5 métodos para hackearte, la magia de lo simple

Hacking al día: 5 métodos muy habituales

Una de las ventajas que tienen los atacantes a la hora de ejecutar su hazañas, es la subestimación de los métodos que utilizan, a menudo los métodos más básicos son los más efectivos, como seres pensantes, creemos estar protegidos o exentos de estos ataques por lo simple que parecen, pero en lo simple esta la magia de hacking.

Un hacker no necesita de una súper computadora para ingresar a un sistema, necesita la confianza del usuario y claro, su desconocimiento.

Veamos cinco de los métodos más habituales que utilizan los cibercriminales para obtener acceso y datos de los internautas y público en general con acceso a un PC o dispositivo electrónico.

1. Las herramientas keyloggers

Uno de los métodos de hackeo más: un software, o incluso un dispositivo, que registra cada tecla que presionas en el teclado. Archiva cada mensaje personal, cada contraseña, cada tarjeta de crédito... para pasarlo a un tercero.

Los keyloggers son el sistema de malware más popular, tanto que puede que tengas uno instalado y no lo sepas.

2. Los ataques de phishing

Consiste en crear una página web "falsa" cuyo propósito es engañarte para conseguir tus datos privados (lo que se conoce como phishing o pescar).

El phishing es uno de los ciber-ataque más simples y a la vez el más peligroso y efectivo, explica Malwarebytes. "Eso porque ataca al equipo más vulnerable y poderoso que haya existido: la mente humana".

3. Macros maliciosas sencillísimo método con Word

Una macro, básicamente es un código que creamos para automatizar un conjunto de acciones dentro de nuestro software de ofimática, Word es el rey en el segmento, por tanto es el más atacado.

Es un método muy efectivo para tomar el control de una organización, al enviarle a alguien un documento Word con un macro `malicioso´, y el empleado abre el documento, podría darle acceso remoto total a un equipo, esto le abre las puerta para hacer todo lo que quiera.

4. Las redes WiFi, en lo sencillo esta le peligo

Todos los routers actuales, tienen algo llamado WiFi Protected Setup o WPS. Lo has visto?

Es un sistema que conecta dispositivos con solo presionar un botón. Al hacerlo, se intercambia un pin de 8 dígitos y tu dispositivo se conecta al router. Muy fácil, ¿verdad? Pues allí está el peligro.

"Con un pin de solo 8 cifras, solo hay 10.000.000 posibles combinaciones. Un ataque tardarías hora para dar con el pin en cuestión".

"El WPS está diseñado para romperse en dos contraseñas de 4 dígitos cada una y te da el pin como suma. Eso significa que solo hay 11.000 combinaciones más o menos. Por lo que solo se requerirán 3 horas para ingresar en cualquier router".

¿Cómo puedes protegerte de este método en concreto? "Desactiva WPS".

5. El método más simple.. La misma clave para todo

"Los hackers saben que muchos acostumbran a reutilizar sus clave y asignar la misma contraseña en todos los sitios, porque? es más fácil, eso hace que navegar por tus sitios favoritos sea un verdadero placer sin pensar en la seguridad".

Un ciber-criminal, sabe, que hackearte en un sitio significa en un 90% haberte hackeado en todas partes, ¡incluso si usas una contraseña compleja! "Algunas páginas no almacenan tus contraseñas de forma segura. La obtienen en una de estas páginas, y la usarán en las otras páginas con mayor protección".

¿Y qué podemos hacer contra esto?

Existen trucos para evitar que te roben tus datos, pero nada es definitivo, siempre existe algo que puede fallar: tu mente. Aún así, hay acciones concretas que puedes ejecutar para protegerte, un poco.

- Usa SIEMPRE la autentificación en dos pasos.
- No abras correos con documentos de Office adjunto de remitentes desconocidos.
- Usa contraseñas diferentes para cada servicio.
- Si recibes un correo extraño, investiga sin hacer clic.
- ¿Crees que has entrado en una web phishing? Verifica la dirección.
- No guardes todas tus contraseñas en un documento de texto.
- Y la regla de oro: utiliza el sentido común