الجمهورية الجزائرية الديمقراطية الشعبية

الإشهارات الخبيثة

كيف تحمي نفسك منها؟

دليل

- المستعملين
- مسؤولي أمن أنظمة المعلومات
- المطورين

الإشهارات الخبيثة : كيف تحمي نفسك منها؟

مقدمة

أصبحت الأنترنيت وسيلة اتصال واسعة المدى وذات امكانيات ضخمة لخبراء التسويق، إذ أصبح الفضاء السيبراني أحد أهم أسواق الإشهار، مما سمح لمقدمي الإشهارات باستغلال الويب لنشر محتواهم عبر عدة أشكال، بما في ذلك اللافتات الإعلانية المدرجة على الصفحات الإلكترونية.
مع ظهور الإشهارات عبر الإنترنيت، استغل مجرمو الفضاء السيبراني بشكل خاص هذه الأخيرة الموزعة عادة على نطاق واسع من أجل إنجاح هجماتهم السيبرانية على أشخاص مستهدفين و غير مستهدفين.
يحتوي هذا الدليل على مجموعة من التوصيات للممارسات الحميدة موجهة للمستخدمين، المطورين و مسؤولي أمن أنظمة المعلومات، والتي تسمح بالوقاية و الحماية من ظاهرة الإشهارات الخبيثة.

ما هي الإشهارات الخبيثة (Malvertising) ؟

تتمثل ظاهرة الإشهارات الخبيثة و التي تعرف ب (Malvertising) في إدخال برمجيات خبيثة في الإشهارات الرقمية، التي عادة ما يتم توزيعها من خلال شبكات إشهار ومواقع واب موثوقة. يمكن أن تصيب هذه الإشهارات جهازك ببرمجيات خبيثة حتى بدون نقر.

كيف يمكنها أن تصيبك؟

تحدث الإصابة بالإشهارات الخبيثة عامة بطريقتينّ :

1. **بالنقر على الإشهارات**، والتي قد تكون على شكل نوافذ منبثقة أو تنبيهات تحذيرية، أين يتم التلاعب بالمستخدمين لتثبيت البرمجيات الخبيثة.

2. **دون النقر**، يصاب المستخدم ببساطة عن طريق تحميل صفحة الواب. حيث تحتوي الإشهارات الخبيثة على روابط مدمجة في السطور البرمجية والتي تسمح بتحميل برامج من صفحات واب ضارة بدون علم المستخدم.

تعتبر الإشهارات الخبيثة مساسا بأنظمة المعالجة الآلية للمعطيات و يتحمل فاعلها المسؤولية الجزائية طبقا للقوانين السارية المفعول كما يعاقب بالحبس و بغرامة.

1

دليل المستعملين

عزز أمن متصفح الواب الخاص بك

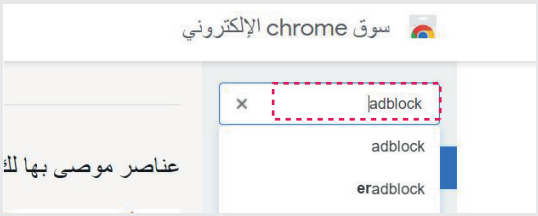
1 تثبيت الإضافات لمنع تدفق الإشهارات

يحجب مانع الإعلانات ظهور الإشهارات على متصفحك. سيقلل هذا من خطر إصابة جهازك. لذا قم بإضافة مانع الإعلانات الذي تريده على متصفحك.

مثال: المتصفح كروم

1. افتح متصفح غوغل كروم وأدخل إلى متجر كروم الإلكتروني.

2. في فراغ البحث أكتب إسم مانع الإعلانات.



3. عند إيجاد الإضافة، أنقر على "أضف إلى الكروم"

4. قم بتأكيد ذلك بالنقر على "إضافة إلى Chrome"

عزز أمن متصفح الواب الخاص بك

2 تحديث متصفح الواب

تعد التحديثات الأمنية ضرورية لضمان أمن المستخدم من الثغرات الأمنية المعروفة و بالتالي يوصى بتفعيل خاصية التحديث التلقائي.

مثال: المتصفح كروم

1. في الزاوية اليمنى العليا من نافذة كروم، انقر على أيقونة قائمة كروم ⋮ .
2. في عنصر "المساعدة"، انقر فوق "لمحة عن Chrome". سيقوم كروم بإجراء فحص تلقائي للتحديثات المتوفرة وتثبيتها على جهازك.

مثال: المتصفح فايرفوكس

1. في الزاوية اليمنى العليا من نافذة فايرفوكس، انقر على أيقونة قائمة فايرفوكس ☰
2. في عنصر "المساعدة"، انقر فوق "عن Firefox". سيقوم فايرفوكس بإجراء فحص تلقائي للتحديثات المتوفرة وتثبيتها على جهازك.

عزز أمن متصفح الواب الخاص بك

3 تسيير وضبط إعدادات ملفات تعريف الارتباط

ملفات تعريف الارتباط هي ملفات نصية مخزنة في الجهاز، يتم إنشاؤها بواسطة خادم موقع الواب الذي تمت زيارته. تحتوي هذه الملفات على البيانات اللازمة لتشغيل الموقع وبيانات إضافية. يتمثل الدور الرئيسي لملفات تعريف الارتباط في تسهيل الاستخدام اللاحق للموقع من طرف نفس المستخدم. بحسب طبيعتها، تستغل بعض ملفات تعريف الارتباط، دون علم المستعملين، في أعمال غير مشروعة مثل جمع البيانات الشخصية ، الإطلاع على عادات التصفح ، التتبع، التصديق والاستبيان، مما يشكل تهديدًا على أمن المستعمل. لذلك يوصى بقبول ملفات تعريف الارتباط القابلة للضبط فقط.

الخطوات التي يجب أن يتبعها المستخدم لتسيير و ضبط إعدادات ملفات تعريف الارتباط :

1 ضبط إعدادت ملفات تعريف الإرتباط :

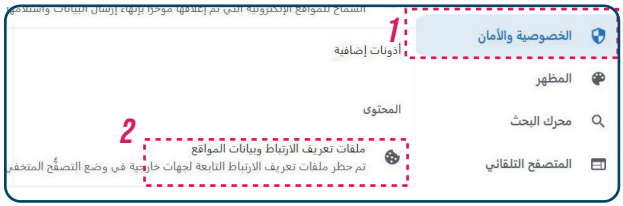
بشكل عام، بعد الولوج إلى موقع واب، هذا الأخير يطلب من الزائر قبول أو رفض ملفات تعريف الارتباط، وحتى ضبط ملفات تعريف ارتباط الجهات الخارجية. في هذه الحالة، يجب على المستخدم اختيار ملفات تعريف الارتباط القابلة للضبط بعناية.

2 ضبط متصفح الأنترنت الخاص بك:

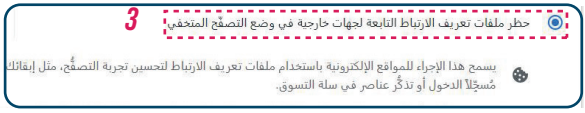
مثال: متصفح كروم

- في الزاوية العليا اليمنى من نافذة الكروم، انقر على أيقونة قائمة الكروم ⋮ واختر عنصر "الإعدادات".

- في النافذة التي تظهر، اختر عنصر "الخصوصية والأمان" ثم "ملفات تعريف الارتباط وبيانات الموقع الإلكتروني الأخرى"



- في خانة "إعدادات عامة" اختر "حظر ملفات تعريف ارتباط للجهات الخارجية".



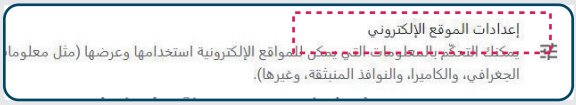
عزز أمن متصفح الواب الخاص بك

4 حجب النوافذ المنبثقة

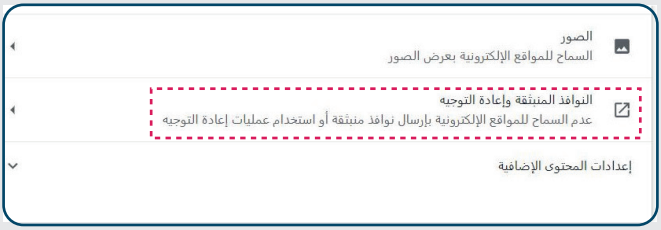
تظهر النوافذ المنبثقة تلقائيا على شاشة الجهاز عند فتح موقع واب، و تحتوي عادة على رسائل ترويجية. يمكن أن تسبب هاته النوافذ تنزيل مخفي لملفات ضارة، منها التي تفتح تلقائيا مسببة أفعال غير مشروعة بدون علم المستخدم. أغلبية المتصفحات الحديثة تحتوي الآن على حاجب النوافذ المنبثقة و الذي يسمح بإزالتها و عدم ظهورها.

مثال: متصفح كروم

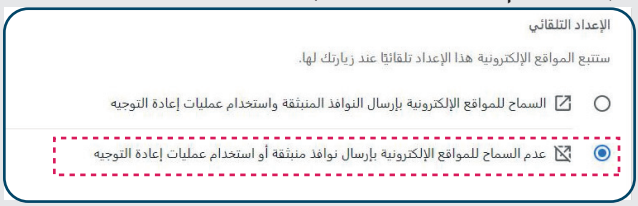
1. - في الزاوية العليا اليمنى من نافذة الكروم، انقر على أيقونة قائمة الكروم ⋮ واختر عنصر "الإعدادات".
2. - في النافذة التي تظهر، اختر عنصر "الخصوصية والأمان" ثم "إعدادات الموقع الإلكتروني"



3. - في خانة "المحتوى" اختر "النوافذ المنبثقة و إعادة التوجيه".



4. -في "الإعداد التلقائي" ضع علامة على "عدم السماح للمواقع الإلكترونية بإرسال نوافذ منبثقة أو إستخدام عمليات إعادة التوجيه".



عزز أمن متصفح الواب الخاص بك

5 تعلم كيف تتعرف على المواقع المزيفة

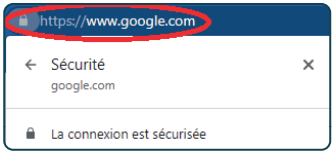
تعتبر مواقع الواب المزيفة أحد عوامل إنتشار الإشهارات الخبيثة، مما يتوجب عليك معرفة العلامات التي تبين هذه المواقع المزيفة.

تعرف على المواقع المزيفة

⚠

عدم وجود تشفير https

تأكد من وجود شعار "https" في شريط العنوان كالتالي:



⚠

تحقق بعناية من عنوان url لموقع الواب

أي عدم توافق قد يكون إشارة على أن الموقع مزيف (تشابه مع أسماء مواقع معروفة، عدم توافق بين عنوان url و محتوي الموقع). مثال www.facebok.com عوض www.facebook.com

⚠

تجنب المواقع التي تقترح عروضا جذابة أو مضللة

أو عروضا على شكل:"أنت الزائر رقم مليون انقر لتفوز بهدية "

عزز أمن متصفح الواب الخاص بك

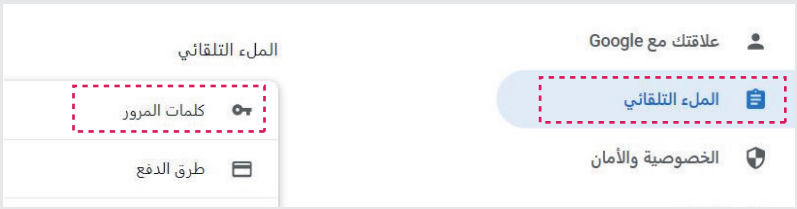
6 حذف كلمات المرور المسجلة في متصفح الواب الخاص بك

لغرض التسهيل، يختار العديد من المستخدمين قبول تسجيل كلمات المرور الخاصة بهم على المتصفحات، غير أنه تبين أن هذه الممارسة محفوفة بالمخاطر، طالما أن المتصفحات ليست آمنة بما يكفي لحماية كلمات المرور الخاصة بك. و بالتالي يوصى بحذف كلمات المرور المحفوظة في متصفحك و منعه من تسجيلها تلقائيا.

مثال: متصفح كروم

1- في الزاوية العليا اليمنى من نافذة الكروم، انقر على أيقونة قائمة الكروم ⋮ واختر عنصر "الإعدادات".

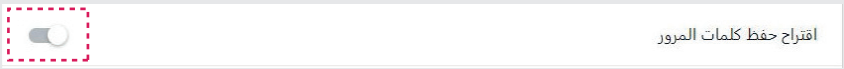
2-في النافذة التي تظهر إختر " الملء التلقائي" ثم "كلمة المرور".



3-في الخانة "كلمات المرور المحفوظة"، قم بإزالة كلمات المرور المبينة واحدة تلو الأخرى و ذلك بالنقر على ⋮ ثم إختر حذف.

لمنع متصفح الواب من تسجيل كلمات المرور تلقائيا:

*-في قائمة "كلمات المرور" قم بإزالة تفعيل "إقتراح حفظ كلمات المرور"



عزز أمن متصفح الواب الخاص بك

7 اجتنب النقر على الإعلانات ذات المحتوى المشبوه

بعض الإشهارات الخبيثة تحتوي على عروض وهمية، و بالتالي، فمن الضروري قبل الاطلاع على أي إعلان، التأكد من صحته من خلال المواقع الرسمية لصاحب العرض.

8 ضبط كلمات المرور بشكل جيد

ضبط كلمات المرور

- استعمل كلمات مرور قوية و صعبة التكهن (طويلة مع استعمال الحروف الأبجدية و الأرقام وكذا الحروف الخاصة).
- استعمل كلمة مرور واحدة لكل حساب قمت بإنشائه.
- قم بفصل الحسابات الخاصة بالإستعمال الشخصي عن تلك الخاصة بالإستعمال المهني.
- إستعمل خاصية المصادقة الثنائية.
- قم بتغير كلمات المرور بصفة دورية.

دليل المستعملين

الإشهارات الخبيثة : كيف تحمي نفسك منها؟

عزز أمن متصفح الواب الخاص بك

كيف تحمي نفسك من الإشهارات الخبيثة؟

تثبيت الإضافات لمنع تدفق الإشهارات

تحديث متصفح الواب

ضبط كلمات المرور بشكل جيد

تسيير وضبط إعدادات ملفات تعريف الارتباط

إجتنب النقر على الإعلانات ذات المحتوى المشبوه

حجب النوافذ المنبثقة

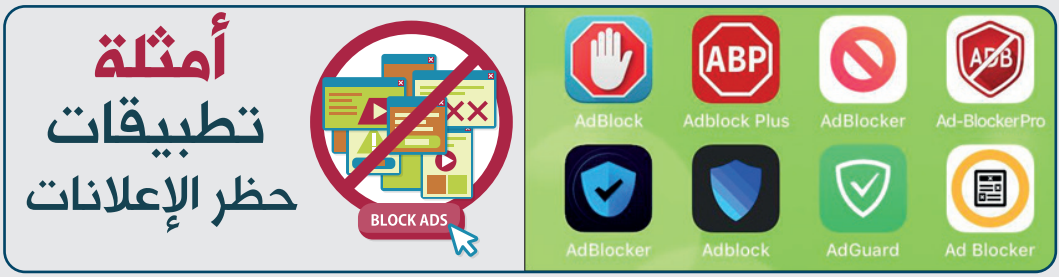
حذف كلمات المرور المسجلة في متصفح الواب الخاص بك

تعلم كيف تتعرف على المواقع المزيفة

عزز أمن الأجهزة الخاصة بك

1 تثبيت تطبيقات حظر الإعلانات على الأجهزة المراد حمايتها

هذه الأدوات تمكن من حظر ظهور أي نوع من الإعلانات فى التطبيقات والمتصفحات وكذا تحمى خصوصيتهما. لذا يوصى باستخدام مثل هاته الأدوات، سهلة الإستعمال و قابلة للتخصيص مثال AdGuard. تتوفر هذه الأدوات فى إصدارات Android و iOS للأجهزة المحمولة و Windowsو MacOs للأجهزة الأخرى.



2 قم بتثبيت مضاد فيروسات احترافي مع ضمان تحيينه بانتظام

يوصى بتثبيت مضاد فيروسات موثوق به ومحترف على جميع أجهزتك التي تتصل بها. يمنع مضاد الفيروسات كل الأفعال الضارة التي تستهدف أجهزتك ويمنع أي محاولة لسرقة البيانات أو الإصابة بالفيروسات عن طريق الإشهارات الخبيثة. يعتبر مضاد الفيروسات خط الدفاع الأول ليس فقط للحماية ضد الإشهارات الخبيثة والفيروسات، ولكن أيضًا للحماية ضد العديد من التهديدات السيبرانية الأخرى. برامج مضاد الفيروسات متوفرة على مواقعها الرسمية في نسخة مكيفة مع كل نوع من الأجهزة Android و Windows ،إلخ). ومن المهم أيضا السهر على تحيينها بصفة منتظمة ومن مصادرها الرسمية.

عزز أمن الأجهزة الخاصة بك

3 قم بإجراء فحوصات دورية وشاملة على أجهزتك

عند تثبيت مضاد الفيروسات على جهازك، من المهم إجراء فحوصات شاملة لجميع الملفات والتطبيقات المثبتة. يمكن الوصول إلى هذه الفحوصات بسهولة من خلال واجهتها الرئيسية، مما يسمح لك بالحماية من أي نوع من الهجمات التي تستهدف أجهزتك، بما في ذلك تلك التي تستغل الإشهارات الخبيثة، كما تحذف البرامج الضارة التي يتم تنزيلها من خلال هاته الأخيرة أو من خلال مصادر أخرى.

4 قم بتحديث مختلف البرمجيات والتطبيقات المستخدمة

تستغل العديد من الهجمات التي تعتمد على الإشهارات الخبيثة الثغرات الأمنية الموجودة على أجهزتك. تتضمن تحديثات البرامج تصحيحات أمنية لمعالجة هذه الثغرات. تتمثل إحدى أفضل الطرق لتجنب هذه الهجمات في تحديث برامجك وتطبيقاتك من مصادرها الرسمية. من المهم أيضًا تحديث أنظمة التشغيل لأجهزتك Windows و Android ،..إلخ)، من خلال تثبيت أحدث تصحيحات الأمن التي يمكنك العثور عليها على مواقع الواب الرسمية أو مباشرة من خلال الوظائف المخصصة «التحديث» الموجودة أساسا في قسم «الإعدادات» في نظامك.

عزز أمن الأجهزة الخاصة بك

5 كن حذرًا عند استخدام وصلة Wi-Fi مجانية من مصدر غير معروف

إن وصلات Wi-Fi المجانية ومن مصادر غير معروفة المتوفرة في الأماكن العامة ليست آمنة. في الواقع، يمكن للمجرم السيبراني إجراء اتصال بين جهازك ومصدر اتصال Wi-Fi لتنفيذ هجمات من النوع رجل في الوسط (Man In The Middle). ، مما يتيح له بعد ذلك الوصول إلى كل من المعلومات المرسلة: رسائل بريد إلكتروني مهمة وبيانات البطاقة المصرفية... الخ. وبالمثل، يقوم بعض مجرمي المجال السيبراني بإنشاء وصلات Wi-Fi مجانية ويحثونك على الاتصال بها لاستعادة جميع المعلومات المرسلة. يمكن لهذه الوصلات إعادة توجيهك إلى صفحات واب مزيفة والتي ستبدو مشروعة بالنسبة لك وتستهدفك بسهولة بإشهارات خبيثة.

6 قم بتنزيل التطبيقات والبرمجيات من مصادر رسمية

يوصى بتنزيل التطبيقات والبرمجيات من المواقع الرسمية، مثل AppStore و PlayStore لتطبيقات الهاتف المحمول. بعبارة أخرى، إذا قمت بتنزيل برمجيات أو تطبيقات من مصادر مجهولة أو من مواقع غير رسمية، فإنك تعرض أجهزتك لأخطار ضارة.

عزز أمن الأجهزة الخاصة بك

7 تأكد من أن الأذونات المطلوبة من التطبيقات أثناء تثبيتها ضرورية

عند تثبيت تطبيق على جهازك، يطلب منك الموافقة على أذونات وصول محددة لتشغيله (التخزين والكاميرا وجهات الاتصال ، إلخ.). يوصى عند التثبيت بالتحقق من أن هذه الأذونات معقولة قبل الموافقة عليها. على سبيل المثال، يمكن ان يكون تطبيق الآلة الحاسبة الذي يطلب الوصول إلى الكاميرا أو الميكروفون الخاص بجهازك تطبيقًا مشبوهًا، لذلك من الضروري عدم الموافقة على هذا النوع من الأذونات أو عدم تثبيته والبحث عن تطبيق بديل.

8 لا تستخدم أبدًا وسائط USB غير معروفة

يستخدم المجرمين السيبرانيين وسائط USB على نطاق واسع لنشر البرامج الخبيثة. عند توصيل وسيط USB غير معروف بجهازك، قد يحتوي هذا الإخيرعلى برامج ضارة يمكن أن تصيب جهازك أو حتى نظام معلومات مؤسستك.

دليل المستعملين

الإشهارات الخبيثة : كيف تحمي نفسك منها؟

عزز أمن الأجهزة الخاصة بك

كيف تحمي نفسك من الإشهارات الخبيثة؟

- تثبيت تطبيقات حظر الإعلانات على الأجهزة المراد حمايتها
- قم بتثبيت مضاد فيروسات احترافي مع ضمان تحيينه بانتظام
- قم بتنزيل التطبيقات والبرمجيات من مصادر مشروعة
- قم بإجراء فحوصات دورية وشاملة على أجهزتك
- لا تستخدم أبدًا وسائط USB غير معروفة
- قم بتحديث مختلف البرمجيات و التطبيقات المستخدمة
- تأكد من أن الأذونات المطلوبة من التطبيقات أثناء تثبيتها ضرورية
- كن حذرًا عند استخدام وصلة Wi-Fi مجانية من مصدر غير معروف

2

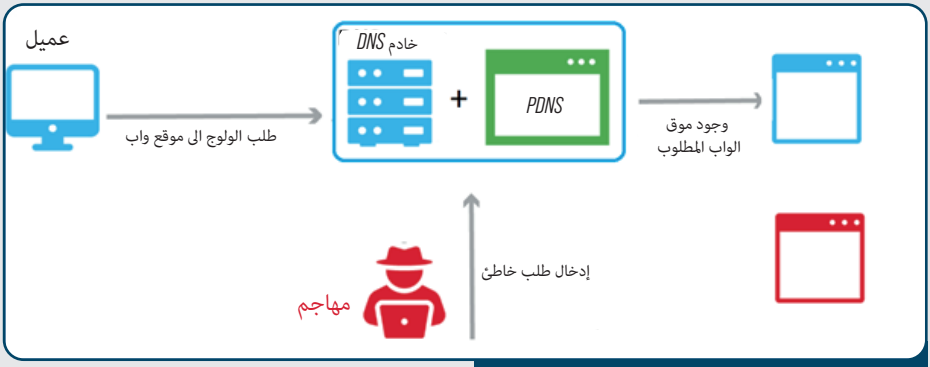
دليل

مسؤولي أمن أنظمة المعلومات

لمسؤولي أمن أنظمة المعلومات

1 وضع نظام واقي DNS (PDNS)

قد تحاول الإعلانات جمع المعلومات من المستخدمين أو قد تحتوي على تطبيقات ضارة خفية، حتى لو لم تكن ضارة، يمكن للإعلانات أن تضر بأداء النظام وتقلل من فعاليته. لمعالجة هذه المشكلة، يوصى بإعداد نظام واقي (PDNS) على مستوى مؤسستك من أجل التقليل من التهديدات المتعلقة بالإشهارات الخبيثة وتعزيز مستوى الأمن لشبكتك المعلوماتية. يمكن استهداف خادم DNS بأنواع مختلفة من الهجمات، يرسل المهاجمون بانتظام حزمًا مصممة خصيصًا إلى خوادم DNS، من أجل اكتشاف ثغرات أمنية إضافية أو استغلال تلك الموجودة بها، و في هذه الحالة يأتي دورنظام واقي DNS، والذي لديه القدرة على تصنيف أسماء النطاقات بناءً على معلومات التهديد السيبرانية. عادةً ما تستغل خدمات PDNS تدفقات المعلومات المفتوحة المصدر والتجارية والحكومية الخاصة بالمجالات الضارة المعروفة منها تلك المتعلقة بالإشهارات الخبيثة.



وثيقة:حماية خادم DNS بنظام PDNS

توفر أنظمة PDNS حماية ضد بعض التهديدات السيبرانية مثل:

- الإشهارات الخبيثة أو غير المرغوب فيها.
- DNS Spoofing الذي يسمح بسرقة البيانات الشخصية ؛
- التصيد الاحتيالي ؛
- البرامج الضارة وبرامج الفدية.

لمسؤولي أمن أنظمة المعلومات

1 وضع نظام واقي DNS (PDNS)

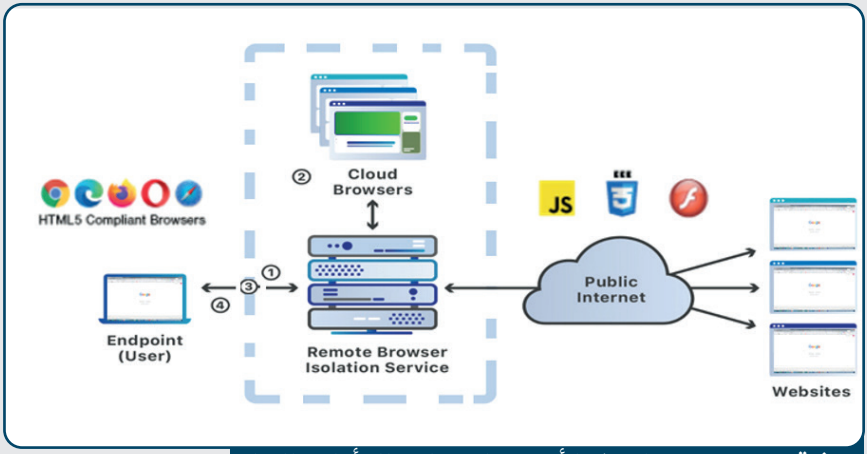
مزايا
النظام الواقي لخادم DNS

- **تصفية المحتوى**: حظر المواقع التي ينتمي محتواها إلى فئات مصنفة محظورة فيما يتعلق بسياسة الولوج للمؤسسة؛
- **تصحيح أخطاء الكتابة**: لتصحيح مثلا "organizm.DZ" إلى "organisme.dz"، غالبًا ما يشتري المهاجمون نطاقات "أخطاء الكتابة" لتثبيت البرامج الضارة أو جمع البيانات ؛
- يمكن أن تتخذ خدمة PDNS عدة تدابير (إجراء تلقائي محدد مسبقًا) للاستجابة لإسم نطاق ضار أو مشبوه؛
- توفير تنبيهات عن النشاط الخبيثة، ونظرة حول مؤشرات المؤسسة، التسجيلات والتحليلات ، للحصول على رؤية دقيقة على بيانات DNS الصادرة للاستجابة للحوادث وتحليلها؛
- **حظر الإعلانات**: حظر التهديدات المتعلقة بالإشهارات الخبيثة؛
- **الحماية ضد النطاقات المستعملة للتصيد**: أي المواقع التى تستضيف التطبيقات التى تجمع معلومات عن المستخدمين ؛
- **الحماية ضد النطاقات التي تحتوي على موزعات البرامج الخبيثة**: المواقع المعروفة بنشر برامج خبيثة؛
- **الحماية ضد مواقع الواب التي تسمح بتوليد نطاقات خبيثة**: المواقع التي تحتوي على أسماء نطاقات تم توليدها عن طريق برامج خبيثة؛
- **تحسين السرعة**: توفر خوادم DNS الآمنة بحثًا أسرع من خوادم DNS البسيطة.

لمسؤولي أمن أنظمة المعلومات

2 عزل التصفح

يسمح لك العزل بفصل عمليات التحميل عن صفحات الواب عن أجهزة المستعملين وبالتالي، لا تعمل صفحة الويب الضارة المحتملة على جهاز المستخدم، وبهذا يمنع خطر الإصابة.



وثيقة:رسم توضيحي لتصفح الأنترنت باستخدام نظام أساسي للعزل

مميزات الإستخدام

- يحمي المستخدمين من الهجمات المستهدفة المخفية في صفحات الواب ومحتوى الواب القابل للتنزيل و لإضافات التي تحتوي على ثغرات أمنية.
- يلغي إمكانية قيام صفحة واب بسحب البيانات أو تعريض جهاز المستخدم للخطر.
- يجعل الهجمات المجهولة غير ضارة.

لمسؤولي أمن أنظمة المعلومات

3 تسيير ومراقبة أنظمة المعلومات

في إطار المهام المكلف بها، على مسؤول أمن أنظمة المعلومات أن يضمن نشاط تسيير ومراقبة أنظمة المعلومات و يسهر على الكشف المبكر لمؤشرات الأخطار السيبرانية الخاصة بالإشهارات الخبيثة و هذا من أجل التصدي لها.

عند وضع نظام لتسيير ومراقبة أنظمة المعلومات فيها يجب الأخذ بعين الاعتبار العناصر التالية:

- تسيير الموارد التكنولوجية الخاصة بنظام المعلومات؛
- إدارة تثبيت أنظمة التشغيل (التثبيت عن بعد)؛
- تتبع و تعقب معدات نظام المعلومات؛
- ضمان رؤية شاملة لموارد نظام المعلومات كعمليات الصيانة المنجزة، مراقبة التحديثات و تصحيحات الثغرات الأمنية..إلخ؛
- مراقبة دورة حياة موارد نظام المعلومات من أجل إستغلال أمثل.

لمسؤولي أمن أنظمة المعلومات

4 ضبط جدران النار لحماية التدفق الداخل

الجدار الناري للجيل الجديد (NGFW) هو نظام أمن (أجهزة أو برامج) مصمم لفحص حركة بيانات الشبكة المعلوماتية. يتولى وظائف تصفية البيانات وفحص حركتها، IPsec و الشبكة الخاصة الإفتراضية VPN . بالإضافة لذلك، لديه القدرة على اكتشاف ومنع الهجمات المتطورة من خلال تطبيق قواعد الأمن المناسبة في جميع طبقات نموذج TCP/IP، ولا سيما طبقة البرمجيات التي تسمح بتصفية عناوين URL التي تحتوي على إشهارات خبيثة بالإضافة إلى التحكم و حماية مستعملي التطبيقات من التهديدات السيبرانية.

- تحديد حركة البيانات وتصفيتها ؛
- فصل مختلف قطاعات الشبكة المعلوماتية (المستوى 7 – 5، 4، 2) ؛
- الوقاية و كشف الإختراقات للشبكة و كذا تخصيص التوقيعات الرقمية، مما يسمح بحماية الخوادم ضد كل أشكال الإختراقات؛
- تسيير جودة الخدمة للحد أو ضمان سرعة التدفق لمجموعة من المستخدمين أو احدى التطبيقات ؛
- التحليل المضاد للفيروسات ؛
- توفير شبكة خاصة إفتراضية VPN من موقع إلى موقع ومن موقع إلى مستخدم (مستخدمو الهاتف المحمول) من أي جهاز (كمبيوتر محمول أو جهاز لوحي أو هاتف محمول) مما يسهل من تنقل المستخدمين ومديري نظام المعلومات ؛
- رؤية على المستعملين المراقبين بواسطة دليل الخدمة Active Directory.

لمسؤولي أمن أنظمة المعلومات

5 تثبيت وضبط مضادات الفيروسات على الأجهزة

تهدف الإشهارات الخبيثة إلى إلحاق الضرر بأجهزة مؤسستك وكذا المعلومات التي تحتويها.
يمكن أن تصاب أجهزتك على إثر تنزيل برامج خبيثة عن غير قصد، والمتواجدة في الملفات المرفقة برسائل البريد إلكتروني المشبوهة، أو مخفية في مفتاح USB ، أو حتى عن طريق زيارة موقع واب مشبوه. إن تثبيت وإعداد مضاد للفيروسات أو حاجب للإشهارات الخبيثة بطريقة مثالية سوف يساهم حتما في تحسين الأمن المعلوماتي لمؤسستك.

برامج مضادات الفيروسات

صممت برامج مضادات الفيروسات للكشف وحذف البرامج الخبيثة،و يتم تثبيتها على أجهزة فردية مثل أجهزة الكمبيوتر المكتبية والمحمولة والهواتف النقالة وكذلك على الخوادم.

الحلول الأمنية Endpoint

تساعدك الحلول الأمنية endpoint على تامين شبكتك والأجهزة المتصلة بها بشكل فعال وذلك بإدارتها مركزيا، بتعريف كل الأجهزة المتصلة وضمان التثبيت والتحديث عن بُعد للبرامج. الحلول الأمنية endpoint تجمع عدة تطبيقات للأمن السيبراني: مضادات الفيروسات، الجدران النارية، أجهزة كشف الإختراق، مضادات البرامج الضارة، إلخ.

VS

لمسؤولي أمن أنظمة المعلومات

6 تحديد استخدام Flash و JavaScript

يمكن للمهاجم استغلال موقع واب وجمع البيانات أو إدخال فيروس عبر JavaScript أو رموز الفلاش التي يتم إدراجها في اللوحات الإعلانية التي تظهر على مواقع الواب ، بما في ذلك تلك التي تعتبر موثوقة.

مثال: متصفح كروم

1. في الزاوية العلوية اليمنى من نافذة Chrome ، انقر فوق أيقونة قائمة الكروم ⋮
2. اختر «الإعدادات» من القائمة المنسدلة ؛
3. على الجانب الأيمن من الشاشة ، انقر فوق «الخصوصية والأمان» ؛

4. قم بتوسيع خيار إعدادات الموقع ؛

5. على صفحة إعدادات الموقع ، قم بالتمرير إلى أسفل الشاشة ، أسفل قسم المحتوى ، انقر فوق خيار «JavaScript» ؛

6. إلى يمين الخيار المسموح به ، انقر فوق الزر  للتبديل بين الأوضاع؛

للسماح أو حظر JavaScript على مواقع واب محددة ، في نفس النافذة انقر فوق الزر "إضافة" في القسم أو السماح بإضافة ارتباطات من هذه المواقع.

لمسؤولي أمن أنظمة المعلومات

كيف تحمي نفسك من الإشهارات الخبيثة؟

- حجب المواقع الخبيثة
- عزل التصفح
- تحديد استخدام Flash و JavaScript
- وضع نظام واقي PDNS
- منع تثبيت البرامج التي لا تحمل تراخيص رسمية
- تسيير ومراقبة أنظمة المعلومات
- تثبيت وضبط مضادات الفيروسات على الأجهزة
- ضبط جدران النار لحماية التدفق الداخل

3

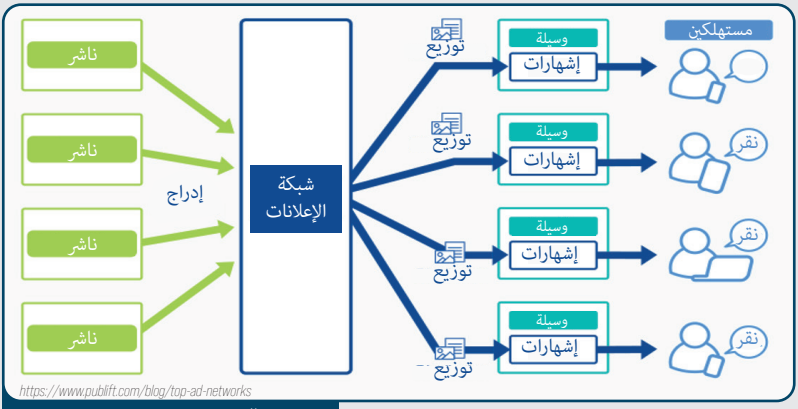
دليل المطورين

للمطورين

1 اختيار الشبكات الإشهارية بعناية

شبكات الإشهار عبارة عن مجموعة من الخوادم المتخصصة، تمامًا مثل خوادم الواب ، حيث تربط المعلنين، من جانب الطلب ، والناشرين (الوسائط / المطور)، من جانب العرض ، لتشغيل الحملات الإشهارية وزيادة عائدات الإعلانات.

لمواجهة ظاهرة الإشهارات الخبيثة ، يجب على المطور اختيار شبكة الإشهار الأفضل من ناحية السمعة وغير المدرجة في القوائم السوداء ولا تتضمن أي محتوى ضار، على سبيل المثال Google AdSense.



وثيقة:هيكل شبكة الإعلان

أمثلة الشبكات الاعلانية المعروفة

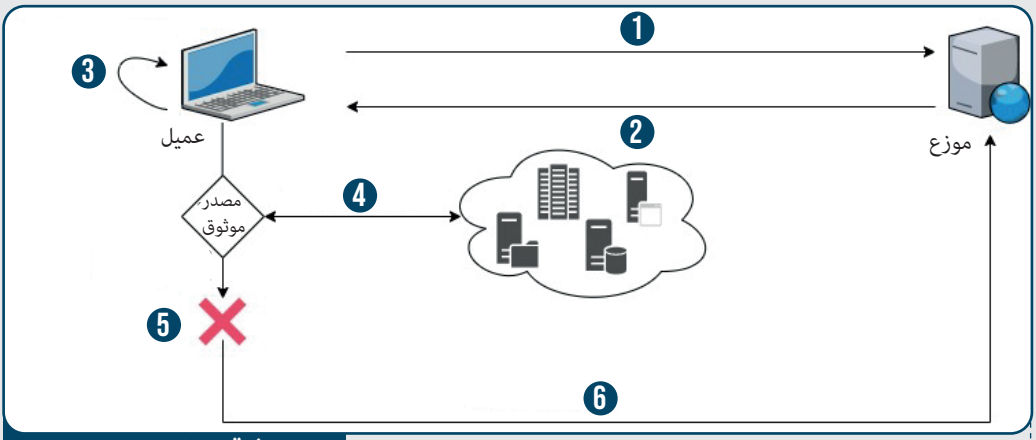
Google AdSense
amazon ads
BuySellAds
media.net

للمطورين

2 اعداد سياسة أمن المحتوى
(Content Security Policy)

سياسة أمن المحتوى (CSP) هي طبقة إضافية لحماية موقع الواب يسهل تنفيذها ومراقبتها. يمكن للمطور او الناشر استخدامها لاكتشاف وتخفيف الهجمات من نوع XSS (Cross-Site Scripting) وهجمات حقن البياناتData injection .

يتيح إعداد CSP للمطور تحديد المحتوى المسموح بتحميله. بهذه الطريقة يمكن للمطور منع تنزيل وتنفيذ البرامج النصية من مصادر خارجية أخرى. يتم وصف تشغيل CSP على النحو التالي:



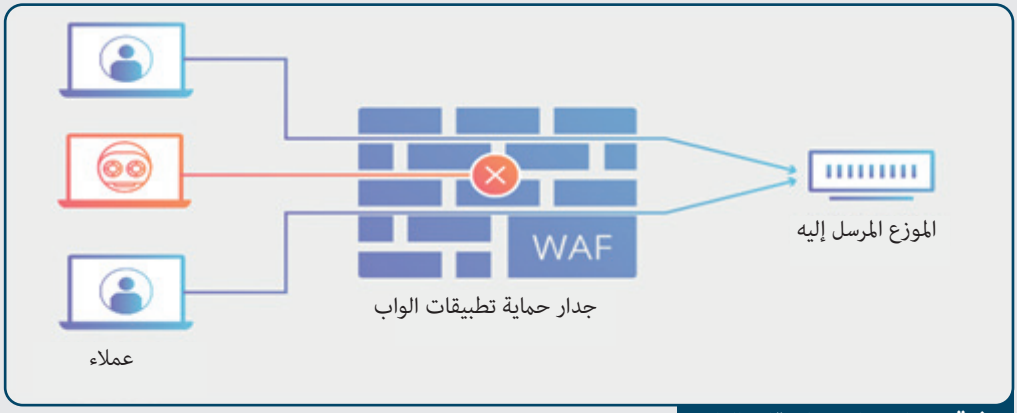
وثيقة:نظام عمل CSP

1. يزور المستعمل الموقع؛
2. يقوم المتصفح باسترداد العناوين من الموقع؛
3. يفحص المتصفح سياسة أمن المحتوى ويسجل المصادر التي يمكن تحميلها؛
4. يبدأ المتصفح في تحميل موارد إضافية محددة في برنامج مصدر موقع الواب ، مثل Google Analytics والخطوط والصور و CSS والنصوص المضمنة وما إلى ذلك؛
5. تتم مقارنة كل مورد مع سياسة أمن المحتوى الصفحة، وإذا لم يتم تحديد المصدر، يتم حظر المورد؛
6. إذا تم تفعيل هذه الخاصية، يتم إرسال تقرير انتهاك من المتصفح إلى نقطة نهاية الإبلاغ مثل URIports.

للمطورين

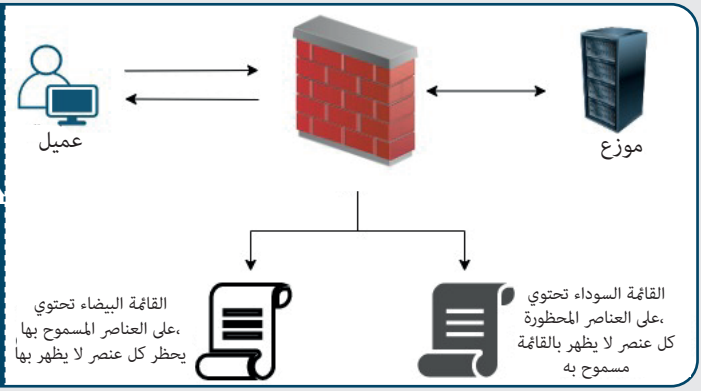
3 استخدام جدار النار لحماية تطبيقات الواب

يقوم جدارالنار لحماية تطبيقات الواب بتصفية و مراقبة حركة البيانات بين تطبيق الواب والإنترنت.
يحمي تطبيقات الواب بشكل عام من الهجمات مثل: XSS (Cross-Site Scripting) وSQL Injection.
جدار النار لحماية تطبيقات الواب هو نوع من البروكسي العكسي الذي يحمي الخادم عن طريق إجبار المستخدمين بالمرور عبره اولا قبل الوصول إلى خادم التطبيقات



وثيقة:جدار حماية تطبيقات الواب

نماذج أمن جدار النار لحماية تطبيقات الواب



للمطورين

4 اختر دائمًا HTML5 بدلاً من Flash

تحتوي مكتبة Flashعلى العديد من نقاط الضعف و الثغرات الأمنية. حيث لا يوصى بإستخدامها و هذا بسبب قدمها.

الثغرات الأمنية لـ Flash

- الرمز القابل للتنفيذ
- الحرمان من الخدمة
- Buffer overflow
- Cross-Site Scripting (XSS)

يتم استغلال هذه الثغرات من قبل المهاجمين السيبرانيين عن طريق إدراج برامج ضارة من خلال الإعلانات التي تستخدم تقنية Flash، مما دفع العديد من خبراء الأمن السيبراني إلى التوصية بعدم تثبيتها واقتراح استخدام أدوات لحظر أي مساحة تقوم بإدراجها على مستوى صفحات الويب. توجد الآن حلول أفضل مخصصة في هذا المجال، وهي HTML5 Canevas. هذا الأخير مدعوم من قبل جميع المتصفحات، وأكثر كفاءة ويعمل على جميع الأجهزة، لا يحتاج إلى برنامج خاص لتشغيله و يحوي على عدد قليل من نقاط الضعف الأمنية المستغلة من طرف الإشهارات الخبيثة.

مزايا HTML5

للمطورين

كيف تحمي نفسك من الإشهارات الخبيثة ؟

- إستخدام جدار النار لحماية تطبيقات الواب
- اختيار الشبكات الإشهارية بعناية
- إعداد سياسة أمن المحتوى (Content Security Policy)
- اختر دائمًا HTML5 بدلا من Flash