنية هي حجر الزاوية للتخطيط لامن المعلومات والتي يمكن الانطلاق منها لتطبيق الخطة على ارض الواقع.
- وتجدر الاشارة الى ان هناك جانباً كبيراً من امن المعلومات هو في حقيقته جانب اداري واجرائي بالدرجة الاولى يتمثل في السياسات الامنية.
- السياسات الامنية هي اجراءات ادارية يتم تطبيقها على ارض الواقع من خلال الانظمة والبرامج المتاحة.
- مثال ذلك، يمكن وضع سياسة امنية تنص على انه في حال عدم ادخال كلمة المرور بشكل صحيح لثلاث مرات متتالية فانه يتم تعطيل حساب ذلك المستخدم ولا يفتح مرة اخرى الا عن طريق مدير الشبكة. وهذا اجراء اداري يتم تطبيقه من خلال التحكم بكلمات المرور.
- ويمكن القول بأن السياسات الامنية هي بمثابة قانون للمنشأة يحدد التعريفات والاجراءات المقبولة على كافة المستويات الادارية من مدراء ومتخذي القرارات والمنفذين.
- وعلى هذا، فإن السياسة الامنية لابد ان تكون واضحة ودقيقة وتحدد ماهو الشيئ الصحيح وما هو الشيئ الخاطئ وما هو الاجراء في حالة الصواب والاجراء في حالة الخطأ. ومما لا شك فيه فانه يجب ان يكون هناك سياسة امنية عامة للمنشأة بدءً من اجراءات منح الصلاحيات للموظف، مروراً بسياسة كلمات المرور، ثم استخدام شبكة الانترنت، وانتهاءً بخطة مواجهة الكوارث.

خصائص وثيقة السياسة الأمنية العامة:

يجب ان تكون السياسة الامنية العامة مكتوبة على شكل وثيقة تفيصيلية تتصف بالخصائص التالية :

1. ان تكون منظمة ومرتبة ومبوبة وفق مهام المنشأة الاساسية.
2. ان تكون مكتوبة بلغة واضحة سهلة الفهم والتطبيق.
3. ان يتم فيها تحديد المسؤوليات والصلاحيات بكل دقة. فمثلاً، يجب تحديد من لديهم صلاحية حرمان المستخدم من الدخول على الشبكة عند مخالفته للسياسة الامنية، وتحديد الاشخاص المسؤولين عن ايقاف خدمة معينة اذا كانت تضر بشبكة المنشأة.
4. تحديد الاجراءات التي يجب اتباعها عند ظهور اي مشكلة بشكل تفصيلي وعدم ترك الموظف في حيرة من امره.

ما يجب ان تحتويه وثيقة السياسة الأمنية العامة:

- **يجب ان تحتوي وثيقة السياسة الامنية العامة (على الاقل) على البنود التالية:**

1) الاجراءات اللازم اتخاذها فيما يخص امن المعلومات وموارد المنشأة لدى تعيين موظف جديد او عند انهاء خدمات موظف سابق.

2) تحديد صلاحيات المستخدمين وتقسيمهم الى مجموعات وتحديد صلاحيات كل مجموعة.

3) وضع الشروط والقيود اللازمة لكلمات المرور لضمان امن وحماية حسابات المستخدمين.

4) تحديد متى يجب ايقاف حساب المستخدم ومنعه من الدخول على شبكة المنشأة او تعطيل حسابه لفترة محدودة، ومتى يجب اعادة تفعيله.

5) الاجراءات اللازم اتباعها والشروط اللازم استيفائها قبل توصيل اي جهاز جديد بشبكة المنشأة.

6) اجراءات امن المعلومات التي يجب تطبيقها على الشبكة بشكل عام، وعلى كل جهاز على حده كقفل منافذ الاتصال وتفعيل التحديث التلقائي لانظمة التشغيل والبرامج وتحديد الاوقات المناسبة لذلك.

7) الاجراءات اللازم اتباعها لحماية شبكة المنشأة من الفيروسات.

8) تحديد المستخدمين أو المجموعات الذين يسمح لهم بتركيب أجهزة برامج إضافية على أجهزتهم.

9) شروط وقيود استخدام شبكة الإنترنت وإجراءات الإتصال بها.

10) الإجراءات اللازم اتخاذها للحصول على بريد إلكتروني وشروط وقيود استخدامه.

11) آلية النسخ الاحتياطي وتحديد مسؤوليات وصلاحيات عمل ذلك.

- يمكن القول بأنه لا توجد سياسة امنية تغطي كافة جوانب أمن المعلومات في جميع إجراءات المنشأة فلا بد من وضع طريقة مناسبة للتعديل او الإضافة على السياسات الأمنية، وترك مجال ذلك وفق ضوابط وشروط محددة.
- يجب مراعاة إمكانية مراجعة السياسة الأمنية والتعديل فيها مع مرور الزمن أثناء التطبيق.

حالات تطبيقية لسياسات امنية:

- الهدف من تقديم حالات تطبيقية لبعض السياسات الامنية (من الناحية الادارية كدليل امني) هو توفير التوجيهات الامنية اللازمة التي تعكس قواعد السياسة الامنية لكل حالة تطبيقية وعرضها في شكل تسهل قراءته وفهمه.
- **والحالات التطبيقية التي سيتم استعراضها هي:**

السياسة الامنية لكلمات المرور ، السياسة الامنية لاستخدام الانترنت والبريد الالكتروني.

❖ السياسة الامنية لكلمات المرور :

- من اقدم الادوات المستخدمة لحماية المعلومات هي استخدام كلمة المرور (كلمات السر) للدخول على الانظمة او المعلومات. وبذلك فإن جانباً هاماً من حماية المعلومات يقع بالكامل في ايدي المستخدمين.
- لذلك ظهرت الحاجة الى ايجاد سياسة امنية تحكم كلمات المرور وتضمن رفع المستوى الامني لها . وتتلخص اهم بنود السياسة الامنية لكلمات المرور في صيغة افعل لا تفعل فيما يلي :

- **افعل ما يلي :**

1- استخدم كلمات مرور تكون خليط من الاحرف (أ-ي) والارقام (0-9) والرموز(%،@،&،...الخ).

2- غير كلمة المرور الخاصة بك بشكل دوري.

3- استخدام حد ادنى من طول كلمات المرور، وينصح بشدة ان لا يقل عن عشرة خانات مكونة من ارقام وحروف ورموز.

4- غير كلمة المرور المقدمة اليك عند فتح حساب جديد او اعطائك صلاحية الدخول على نظام خاص بالمنشأة لاول مرة.

5- وضع حد معين لعمر كلمة المرور بحيث يجب استخدام كلمة المرور طوال فترة (عمر) معينة ولا يسمح للمستخدم بتغييرها قبل اكتمال تلك الفترة.

6- استخدام كلمات مرور عشوائية للانظمة عالية الحساسية.

7- تعطيل (او الغاء) كلمة المرور بعد ثلاث محاولات خاطئة.

- **لا تفعل ما يلي :**

1- استخدام كلمات مرور مكونة من كلمات موجودة في المعجم، بمعنى يجب ان لا تكون كلمات عادية يمكن لطرق الاختراق المعتمدة على المعاجم ان تكسرها.

2- استخدام اسم المستخدم او اي جزء منه او اي جزء من الاسم العادي للمستخدم ككلمات مرور.

3- كتابة كلمات المرور على ورق او ملصقات من اجل تذكرها.

4- استخدام كلمات المرور التلقائية (default) ككلمات مرور اساسية.

5- استخدام اي كلمة مرور من اخر خمس كلمات مرور تم استخدامها في الماضي.

6- اطلاع غيرك على كلمة المرور الخاصة بك حتى ولو كان مدير النظام.

7- استخدام كلمة المرور نفسها في عدة حسابات وانظمة (مثال ذلك: استخدام كلمة المرور نفسها للبريد الالكتروني العام وللدخول على شبكة الحاسب الالي المحلية للمنشأة).

8- تخزين كلمة المرور على الحاسب الالي.

❖ **<u>السياسة الامنية لاستخدام شبكة الانترنت والبريد الالكتروني:</u>**

- يتم توفير شبكة الانترنت والبريد الالكتروني للعاملين في المنشأة لتسهيل القيام باعمالهم والتواصل فيما بينهم ومع الجهات الخارجية.
- هناك بعض المخاطر المتأصلة في استخدام الانترنت والبريد الالكتروني من اجل ذلك يتم وضع السياسة الامنية لاستخدام شبكة الانترنت والبريد الالكتروني في صيغة افعل لا تفعل لعدد من التوجيهات المنظمة لذلك كما يلي:

- **افعل ما يلي :**

1- التاكد من عنوان الموقع او الصفحة المراد زيارتها على شبكة الانترنت.

2- التأكد من موثوقية مصادر الروابط المستخدمة للدخول على المواقع.

3- تخزين الروابط المهمة وكثيرة الاستخدام في قائمة المفضلة للرجوع لها وقت الحاجة وكذلك لضمان صحتها عند استخدامها.

4- المعرفة التامة بانواع الملفات التنفيذية التي تحمل اكواد ضارة مثل (activeX).

5- التاكد من ان رسائل البريد الالكتروني الصادرة منك تتضمن عناوين الاتصال الخاصة بك.

6- التاكد من صحة عنوان البريد الالكتروني للمرسل اليه وكذلك عنوان من تريد ان تزودهم بصورة كربونية (CC) او صورة معماة (BCC) حيث ان الاخطاء في مثل ذلك قد تؤدي الى عواقب وخيمة.

7- التاكد من ان مرفقات البريد الالكتروني هي نفسها ما قصدتها وليس غيرها، الاهمال في ذلك قد يؤدي الى بعث معلومات خامة وحساسة الى جهات ليس لها الحق في الاطلاع عليها.

8- ضغط الملفات والمجلدات كبيرة الحجم قبل ارفاقها بالبريد الالكتروني.

9- تشفير المحتويات والمرفقات الهامة قبل ارسالها.(لاحظ انه يفضل بشدة ضغط الملفات قبل تشفيرها حتى يمكن الاستفادة من عملية الضغط اقصى ما يمكن).

10- التاكد من ان جميع الرسائل الواردة اليك يتم فحصها من البرامج الضارة.

11- حذف الرسائل الغير ضرورية سواء المرسلة او المستقبلة والرسائل غير موثوقة المصدر خاصة التي بها روابط دعائية.

12- ترتيب الرسائل وحفظها في مجلدات حسب طبيعة عملك واحتياجك.

13- الابلاغ عن اي خطأ ارتكبته او موقع تمت زيارته واتضح انه موقع ضار او بريد الكتروني استقبلته وبه روابط غير موثوقة او به برامج ضارة

- **لا تفعل ما يلي :**

1- استخدام روابط غير متأكد من صحتها او التي تكون من مواقع اخرى غير موثوقة.

2- استخدام النوافذ المنبثقة الغير موثوقة.

3- تخطي رقابة الشبكة للدخول على مواقع محجوبة.

4- قضاء اوقات طويلة في تصفح مواقع ليس لها علاقة بعمل المنشأة.

5- ترك الانترنت مفتوح طوال اليوم لاغراض ليس لها علاقة بعمل المشأة.

6- تنزيل الصور والفيديو والصوتيات التي ليس لها علاقة بعمل المنشأة.

7- تنزيل المواد والبرامج بطريقة تنتهك حقوق ملكية الاخرين.

8- تنزيل البرامج وتشغيلها او تثبيتها على الاجهزة بدون اذن مسبق.

9- تنزيل او تثبيت البرامج الضارة وبرامج الاختراق والتجسس بأي شكل من الاشكال.

10- القيام بأي نشاط تخريبي او تجسسي او وصول غير مشروع من خلال اجهزة وشبكة المنشأة.

11- استخدام البريد الالكتروني لاشخاص اخرين والقيام بقراءة محتواه او ارسال الرسائل منه.

12- ارسال رسائل بريد الكتروني او مرفقات غير مصرح بها كالرسائل الدعائية والنكت واخبار الاندية الرياضية.

13- تفعيل التمرير الآلي للبريد الالكتروني الى خارج المنشأة او الجهات الغير مصرح لها داخل المنشأة.

14- فتح رسائل البريد الالكتروني مجهولة المصدر والمواضيع.

15- ارسال او فتح الرسائل او المرفقات الغير لائقة او التي بها محتويات غير مناسبة.

برامج التجسس وطرق مكافحتها:

مقدمة:

خلال السنوات القليلة الماضية ظهرت فئة جديدة من البرامج الماكرة هي برامج التجسس. وبرنامج التجسس ليس بفيروس ولكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يعمل عمله من وراء الكواليس بكل هدوء ودون علم المستخدم، ويقوم بنقل المعلومات لمالكه. وبرنامج التجسس هو عبارة عن خدعة ماكرة مثله في ذلك مثل الفيروس ولكنه بصورة عامة أقل شهرة.

تعريف برنامج التجسس:

- **يعتبر تعريف ويبوديا لبرنامج التجسس أفضل التعاريف الموجودة حيث عرّفه بأنه:**

"أي برنامج يقوم سراً بالحصول على معلومات عن المستخدم عن طريق الربط بالانترنت وخاصة بدعاوى دعائية وإعلانية".

- عادةً يتم تضمين برامج التجسس في شكل مكونات مجانية خفية أو برامج مشاركة يمكن تنـزيلها من شبكة الإنترنت.
- **يمكن تصنيف برامج التجسس إلى نوعين رئيسيين:** برامج رصد وتسجيل، وبرامج تتبع.

1- برامج الرصد والتسجيل:

- النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة وهي أكثر الأنواع شيوعاً وإزعاجاً في عملية سرقة كلمات السر وأرقام بطاقات الائتمان.
- يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يقوم بفعله المستخدم.
- هناك أيضاً راصدات ومسجلات للبريد الإلكتروني والدردشة.

2- برامج التتبع (المتتبعات):

تقوم بمراقبة عادات الاستخدام وأنماطه وتخزينها كبيانات إحصائية بهدف عمل التقارير بناءً عليها.

طريقة عمل برنامج التجسس:

- تقوم الفيروسات بإتلاف البيانات على جهاز الحاسب الآلي ونسخ نفسها ذاتياً، في حين تعمل برامج التجسس خلسة ولا تتلف البيانات بل تتجسس عليها.
- يمكن لبرامج التجسس أن تقوم بنسخ نفسها على الجهاز وتعمل كمهمة خلفية، وتنقل المعلومات السرية الخاصة بالمستخدم لمالكها دون علم المستخدم.
- يمكن لبرنامج التجسس البقاء في أي صورة أو شكل من أشكال البرامج القابلة للتنفيذ بما في ذلك التطبيقات مثل (ActiveX, Plug-in) أو أكواد (Applets).
- **لدى برنامج التجسس مكونان أساسيان:**
  1. جزء في الواجهة الأمامية وهو برنامج عادي يعمل في العلن ويوفر وظائف مفيدة.
  2. جزء في الخلف وهو برنامج تجسس يراقب وينقل المعلومات.
- عادة لا تقوم برامج التجسس بجمع المعلومات الشخصية فقط، ولكن بالإضافة إلى ذلك تجمع المعلومات الديموغرافية وعادات التصفح.

- المعلومات المتحصل عليها من المحتمل أن يتم بيعها وإضافتها لقواعد البيانات الأخرى لبناء سجلات عن المستخدم وعادات استخدامه.
- يقوم البرنامج (الذي في جهاز الضحية) في كل مرة بنسخ المعلومات من جهاز الضحية بغرض تحديث سجل الضحية لدى مالك برنامج التجسس.
- **أعراض وجود برامج التجسس وطرق انتقالها:**
  - نشاط أعلى من الحد المعتاد.
  - القيام بطلب الإتصال بالإنترنت تلقائياً.
  - ظهور أشرطة أدوات غير مألوفة تتم إضافتها لمتصفح الإنترنت.
  - اختيار صفحة بداية لمتصفح الإنترنت خلاف الصفحة التي تم ضبط المتصفح عليها من قبل المستخدم.

ـ ومن أشهر الطرق التي تنتقل بها برامج التجسس طريقتين هما :

1. تظهر وكأنها برامج نافعة أو عادية حتى يتم تثبيتها على الحاسب الآلي من قبل المستخدم وبعلمه.
2. الاختفاء في برامج أخرى بحيث يتم تثبيتها مع تثبيت هذه البرنامج دون علم المستخدم.

- **مكافحة برامج التجسس:**

من أخطر ما تقوم به برامج التجسس هي أنها تقوم بإزالة برامج مكافحة التجسس. ويمكن القول بأنه ليس هناك برنامج يقوم بالحماية من برامج التجسس بدرجة كاملة، **ولكن يمكن أخذ بعض التدابير الوقائية ومنها:**

1- فلاتر خصائص استرجاع البيانات.
2- حاجبات الإعلانات والنوافذ المنبثقة.
3- استخدام مضادات برامج التجسس.
4- استخدام جدار النار الشخصي وبرامج كشف التطفل.
5- تأمين متصفح الإنترنت.
6- تأمين إدخال كلمات المرور.

1- فلاتر خصائص استرجاع البيانات:

- يمكن إعداد (تفعيل/تعطيل) وسائل استرجاع البيانات أو ما يسمى بملفات الكوكي (Cookie Screeners) الخاصة بالمواقع التي تتم زيارتها وذلك من خلال المتصفح.
- العديد من المستخدمين يقومون بتعطيل كافة وسائل استرجاع البيانات إلا أن هذا الإجراء قد لا ينصح به لأن الكثير من المواقع تتطلب تفعيل هذه الخدمة بالكامل.
- البديل الآخر هو استخدام خاصية "التحذير قبل القبول" لكي يتم تنقيح المسترجعات يدوياً. ولكن هذا من شأنه أن يؤدي لامتلاء الجهاز بأوامر حث تشغيل ملفات الكوكي (Cookie) عند القيام بتصفح الإنترنت.
- في متصفحات الإنترنت الحديثة يمكن للمستخدمين نقل إعدادات الخصوصية للمواقع التي تتم زيارتها، وسيقوم المتصفح برفض الإسترجاعات تلقائياً بالنسبة للمواقع التي ليس بها سياسة خصوصية.

2- حاجبات الإعلانات والنوافذ المنبثقة:

- حاجبات الإعلان والنوافذ المنبثقة (Pop-UP Blockers) هي عبارة عن برامج تقوم على إجهاض تنزيل وعرض صور الإعلانات الدعائية والإغراق الإعلاني، وكذلك منع النوافذ المنبثقة من الظهور التلقائي.
- يمكن لحاجبات الإعلان أن تحسن من أداء المتصفح. ويمكن للمستخدمين أن يحافظوا على خلو الأقراص الصلبة الخاصة بهم من أي ملفات غير ضرورية باستخدام حاجبات الإعلانات.

- يمكن لبعض حاجبات الإعلانات أن تحسن من عملية الخصوصية عن طريق تحديد المعلومات التي يتم إعطاؤها.
- لدى مانعات الإعلان بعض الأثر السلبي الخفيف حيث إنها تعمل على حجب بعض الإعلانات المفيدة من خلال بعض المواقع غير الموقع الأصلي للإعلان.
- ينصح بشدة بعدم السماح للنوافذ المنبثقة التي تظهر تلقائياً عند زيارة بعض المواقع وعدم استخدامها إلا بعد التأكد من مرجعيتها وصحة العنوان الذي تحمله.

3- استخدام مضادات برامج التجسس:

- من أفضل وسيلة للدفاع ضد برامج التجسس وإزالتها في حال وجودها هي استخدام برامج مكافحة التجسس (Antispyware Scanners). وهي برامج شبيهة ببرامج مضادات الفيروسات من حيث طريقة تركيبها وتشغيلها وتحديثها.
- يعمل برنامج مكافحة برامج التجسس بنفس طريقة برنامج مكافحة الفيروسات، كما يقوم برنامج مكافحة التجسس بحذف ملفات الكوكي الغير آمنة.

4- استخدام جدار النار الشخصي وبرامج كشف التطفل:

- برامج التجسس يمكن أن تثبت نفسها أثناء تصفح الإنترنت، لذا فإن تثبيت برنامج الجدار الناري (Personal Firewall) قد يوفر بعض الحماية. وهذه الجدران النارية تقوم بحجب برامج التجسس إن وجدت ومنعها من الإتصال بالانترنت دون إذن المستخدم.
- يمكن للجدران النارية تنبيه المستخدمين حول أي محاولات للدخول لجهاز الحاسب أثناء تصفح الإنترنت. وكذلك إعلام المستخدمين إن كان هناك أي برنامج يحاول إرسال بيانات دون تفويض بذلك.
- تستخدم أنظمة كشف التطفل ((Intrusion Detection Systems (IDS) لرصد محاولات الدخول الغير المصرح به،وكذلك مراقبة حركة الشبكة أو حالة النظام.
- يعتمد نظام (IDS) على الخطة الموضوعة له. فهو يتطلب قاعدة بيانات تحدد ما هي السلوكيات السيئة أو غير المقبولة.
- عن طريق قاعدة البيانات يتعرّف نظام كشف التطفل على ماهية الأنشطة العادية، ومن ثم يمكنه مراقبة التغييرات التي جرت والتي تدل على عملية التطفل أو النشاط المشكوك فيه.

5- تأمين متصفح الإنترنت:

- من الإجراءات المضادة لبرامج التجسس هي ضبط إعدادات أمان متصفح الإنترنت لدرجة مقبولة من الأمان.
- يجب وضع الأمان في المستوى المتوسط أو العالي، مع الخيارات التالية لكل من (ActiveX) و (Plug-ins) (في أنظمة تشغيل ويندوز) :
  1. إبطال كود (ActiveX) الغير مؤشر عليها بأنها آمنة.
  2. تنشيط التحكم بكل من (ActiveX) و (Plug-ins).
  3. تنشيط التحكم بتنـزيل (ActiveX)، وذلك من خلال السماح للمعروفة منها بأنها آمنة (Singed) ومنع غير الآمنة (Unsigned).

تأمين إدخال كلمات المرور:

- من أحد طرق مكافحة برامج التجسس هي استخدام لوحة مفاتيح افتراضية مرسومة على الشاشة عوضاً عن لوحة المفاتيح العادية عند إدخال كلمات المرور والأرقام السرية.
- يمكن من خلال هذا الإجراء منع برامج الرصد والتسجيل من التقاط الأزرار التي يتم الضغط عليها من قبل المستخدم. وقد تم استخدام هذه الطريقة من قبل العديد من مواقع البنوك التجارية.