



المخاطر الأمنية في تزايد.. ما هو خط الدفاع الأول عن أجهزتنا الإلكترونية؟

أفضل برامج "جدار الحماية" و"مكافحة الفيروسات" المجانية لعام 2020

في عصرٍ رقميٍّ يفتقر إلى الأمان وتزايد خلاله المخاطر الأمنية المحدقة بالمستخدمين يوماً بعد يوم، أصبح لمواكبة مستجدات الحماية الرقمية أولوية قصوى تُلقى على عاتقنا، إذ قد يؤدي تجاهلها إلى تدمير الملفات والبيانات المخزنة والمعلومات الحساسة، وخسارة الخصوصية، ويعد استخدام جدار الحماية خط الدفاع الأول للحفاظ على الأمن الرقمي، إلى جانب برامج مكافحة الفيروسات التي يجب العمل على تحديثها باستمرار.

يُشكل الفضاء الإلكتروني بيئة خصبة للمواقع الخطرة، وقرصنة الإنترنت، والبرامج الضارة المصممة للتسلل إلى الأجهزة، وهو ما يستدعي تثبيت جدار حماية وبرنامج مكافحة للفيروسات موثوقين على نظام التشغيل، ورغم ما قد تتسبب به هذه البرامج من إبطاء لأداء جهاز الحاسوب في بعض الأحيان، إلا أن منافعها تعتبر أكبر بكثير مع قدرتها على حماية المعلومات الشخصية بعيداً عن متناول المخترقين والمجرمين.

- تشير **توقعات** شركة "CyberSecurity Ventures" إلى أن تكلفة الجرائم الإلكترونية التي سيتكبدها العالم بحلول عام 2021 ستبلغ ستة تريليونات دولار.

- تم الإبلاغ منذ بداية عام 2019 وحتى شهر أيلول منه عن نحو **5183 اختراقاً أمنياً** ما تسبب في الكشف عن 7.9 مليار سجل، وبذلك يكون قد ارتفع إجمالي عدد الخروقات عما كان عليه عام 2018 بنسبة 33.3%، وزاد إجمالي عدد السجلات المكشوفة بنسبة 112%.

- أظهرت أحدث **دراسة** أجرتها شركة "TBM"، العاملة في مجال تطوير الحواسيب والبرمجيات، ارتفاع تكلفة خرق البيانات على مدار السنوات الخمس الماضية بنسبة 12%، إذ بات الاختراق الأمني يكلف نحو 3.92 مليون دولار في المتوسط، وتشمل هذه النفقات تغطية تكاليف التحقيق والدعاوى القضائية والغرامات والتحكم بالأضرار، وتُشكل هذه الخروقات خطراً متزايداً على الشركات الصغيرة، إذ يكلفها ذلك ما يصل إلى 5% من إيراداتها السنوية.

○ جدار الحماية أو الجدار الناري:

يُستخدم جدار الحماية لضبط حركة دخول البيانات إلى الحاسوب وخروجها منه عبر وضع قواعد معينة، وهو يمنع وصول أي حزم مشبوهة يقوم بالتقاطها إلى نظام الحاسوب والشبكة الخاصة به.

بإمكان المستخدم تضيق مجال الوصول تبعاً لنمط جدار الحماية المستخدم ليشمل عناوين "IP" (بروتوكول الإنترنت) محددة وأسماء المجال، كما يمكن حظر أنماط محددة من حركة البيانات من خلال حظر أجزاء TCP/IP (بروتوكول التحكم بالنقل) المستخدمة.¹

○ أفضل برامج جدار الحماية المجانية

1. Windows Defender Firewall

وهو مثبت مجاناً لمستخدمي نظام التشغيل ويندوز 10، وفي حال كان مفعلاً ويتلقى تحديثات فإنه يوفر الحماية الأساسية من البرامج الضارة كالفيروسات وأحصنة طروادة وبرامج رانسوم واير وغيرها، وهو يقدم إشعارات حول المحتوى المحظور، كما يتضمن مستكشف ومصحح أخطاء للشبكة.²

2. Comodo Free Firewall

يعد من أقوى برامج الحماية ضد هجمات الاختراق، وهو يسمح بمراقبة البرامج والأنشطة المشبوهة، وتصفية عناوين الويب الضارة، إضافة لوضع "بيئة الاختبار الافتراضية" التي تمكّن من زيارة صفحات الويب وتشغيل البرامج في بيئة آمنة لاختبارهم قبل تشغيلهم على الجهاز فعلياً.

¹ "What Is a Firewall and How Does a Firewall Work?", lifewire, 13 December 2019. Last visited February 11, 2020. <https://www.lifewire.com/what-is-a-firewall-2487290>.

² "ما هو جدار الحماية وهل يمكنه حماية الكمبيوتر بالكامل في عام 2020؟". Safety Detectives. 27 كانون الأول/ديسمبر 2019. (آخر زيارة للرابطة: 11 شباط/فبراير 2020). <https://ar.safetydetectives.com/blog/what-is-a-firewall-ar>.

VPN أو "الشبكة الخاصة الافتراضية":

هي الطريقة الأكثر أماناً للاتصال بالإنترنت، إذ تقوم بالمحافظة على بيانات المستخدمين ونشاطاتهم مخفية ومشفرة عبر إنشاء نفق وهمي بين الجهاز ومزود الخدمة مما يعني عدم قدرة أي أحد على اعتراضها. ويكون استخدامها ضرورة وأمراً جدياً، في حالات السفر، ولتفادي المراقبة الحكومية، ولدى استخدام شبكة WIFI عمومية، وعند الرغبة في حماية الرسائل الحساسة.³

Tor أو "التور" - The Onion Router

يعمل على إخفاء هوية المستخدم ومراسلاته والمواقع التي يتصفحها، ويمنع أي جهة من التعرف على الدولة التي يتواجد فيها من خلال عنوان الـ "IP" الخاص به، كما أنه وعند تشغيله لن تتمكن الجهات التي تجمع البيانات على الإنترنت مثل Google Ads من تحليل نشاطات المستخدم وجمع البيانات من خلالها. ويصبح استخدام "Tor" حاجة ملحة في حال السفر إلى دولة تعارض عمل الشخص أو الأنشطة التي تقوم بها منظمته، ولكن يجب الانتباه إلى أنه محظور في بعض الدول مثل الصين وكازاخستان.

○ برامج الحماية من الفيروسات

تساعد برامج مكافحة الفيروسات في اكتشاف وإزالة البرمجيات الخبيثة، ووقاية الأجهزة من الإصابة بها، وينبغي تحديثها بشكل دوري من أجل التصدي لأحدث الفيروسات المنتشرة عبر الإنترنت، والتي يطورها العاملون على الدوام لمواجهة التحديات المتجددة التي يفرضها مطوروا البرمجيات الخبيثة.

الفيروسات هي برمجيات تعمل على اختراق الحاسوب والانتشار داخله بسرعة هائلة، كما يمكنها عدوى الحواسيب الأخرى السليمة، وذلك دون معرفة أو إذن المستخدم، وهي قادرة على تغيير محتويات الملفات الإلكترونية وسرقتها وحتى حذفها نهائياً، وسميت بهذا الاسم لتشابهها الكبير مع الفيروسات الحية التي تتطفل على الإنسان.⁴

○ أفضل البرامج المجانية لمكافحة الفيروسات

1. [Bitdefender Antivirus Free Edition](#)

يعتبره خبراء الأمن الرقمي من أفضل وأسرع برامج الحماية من الفيروسات المدمرة والبرمجيات الضارة،⁵ مع تأثير طفيف على أداء الحاسوب أثناء عمله، وهو يؤمن -في حالة الاشتراك الكامل المدفوع- الفحص التلقائي، والحماية من التصيد الاحتيالي وأحصنة طروادة، ورصد أي نشاط مشبوه للبرامج المثبتة في الجهاز أو المواقع التي تحاول

³ "خطوات عملية في الحماية الرقمية". سوريون من أجل الحقيقة والعدالة. 30 تشرين الثاني/نوفمبر 2018. (آخر زيارة للرابط: 11 شباط/فبراير 2020). <https://stj-sy.org/ar/1029>.

⁴ المصدر السابق نفسه.

⁵ "The best free antivirus software for 2020". Digital Trends, January 27, 2020. Last visited February 11, 2020. <https://www.digitaltrends.com/computing/best-free-antivirus-software/>.

سرقة البيانات المالية والحسابات الخاصة على الإنترنت،⁶ أما في حالة الاشتراك العادي (غير المدفوع) فيقوم البرنامج بفحص جهاز الحاسوب والبرامج والملفات الموجودة عليه فقط.

2. [ZoneAlarm Free Antivirus 2019](#)

يُعد من أفضل برامج مكافحات الفيروسات المجانية مُتصفح الويب، إذ إن العديد من ميزاته موجهة للحماية عبر الإنترنت، كما أنه يأتي مع جدار حماية مدمج قوي يسهل تثبيته وتهيئته، ويشكل أداة فحص لمكافحة البرامج الضارة مع القدرة على جدولة عمليات الفحص.⁷

ينصح الخبراء بفحص الروابط المجهولة قبل فتحها عبر الموقع التالي:

<https://www.virustotal.com/ar/>

○ نصائح للحماية

في حال إصابة الحاسوب بفيروس بسبب فشل برنامج الحماية باكتشافه نتيجة عدم وصوله إلى الشركة المطورة، ينصح الخبراء بتنفيذ الخطوات التالية:

1. فصل الحاسوب عن الإنترنت لتجنب إرسال أي معلومات.
2. إيقاف تشغيل الحاسوب للمساعدة على إيقاف نشاط الفيروس.
3. فحص الحاسوب باستخدام إحدى أدوات الحماية بعد التأكد من الحصول على تحديثات لقاعدة بياناتها.
4. استعادة الحاسوب لفترة سابقة باستخدام ميزة System Restore.
5. تغيير كلمات مرور البريد الإلكتروني ووسائل التواصل الاجتماعي لضمان عدم اختراقها.

⁶ "أفضل 10 مكافحات فيروسات للويندوز (مجانية حقاً) في 2020". Safety Detective. 28 كانون الأول/ديسمبر 2019. (آخر زيارة للرابط: 11 شباط/فبراير 2020). <https://ar.safetymagicians.com/blog/ar-best-free-antivirus-for-win>

⁷ المصدر السابق نفسه.