Mantén tu smartphone seguro del cibercrimen

Según Gartner, **cada año los dispositivos móviles sufren 42 millones de ataques de malware por parte del cibercrimen**. Esto es muy preocupante si se considera la cantidad de información personal que hoy en día almacenamos en nuestros smartphones: datos personales y familiares, información confidencial de nuestros trabajos, datos bancarios, fotografías y muchos más que en manos equivocadas podrían traernos muchos problemas.

De hecho, más de **60% de los fraudes en internet ocurren en plataformas móviles** y hay un incremento de 600% en fraudes de aplicaciones móviles desde 2015, así que los smartphones están particularmente en peligro.

La seguridad no es algo en lo que los usuarios pensamos constantemente al momento de adquirir un smartphone, y tampoco es necesariamente la prioridad de todos los fabricantes. El estudio Actualizaciones de Software y Seguridad: El Eslabón Perdido de los Smartphones, de CounterPoint Research, descubrió que HMD Global, que hoy fabrica los teléfonos Nokia, lidera en cuanto a actualizaciones de seguridad constantes a sus equipos, en todo su portafolio, desde la gama de entrada.

Si tu teléfono se sobrecalienta, o utiliza demasiados datos y no logras identificar por qué, o hasta comienza a mandar notificaciones extrañas o de aplicaciones que no reconoces, es posible que esté tenga un virus o que haya sufrido un ataque de malware.

Algunos consejos

Para mantener tu equipo, y hasta la seguridad de tu empresa, se recomienda lo siguiente:

–**No accedas a tu información privada en redes públicas**. Es decir, no, no te metas a la app de tu banco desde el WiFi gratis del aeropuerto.

–Cuando accedas a tu banco u otras aplicaciones con información privada importantes, no le digas a tu navegador que recuerde tus contraseñas.

–Respalda tu información. Una de las formas más sencillas de hacerlo es **utilizando Google Drive en tu smartphone**. Así podrás tener toda tu información: fotos, documentos, etc., en la nube, lista para accederse en cualquier momento. También, si eres más paranoico, podrías hacer otro respaldo en un disco duro externo.

–**Verifica que los sitios web** en donde ingreses información privada inicien con “https”. Esto garantiza que son seguros.

–**Activa la verificación de dos pasos**. Muchas aplicaciones tienen este tipo de verificación, desde el correo hasta tus redes sociales. Es como tener dos candados en tu puerta en lugar de sólo uno.

–Asegúrate de que tu **teléfono se mantenga actualizado**. Menos del 1% de los teléfonos Android con Android Pie y Android Oreo fueron afectados por aplicaciones potencialmente dañinas en 2018. Así que contar con la última versión no sólo es útil para mejorar el desempeño de tu equipo u obtener nuevas funciones, sino para que esté lo más seguro posible.

–Asegúrate de que tu teléfono reciba todos los parches de seguridad existentes.