# Así roban perfiles de Twitter, Facebook y correos electrónicos

Descubra cómo hacen los 'hackers' para usurpar su identidad en la red.

En días pasados las noticias registraron distintos golpes que grupos de 'hackers' propinaron contra las identidades digitales y sitios web de distintas personalidades y entidades oficiales. Los perfiles de Twitter del ex presidente Álvaro Uribe y de las actrices Isabella Santodomingo y Carolina Sabino, entre otros, fueron usurpados y usados indebidamente para la publicación de información privada de sus dueños y para protestas políticas. También se atacaron perfiles de Facebook del presidente Juan Manuel Santos e, incluso, lograron dejar por fuera de línea el sitio web del Ministerio de la Defensa.

Según Andrés Velázquez, de la empresa de seguridad Mattica, "el objetivo principal de atacar a figuras públicas es el de generar ruido y promoción en medios y alimentar el miedo y la zozobra entre el público".

Para expertos en delitos informáticos de la Policía, "en la mayoría de modalidades de ataque no se usaron herramientas sofisticadas, aunque ya se empiezan a presentar casos de ataques dirigidos y 'personalizados', que tienen un nivel de complejidad técnica mayor".

Según Daniel Rojas, de la empresa de seguridad Symantec, "todo comienza por el usuario. Al compartir tanta información en redes sociales, es muy fácil para el delincuente perfilarlo: sus gustos, familia, domicilio, propiedades, viajes, trabajo, etc. Eso, sumado a unos malos hábitos de seguridad en la Red, permite que los ataques tengan éxito".

A continuación, y con ayuda de los expertos en seguridad, explicaremos algunas de las modalidades más usadas por los delincuentes para usurpar la identidad digital de los usuarios de Internet.

¿Cómo recuperar un perfil robado?

En casos de usurpación, hay que decir que el proceso de recuperación de un perfil o cuenta no es sencillo. Si el caso reviste delitos (calumnia, injuria, amenazas, extorsión), debe acudir a las autoridades. En[www.policia.gov.co](http://www.policia.gov.co/) o [www.delitosinformaticos.gov.co](http://www.delitosinformaticos.gov.co/) es posible conseguir asesoría y acompañamiento.

Si desea recuperar una cuenta de Twitter, en la dirección support.twitter.com/forms encontrará la ayuda para denunciar el caso de robo. Deberá demostrar, con documentación, el caso de usurpación y esperar que el servicio compruebe la propiedad y le retorne la cuenta.

Los casos de recuperación de un perfil de Facebook son parecidos. En[www.facebook.com/security](http://www.facebook.com/security) está el centro de seguridad de dicha red social, que explica y detalla los riesgos recientes del sistema. En la dirección [www.facebook.com/roadblock/roadblock\_me.php?r=5](http://www.facebook.com/roadblock/roadblock_me.php?r=5) puede elegir una opción de 'protección de la cuenta', que sirve para alertar a Facebook en caso de que tenga sospechas de que su cuenta puede ser 'hackeada' o usurpada. En [www.facebook.co](http://www.facebook.co/) m/help está el centro de ayuda, en el que le informan las maneras de recuperar su cuenta, por ejemplo, mediante la ayuda de sus amigos, quienes pueden argumentar en el caso para que la red social le retorne un perfil 'hackeado'.

Software espía, silencioso enemigo

**Explicación.**Se trata de programas que se instalan en su PC o celular sin su permiso y que se encargan, de manera silenciosa, de 'grabar' lo que usted teclea o escribe en el equipo, para luego enviar dicha información al delincuente.

**¿Cómo opera?**Usando técnicas de engaño (ingeniería social) le envían un mensaje invitándolo a ver información curiosa (fotos privadas de una figura o el video de moda ) o a descargar contenido gratuito (música, películas o un antivirus). Estos archivos llevan 'escondido' el programa espía que se aloja en su PC y termina enviando información de nombres de usuario y contraseñas.

**Cómo prevenirlo.**Lo primero es tener sentido común. No bajar de la Red nada sospechoso, así provenga de un conocido o un familiar. Puede ser parte del engaño. Debe tener un antivirus instalado que detecte este tipo de programas.

En el 'Phishing', el señuelo es el enlace

**Explicación.** Es una modalidad de engaño que busca captar los datos de ingreso de la página en la que está navegando.

**¿Cómo opera?**Le envían un mensaje invitándolo a descubrir una información curiosa (quién mira su perfil de Facebook, por ejemplo). Al hacer clic en el enlace, le sale una supuesta página de ingreso al servicio que le quieren usurpar (su banco, correo o red social) que le pide sus datos de usuario y contraseña.  Esa página es falsa.

**Cómo prevenirlo.**El sentido común es la clave. Nunca entregue los datos de ingreso a ningún sitio al que haya llegado por un enlace. Siempre revise la dirección de la página en la que está, del navegador, para comprobar que es la verdadera.

Ataques DOS

**Explicación.**El ataque de denegación de servicio (DOS, por sus siglas en inglés) es una modalidad con la que logran dejar por fuera de línea un sitio web específico.

**¿Cómo opera?**Desde varios PC previamente dominados por los delincuentes, se ordena con un programa la ejecución de miles de solicitudes al tiempo y de manera constante hacia el sitio web. El servidor que aloja al sitio web atacado no logra responder a la ola de solicitudes y termina colapsando.

**Cómo prevenirlo.**Con aplicaciones que permiten detectar y reaccionar ante un ataque. Es una tarea de alta ingeniería.

Fuerza bruta

**Explicación.**Son ataques personalizados, muy sofisticados, que tienen el objetivo de violentar la seguridad de una empresa o usuario para lograr un archivo o datos específicos.

**¿Cómo opera?**Se usan aplicaciones que intentan descubrir contraseñas, procedimientos de acceso a bases de datos y analizar huecos de seguridad. Dichos programas atacan generando millones de combinaciones de contraseñas.

**Cómo prevenirlos.**Son difíciles de detectar por su nivel de sofisticación. Por estar dirigidos a personalidades o empresas, lo ideal es contar con la ayuda de compañías expertas en alta ingeniería.

REDACCIÓN TECNOLOGÍA