

Internet básico. Seguridad básica I. “Es que me hackearon mi cuenta”. **Basic Internet. Basic Security I. “Someone hacked my account”.**

Cuantas veces rondando por la red hemos leído que a alguien “le hackearon su cuenta”, ya sea de correo electrónico, o su página de internet, o su acceso a algún otro servicio.

Tal vez lo primero que debemos saber es ¿qué es “hackear”?

Hackear no es andar causando problemas y molestando gente. El trabajo de un hacker es entender y aprender el funcionamiento de las cosas.

Quienes se dedican a perjudicar personas son LAMMERS o CRACKERS, es decir, simples y vulgares “adivina-cuentas” o usuarios que utilizan programas desarrollados por los hackers, pero que no tienen ni idea de que es lo que hacen ni como lo hacen.

¿Cómo nos podemos proteger de ellos?

Bueno, cuando se lidia con gente que tiene ganas de molestarnos sin tener grandes y profundos conocimientos de computación y/o electrónica, lo que es importante es que nosotros los usuarios seamos quienes tengamos nuestras precauciones.

Contraseñas.

Normalmente cuando nos “hackean” una cuenta, ya sea de correo electrónico, de alguna pagina, o cualquier otro servicio, lo que realmente sucede es que nos han robado la contraseña. Y lo peor es que casi siempre ni siquiera les cuesta trabajo a los lammers robárselas. Es mas, ni se la roban, simplemente... la adivinan.

Por lo tanto

Precaución No. 1: la primera precaución que debemos tener con nuestras contraseñas es que SEAN DIFICILES, nada de usar el nombre de la mascota, el apellido, la fecha de nacimiento, el auto preferido, ni nada por el estilo. Una buena contraseña debe tener combinados letras y números, y de preferencia NO SIGNIFICAR NADA. La complicación inicia cuando necesitamos recordarla, es decir, tiene que ser algo que podamos recordar para que no tengamos necesidad de tenerla escrita.

Algo que esta demostrado es que normalmente quienes nos perjudican ¡son personas cercanas! Amigos, hermanos, conocidos, etc. Personas con quienes tenemos contacto por la misma red. Este tipo de personas muchas veces logran adivinar las contraseñas con lo que llaman “ingeniería social”, es decir, simplemente conocer a la “víctima”: sus gustos, nombres de mascotas, el carro que les gusta, que películas les gusta, etc., con lo que llegamos a la

Precaución No. 2: aquellos “amigos” que tenemos en la red muchas veces pueden volverse en un abrir y cerrar de ojos en nuestros peores enemigos. NUNCA se le confía a NADIE la contraseña. A NADIE. Y de aquí podemos regresar a la precaución 1, CONTRASEÑAS DIFICILES y sin sentido, que no tengan nada que ver con nuestros gustos o preferencias.

Es curioso. Muchas veces la misma red puede ser la fuente de donde un “adivina-cuentas” tenga lo necesario para causarnos dolores de cabeza. Los “perfiles” que quedan públicos en la red en lugares como esta comunidad muchas veces pueden tener la información necesaria para que un “adivina-cuentas” haga sus tonterías. Es en estos casos donde nuevamente toma importancia la dificultad de nuestra contraseña. Así que

Precaución No. 3: la información que quede pública de nosotros mismos debe ser la menos posible y no debe existir relación entre esa información y nuestra contraseña. Hay sitios donde nos piden fecha de nacimiento y que la hacen pública. O nuestro nombre real. Lo ideal es que esa información no sea pública, aunque si nuestra contraseña es segura no importara mucho que se sepa esa información.

Otro medio muy utilizado por los “adivina-cuentas” son los métodos de recuperación de contraseñas que la mayoría de los sitios utilizan para ayudar a sus usuarios. Cuando un “adivina-cuentas” ya conoce a su “víctima”, ya tiene una idea de sus gustos y sus preferencias, y ya intentó adivinar por prueba y error la contraseña y no lo ha logrado, normalmente lo que queda por probar es este método. Así que también hay que

Precaución No. 4: cuidar las preguntas secretas para recuperación de contraseñas. Los sitios que nos permiten usar este recurso para recuperar las contraseñas -como Hotmail- pueden delatar la contraseña real, por lo tanto, también hay que tener cuidado con esas preguntas. Es muy fácil. Simplemente lo ideal es que la pregunta y la respuesta no tengan relación. En su pregunta secreta usen una respuesta SIN SENTIDO con respecto a la pregunta, pero, que ustedes recuerden AMBAS, la pregunta y la respuesta. Por ejemplo, pongan su pregunta como ¿Cuál es su fecha de nacimiento? Y pongan como respuesta un color. Algo por el estilo.

Cuando alguien se ha propuesto adivinar nuestra contraseña cuenta con otro factor adicional a su favor: tiempo. En casi todos los sitios pueden intentar tantas veces como quieran. Por lo tanto

Precaución No. 5: CAMBIEN CON FRECUENCIA SU CONTRASEÑA. Como mínimo cada 3 o 4 meses.

Bueno, ya hemos visto como cuidarnos de los “adivina-cuentas”: debemos usar contraseñas seguras, debemos tener cuidado con los “amigos” en línea, debemos cuidar nuestra información pública, debemos cuidar los métodos de recuperación de contraseñas y debemos cambiar nuestra contraseña con frecuencia.

¿Qué pasaría si el riesgo no fuera que nos adivinen la cuenta? ¿Qué pasaría si el “lammer” utiliza algún método de hacking para fastidiarnos? No hay problema, también de ellos nos podemos cuidar.

Un lammer puede intentar atacarnos con:

Xploits.

Un xplóit es un código utilizado para aprovechar alguna vulnerabilidad de algún sistema. Es una manera de sacar provecho a los famosos “hoyos de seguridad”. Xploits existen muchos, muy variados y prácticamente para cualquier servicio o sistema. Hasta hace algún tiempo eran comunes para robar contraseñas en Hotmail aunque por ahora no hay –al menos que yo sepa- alguno que funcione.

Los xploits se pueden presentar de muchas y muy diversas formas. Se pueden enviar por correo electrónico –como el caso de Hotmail-, se pueden instalar en algún lugar dentro de sitios web, e incluso se pueden instalar a distancia en la máquina de la víctima.

Precaución No. 1: Podemos sospechar que nos intentan aplicar un xloit si “misteriosamente” termina nuestra sesión en cualquier servicio o recurso que estemos utilizando. Por ejemplo, si se encuentran un tópicos en alguna comunidad como ésta o al abrir un correo electrónico y les solicitan su nombre de usuario y su contraseña, o solo la contraseña. En estos caso es se VITAL IMPORTANCIA NO, repito, NO introducir los datos ahí. Lo recomendable es cerrar esa ventana y en una ventana nueva del navegador retomar nuestra actividad. Si en verdad terminó nuestra sesión, la podremos iniciar con confianza. Por ejemplo, si les llega un correo electrónico al Hotmail y como por arte de magia les aparece la pantalla de inicio de sesión, mejor cierren esa ventana y en una ventana nueva del explorador reinicien su sesión directamente en www.hotmail.com, solo por citar un ejemplo.

Nunca ningún sitio, servicio o recurso les deberá pedir su contraseña fuera de las páginas indicadas para este fin.

Precaución No. 2: ningún sitio, correo electrónico, ni nada, NUNCA les va a pedir ni su nombre de usuario, ni su contraseña, ni su pregunta secreta, ni su respuesta secreta, NADA, fuera de los apartados para este fin. NUUUUNNCAAAA. ¡NUNCA!

Si algo así les sucede, si les llega algún mail donde les piden que tecleen sus datos, tengan por seguro que alguien les esta queriendo robar la cuenta. Pero no se espanten tampoco, basta con no hacerle caso al engaño. Puede ser que nos digan que la cuenta tiene alguna falla, puede ser que nos digan que es para que nos entreguen un regalo, puede ser que nos digan que es para confirmar los datos, puede ser que nos digan que si no lo hacemos nos quitaran la cuenta. Lo que sea. NUNCA den sus datos de esa forma. Su información se debe manejar única y exclusivamente en los apartados adecuados para tal fin. Nunca fuera de ahí.

Desconfíen SIEMPRE que alguien o algo, ya sea por un correo, por un contacto, o por la manera que sea, les pide sus datos, ya sea del MSN, del ICQ, de su correo, de su IRC, ¡de lo que sea!

Otro recurso muy utilizado son los terribles Troyanos.

Cuando hablamos de troyanos nos referimos a códigos ocultos dentro de algún programa. Algo como “un programa dentro de otro programa”, en alusión a la famosa historia del Caballo de Troya.

Con un troyano se puede hacer mucho daño. Básicamente existen como troyanos los siguientes programas:

- Virus.
- Keyloggers.
- Back doors.

¿Cómo prevenir los Troyanos?

Básicamente son 5 precauciones, y estas les servirán en general para cuidarse de cualquiera de ellos incluyendo los siempre temibles Virus.

Precaución No. 1: SIEMPRE utilicen un antivirus ACTUALIZADO, tanto en el programa como en el patrón de virus. SIEMPRE manténgalo actualizado. Hay algunos antivirus que por si mismos pueden detectar códigos de troyanos sean cuales sean (virus, keyloggers, backdoors y cualquier otro código malicioso).

Precaución No. 2: SIEMPRE mantengan actualizado su sistema operativo. NO IMPORTA QUE SEA LINUX. En el caso de Windows, aunque sea pirata la copia, pueden utilizar con confianza la

opción Windows Update (disponible a partir de Windows 98) para hacer actualizaciones. Si no quieren lidiar con todas, las que SI resultan OBLIGATORIAS son las que están marcadas como CRITICAS.

Precaución No. 3: NUNCA abran correos electrónicos que no sepan quien se los envió. ¡NUNCA! ¡NUNCA! ¡NUUUUNCAAAA!

Precaución No. 4: NUNCA EJECUTEN UN PROGRAMA QUE LES ALLA LLEGADO POR CORREO, POR IRC, O POR MENSAJERO INSTANTANEO, NO IMPORTA QUE SE LOS ENVIE ALGUIEN CONOCIDO. Esto incluye archivos con extensión .exe, .com, .vbs, .dll, .src, .js, .jsc. Y cuidado, porque luego lo “disfrazan” poniendo dos extensiones, algo como “archivo.xls.src”, la “ultima” extensión es la que cuenta. (Esto incluye aquellos correos que les ofrecen a Anna Kurnicova desnuda =P).

Precaución No. 5: Tengan mucho cuidado con los envíos de archivos de cualquier tipo mediante MSN, ICQ, IRC, y cualquiera de esos. En cualquiera de ellos hay maneras de aprovechar el momento en que se esta haciendo la transferencia ¡para conectarse remotamente mediante los puertos abiertos de la maquina! Así que, si recién hoy conocen a alguien y ya les esta queriendo mandar imágenes o cualquier otro tipo de archivos por el IRC, o por el MSN, mejor no los acepten. No importa que tipo de archivo sea.

Y finalmente, como cuidarnos de verdaderos lammers/crackers peligrosos.

¿Qué sucede si por desgracia caemos entre ojos de un lamer/cracker que cuente con recursos y conocimientos? Bueno, aquí la situación puede en verdad tornarse peligrosa, mas sin embargo, también hay maneras de cuidarnos de ellos.

La principal herramienta de defensa que deberemos utilizar es el siempre infaltable FIREWALL. Los firewall pueden existir en dos formas, por hardware o por software. Un firewall es un “filtro” que se encarga de regular las conexiones que entran y salen. Por hardware son equipos que se conectan a la línea por donde nos estamos conectando a internet, aunque en este caso hablaremos en específico de los de software. Un firewall es un programa que realiza el filtrado de las conexiones entrantes y salientes a nuestra maquina, lo que nos permite tener cierto control y confianza en lo que sucede con nuestra conexión a la red. Es importantísimo que se tenga siempre un firewall instalado y bien configurado. Normalmente un firewall nos reporta que programa esta utilizando la conexión y que es lo que esta enviando o recibiendo. Si un firewall les reporta que esta enviando o recibiendo información a alguna conexión rara, cancelen esa conexión.

Un firewall nos permite hacer “la prueba del ñejo” a nuestra conexión. Mientras están conectados a internet como normalmente lo hacen, cierren TODAS las aplicaciones, todas las ventanas del navegador de internet, toooodo, esperen unos segundos, y miren el indicador de estado de su conexión y a su firewall. Si no hay nada solicitando o enviando información, NO DEBE HABER ACTIVIDAD, pero, si cierran toooodo y su indicador de estado de su conexión y/o su firewall sigue reportando actividad, quiere decir que tienen algo raro por ahí. Puede ser desde un molesto spyware, hasta un peligrosísimo troyano. Si están en esta situación su computadora podría NO SER CONFIABLE YA.

¿Cómo puede ser el ataque de un lammer que si tenga conocimientos?

Básicamente la idea seria hacernos caer en un xloit, adivinar la contraseña, robar la contraseña, o de plano, infiltrarse a nuestra maquina.

Ya hemos visto como cuidar nuestra contraseña, como vigilar posibles exploits, como cuidar posibles infiltraciones a la máquina mediante troyanos, y, con un firewall también estamos cuidando infiltraciones mediante conexiones directas a los puertos como con telnet, netBIOS, y cualquier otra situación por el estilo.

Una forma mas de ataque a la que se puede someter alguna cuenta nuestra es la “fuerza bruta”. La fuerza bruta no es más que lanzar alguna aplicación que probará con combinaciones tanto de letras y/o números como de palabras, para “adivinar”, ya sea el nombre de usuario y la contraseña, o solo la contraseña en caso de que ya se sepa el nombre de usuario. Pero, ¿qué creen? Si nuestra contraseña esta bien formulada, un fuerza bruta resulta inútil y hasta primitivo.

¿Cómo ven?

Como se dijo desde un principio, esta es una guía “for dummies”, para novatos en la red. ¡Básicamente la idea de esta guía es corregir malos hábitos! Muchas veces –la mayoría- les dejamos las cosas servidas en charola de plata a los lammers-adivina-cuentas-crackers para que nos causen dolores de cabeza. Más adelante se presentara la guía para usuarios avanzados. Mientras, el siguiente tema a tratar es “Spywares, advwares, y cadenas”.

Algunos términos:

HACKER: Usuario, de cualquier tipo de equipo o tecnología, que investiga y profundiza acerca de su funcionamiento, lo que le permite modificarlo, mejorarlo, y como es suposible, eso también le permite saltar los sistemas de seguridad, pero ojo, NUNCA utilizara lo que sabe para perjudicar a nadie, si acaso, para hacer travesuras.

CRACKER: Hacker amargado con complejo de inferioridad que se dedica a fastidiar a la gente con lo poco o mucho que sabe. Son los que normalmente crean los “virus”.

LAMMER: Intento de hacker, frustrado, con grave complejo de inferioridad, que lo único que si sabe hacer es utilizar los conocimientos obtenidos por los hackers o los crackers para fastidiar gente, pero, sin entender nada de lo que hace o utiliza.

Hoyo de seguridad: Recurso de un sistema operativo que permite que alguien remotamente se infiltre al recurso que lo tiene.

Back Door: Programa que permite a alguien conectarse remotamente a una computadora normalmente aprovechando algún hoyo de seguridad.

Keylogger: Programa que “guarda” todas y cada una de las teclas presionadas en la computadora mientras esta activo.

Troyano: El peor de todos, porque normalmente incluye un back door, un keylogger, y además puede traer su propio servicio de correo electrónico, y además, la peor parte, puede permitir que alguien, quien lo controla, se conecte y utilice la computadora donde esta instalado de manera remota como si estuviera frente a ella.



Contáctanos si necesitas ayuda u orientación, estamos para servirte:

Ahoraybien.com
e-mail informes@ahoraybien.com
website <http://www.ahoraybien.com>
Tel. directo (0155) 5837-1707
Fax (0155) 5837-7208
Cel. 04455-1191-3202 y 04455-5456-7271