# Adquisición de cuenta

La adquisición de cuentas (ATO) debe ser familiar para cualquiera que usa internet y cuentas online. Debes haber recibido un email de Gmail o Twiter mientras estabas de vacaciones o viaje de negocios diciéndote que un inicio de sesión sospechoso acaba de ocurrir. Es porque la localidad geográfica con la que la aplicación está familiarizada ha cambiado y el API automático envía un aviso. Básicamente lo que quiere es asegurarse de que seas tú. Sin embargo, estas advertencias no deben ser tomadas a la ligera. Al día de hoy para clientes de internet ATO es una de las amenazas más persistentes y en más rápido crecimiento.

ATO es un ataque a través del cual un hacker ingresa a tu cuenta mediante el robo de tus credenciales al iniciar sesión. Estos ataques han iniciado con la usual estrategia de fraude electrónico, ingeniería social, relleno de credenciales y virus. Los administradores son objetivos preciados porque son los guardianes de la plétora de cuentas de usuario en un sistema.

### Fraude ATO

ATO a menudo dirige al fraude ATO, el cual puede tomar muchas formas, empezando con algo tan inocuo como una compra online y yendo en todas las direcciones al agotamiento de las cuentas de banco. ATO algunas veces es una actividad de vandalismo con finalidad de recreación, pero más frecuentemente es el resultado de un hacker profesional buscando más puntaje. Entre más puntos mejor, entonces los profesionales se centran en objetivos de alto valor. Incluso si es una horrible violación a cualquier escala. Imagínate encontrar mil dólares en tu tarjeta de crédito y verte en apuros por recordar cuándo se hizo la compra, luego, poco a poco te vas dando cuenta de que fuiste víctima de ATO.

Este tipo de fraude solamente va en aumento. Ha crecido más del doble desde 2020. Parte de esto es la proliferación de compras en línea debido a la pandemia, en la cual muchas más personas se quedaron en casa, otra razón peculiar es el aumento de programas de lealtad en línea, donde los vendedores online tratan de retener a sus clientes basados en programas de fidelización similares a air miles. Este tipo de programas es para los hackers una forma de monetizar. Muchas compañías han aprendido de una forma desagradable que esto debe tomarse con mayor seriedad.

Gran parte de la seguridad ha sido invertida en el proceso de compra. Desafortunadamente para el cliente digital, el número de vulnerabilidades se ha extendido más allá de este proceso, y la vulnerabilidad personal es casi ilimitada una vez que el hacker gana acceso a una de sus cuentas en línea. Uno de los problemas es el número de cuentas online que las personas tienen hoy día.

La mayoría de usuarios de internet pueden tener al menos cien cuentas y típicamente utilizan solamente una docena de ellas con regularidad. Las otras ochenta o noventa están completamente olvidadas. Esto es lo que los hackers aprovechan – las personas utilizan el nombre de usuario y contraseña una y otra vez. –

Pese a innumerables recordatorios e incluso sugerencias de contraseñas más complejas, muchas personas se apegan a sus antiguos hábitos, nombres de familiares, cumpleaños y otras costumbres.

### Previniendo el Fraude ATO

Hay un gran número de maneras en las que una adquisición de cuentas puede ocurrir, pero pueden reducirse a técnicas manuales. Probablemente el más conocido es el fraude electrónico. Que ocurre cuando posterior a un engaño cambias las credenciales de inicio de sesión.

Otra técnica es cuando expertos en seguridad llaman a ingeniería social. Alguien puede hacerse pasar por una fuente confiable y solicitar los datos de inicio de sesión. Programas malignos como registradores de claves también son utilizados frecuentemente. Hay una técnica llamada credencial de relleno, que es algo así como lo que en artes marciales mixtas se llama *ground and pound.* Es aquí donde listas previamente recopiladas de credenciales robados son atestadas de múltiples intentos de infringir cuentas online. La técnica final es una en la que el usuario debe ser más responsable, no utilizar contraseñas fáciles.

La mejor manera de evadir ATO es utilizar contraseñas largas y complejas en cada cuenta. Dejar el hábito de repetir la misma contraseña y nombre de usuario en múltiples cuentas. Ahora la mayoría de sistemas operativos vienen con administrador de contraseñas para generar y almacenar contraseñas complejas. No hay excusa.

Si el proveedor de servicio ha habilitado el multi-factor de autenticación entonces úsalo. Esto agrega una capa extra de protección. La mayoría de ATOs ocurren a través de un punto de acceso único. Si hay un respaldo de seguridad como los mensajes de texto enviados a un celular los ATOs no serán capaces de ingresar a tu cuenta.

Nunca brindes información personal a una mensajería de correo desconocida. Esta es una de las principales maneras en que los hackers ganan acceso a tus cuentas. Las estafas son casi ilimitadas. Esto incluso ha funcionado a personas con hackers haciéndose pasar por el servicio de impuestos de su país, informándoles que sus impuestos han sido reevaluados y que ahora deben más dinero, además de incitarlos a declararlo si no pagan en un periodo establecido, usualmente muy pequeño, las consecuencias pueden ser penalizaciones e intereses.

Mantén siempre tu software, tus aplicaciones y tus sistemas operativos actualizados. Descarga e instala todos los parches y actualizaciones de seguridad. Los ATO profesionales son expertos explotando pequeñas ventanas de tiempo entre nuevos parches de seguridad y antiguos sistemas. Ni por un momento pienses que tu adversario es vago o indisciplinado. Los profesionales son pacientes y disciplinados como un depredador en la jungla. Entrando en tus cuentas es como ellos comen.

Procura un buen conocimiento de todas tus cuentas. Recuerda pequeños detalles. Mantente alerta y asegúrate de que nada cambia. Si notas algo extraño investiga a como dé lugar. Dirige siempre correspondencia de los dueños legítimos de la aplicación de software, están ahí para ayudarte. Ellos tienen un trabajo familiarizado con tu uso de herramientas y de dónde lo usas generalmente. Cualquier anomalía en este uso podría ser documentado en un email. Asegúrate de que si recibes un email del propietario de software este es auténtico. Sé siempre cauteloso con los mensajes que te piden ingresar a tu cuenta y cambiar la contraseña.

Invierte en seguridad. Permanece informado sobre las últimas tecnologías y metodologías para impedir los ATOs. Esto es válido para cualquiera, pero especialmente importante para administradores de sistemas que son guardianes de grandes reservorios de datos e información de cuentas online. Invierte en detección de fraudes y sistemas que respondan a comportamientos extraños. Ha habido avances significativos en inteligencia artificial (AI) y aprendizaje autónomo (ML). Monitoreos en tiempo real para comportamientos anómalos se están convirtiendo en un requerimiento esencial de mercado para la integridad de reputación, la mejor defensa es hacer consciencia del problema. Permanezca informado y seguro.