abacus
EXCHANGE

GUÍA DE SEGURIDAD · 2026

Tu cuenta, blindada.

Guía completa de seguridad para traders.
Cómo prevenir, detectar y responder a un compromiso de cuenta.

VI
CAPÍTULOS

CAPÍTULO

I

Entender el riesgo.

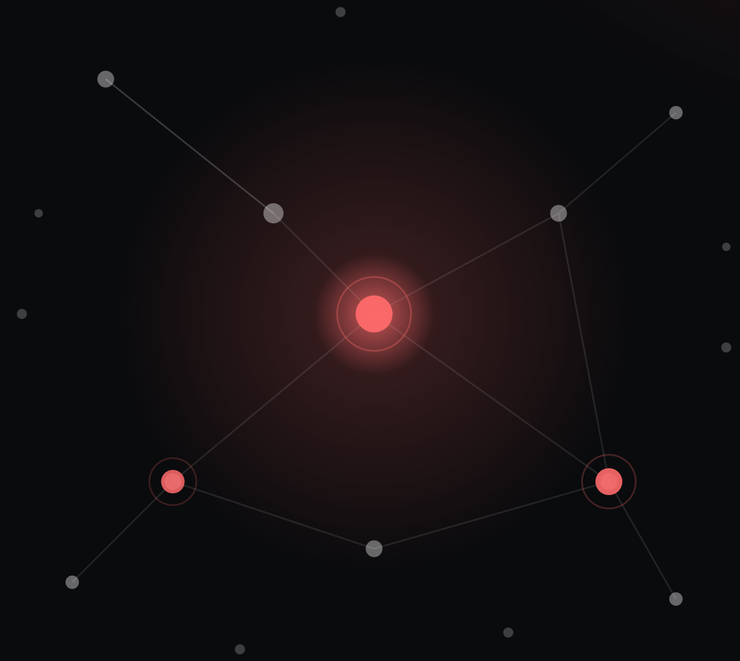
Qué es un compromiso de cuenta, por qué tú eres un blanco, y cómo te llegan.

01 • PERFIL

¿Quién es el hacker, hoy?

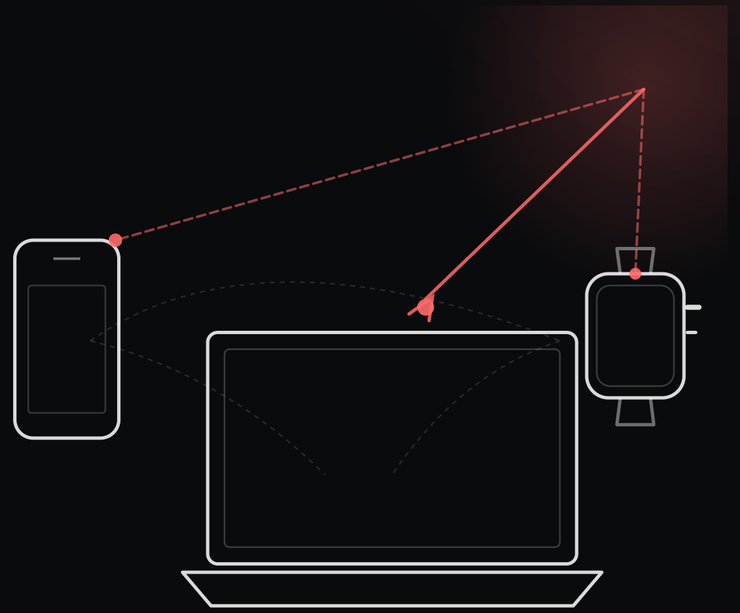
Olvida la imagen del adolescente con capucha. Hoy es **industria organizada** — equipos especializados, motivación financiera, operando como cualquier empresa.

- **Organizaciones**, no individuos. Grupos con divisiones internas.
- **Operan desde cualquier país**, en horario laboral, con KPIs.
- **Motivación principal: dinero.** Tus datos son producto secundario.
- **Especializados**: unos vulneran, otros lavan, otros revenden el acceso.



02 • SUPERFICIE DE ATAQUE

Y entran por cualquier dispositivo.



No necesitan tu app del broker directamente. **Cada dispositivo conectado a tu vida** es una puerta — y una vez dentro de uno, pivotean al resto.

- **Teléfono** — apps maliciosas, SIM swap, links infectados.
- **Computadora** — infostealers, extensiones de navegador, software pirata.
- **Tableta o reloj** — vía sesiones compartidas o cuentas iCloud/Google.
- **Router de casa** — manipulan tu tráfico desde la raíz, sin que entres a nada.

03 • DEFINICIÓN

¿Qué es un hack en una cuenta de brokerage?

No es solo robarte dinero. Es **tomar el control** de tu cuenta y operarla como si fueran ellos. Una vez dentro, las opciones del atacante son amplias.

- **Ejecutar trades** que tú no autorizaste — incluso para mover precios
- **Drenar fondos** vía ACH o wire a cuentas fuera de tu alcance
- **Usar tu cuenta como liquidez** para esquemas de pump & dump
- **Robar tu identidad** — los datos valen tanto como el dinero
- **Cascada**: tu cuenta da acceso a tu email, tu email a todo lo demás

04 • POR QUÉ TÚ

Los traders son el blanco favorito.

No es accidente. Una cuenta de trading combina **liquidez, conectividad y normalización de movimientos grandes**. Es el cóctel perfecto.

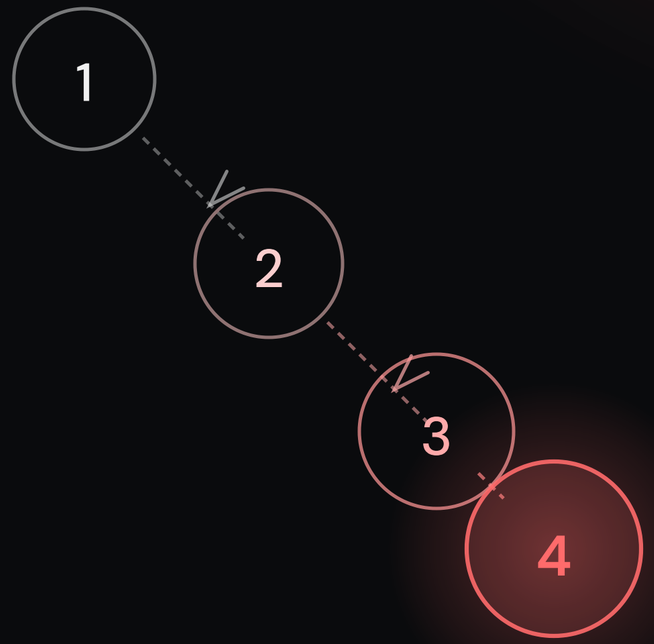
- **Liquidez instantánea** — efectivo y valores convertibles en horas
- **Conexión ACH y wire** al banco — drenaje rápido y permitido
- **Actividad alta** — un trade fraudulento se camufla en el flujo normal
- **Movimientos grandes son rutina** — un retiro fuerte no levanta sospecha
- **Sirves como liquidez** de un pump & dump organizado por otros
- **Confianza propia** — el trader experimentado baja la guardia primero

05 • ANATOMÍA DEL ATAQUE

Cómo suceden estos ataques.

El ataque no es un solo evento — es una **cadena de cuatro fases**. Romper una fase rompe el ataque completo.

- **Reconocimiento** — recopilan tu información de redes y filtraciones.
- **Acceso inicial** — phishing, credenciales reutilizadas, SIM swap, malware.
- **Toma de control** — cambian tu email, desactivan tu 2FA, te bloquean.
- **Monetización** — retiros, trades manipulativos, venta de tu identidad.



06 • VECTORES DE ATAQUE

Las puertas que tú abres.

Cada ataque empieza con una acción tuya — un clic, una descarga, una contraseña repetida. **Tú abres la puerta. Ellos solo entran.**

- **Haces clic** en un email o SMS "urgente" del broker y escribes tu clave en una página falsa — phishing.
- **Reutilizas** la misma contraseña en otro sitio que ya fue vulnerado — credential stuffing.
- **Dejas tu 2FA por SMS** y un atacante hace SIM swap a tu carrier — recibe los códigos en su teléfono.
- **Tu email madre** aparece en redes, foros y suscripciones — lo comprometen y desde ahí reinician todo.
- **Instalas** una extensión de navegador, app pirata o archivo de un desconocido — infostealer capturando lo que escribes.
- **Operas desde WiFi pública** — interceptan tu sesión en tránsito o te muestran una red falsa con el mismo nombre.

07 • DETECCIÓN TEMPRANA

Señales de alerta inmediatas.

El broker no te va a llamar para avisarte. **Verlas a tiempo es tu trabajo** — y cada una merece una respuesta dentro de los 60 minutos del Capítulo II.

1. Email de **login desde un lugar o IP** que no reconoces.
2. Push de **2FA que tú no iniciaste**, sobre todo a horas raras.
3. **Pérdida súbita de señal celular** — el clásico inicio de SIM swap.
4. Email de **reseteo de contraseña** que tú no solicitaste — broker, banco o email.
5. Tu **email ya no abre**, tu teléfono cambió, o tu app del broker pide reconfigurar 2FA sola.
6. Pequeños **"test trades"** o depósitos extraños — están probando si te das cuenta.
7. **Sesiones activas** en dispositivos o navegadores que no reconoces.
8. **Cambios en tu perfil** (email, teléfono, dirección, banco vinculado) que tú no hiciste.

II

CAPÍTULO

Si ya fuiste hackeado.

El tiempo de reacción es lo que determina cuánto recuperas. Tres ventanas críticas.

60 min

VENTANA DE CONTENCIÓN

Detén el sangrado.
Documenta todo lo que veas.

1. **Llama al broker** al número de fraude (Capítulo VI). Pide congelar la cuenta y bloquear retiros y trades.
2. **Captura pantallas** de todo: órdenes no autorizadas, retiros, mensajes, sesiones activas. Pon timestamp.
3. **Cambia la contraseña** del broker y del email asociado. Cierra todas las sesiones activas desde el panel del broker.
4. **Desconecta el dispositivo** sospechoso de internet hasta que lo escanees. Si fue tu computadora, no toques esa cuenta desde ahí.

24 h

VENTANA DE RECLAMO

Formaliza el reclamo.
El registro escrito es tu protección.

1. **Envía un email formal** al broker describiendo los hechos, la hora, las transacciones no autorizadas. Pide número de caso.
2. **Reporta al FBI IC3** (ic3.gov). Crítico si hubo wire o ACH a destinos fuera de US — pueden ayudar a revertir.
3. **Notifica a tu banco** si la cuenta estaba conectada. Reporta los retiros como no autorizados y bloquea ACH/wires al broker.
4. **Activa fraud alert** con Equifax, Experian y TransUnion. Una llamada a una agencia notifica a las tres.

7 d

VENTANA DE RECUPERACIÓN

Escala con autoridades. Reconstruye desde cero.

1. **Reporta a la SEC** en sec.gov/tcr y a **FINRA** en finra.org. Adjunta el número de caso del broker y tus capturas.
2. **Pide un affidavit de fraude** al broker si lo requieren. Es requisito para activar muchas pólizas de cobertura.
3. Considera **cerrar la cuenta y abrir una nueva** con identificadores limpios: nuevo email, nuevo número, nueva contraseña, nuevo 2FA.
4. **Conserva todo el expediente** al menos 7 años: emails, capturas, números de caso, fechas, montos. Es tu evidencia para reembolso.

III

CAPÍTULO

Configuración obligatoria.

Los cinco pilares que no son opcionales si tu cuenta tiene capital real.

01 • BASE MÍNIMA

Configuración mínima de seguridad obligatoria.

1 **2FA por app o llave física** — nunca SMS. Authy, Google Authenticator o YubiKey.

2 **Contraseña única** de 20+ caracteres, generada por un gestor.

3 **Alertas de login** activas por push o email. Todas, sin excepción.

4 **Alertas de retiro y wire** — el segundo más crítico después del login.

5 **Trusted devices** configurados — limitar qué dispositivos pueden operar.

6 **Whitelist de cuentas bancarias** para retiros donde el broker lo soporte.

02 • EMAIL

Tu email es la llave maestra. Protégelo como tal.

Si comprometen tu email, comprometen todo: los resets de contraseña pasan por ahí. **El email es la única puerta que abre todas las demás puertas.**

- **Email dedicado a finanzas**, distinto al personal y al laboral
- **2FA con app o llave física** — más fuerte que el de cualquier otra cuenta
- **No lo uses** para redes sociales, foros, suscripciones o newsletters
- **Recovery options** al día: número de respaldo, email alterno, ambos protegidos
- **Filtros y alertas** que detecten intentos de cambio o resets sospechosos
- **Proveedor con buena recuperación**: Gmail, ProtonMail. Evita proveedores oscuros.

03 • DISPOSITIVO

Higiene del dispositivo.

1 **Actualizaciones automáticas** de sistema operativo y navegador.

2 **Sin WiFi pública** para operar. Usa datos celulares o VPN confiable.

3 **Dispositivo dedicado** a tus cuentas financieras, si tu volumen lo justifica.

4 **Antivirus actualizado** en Windows. macOS y iOS son más resistentes, no inmunes.

5 **Sin software pirata** ni extensiones de fuentes no oficiales — vector clásico de malware.

6 **Bloqueo con biometría + PIN**. Sin esto, perder el teléfono es perder la cuenta.

04 • COMUNICACIÓN CON TU BROKER

Las reglas de oro. Sin excepciones.

NUNCA	Tu broker **te pide tu contraseña**. Por ningún medio. Nunca.
NUNCA	Tu broker **te pide tu código 2FA** "para verificar". Ningún equipo real lo hace.
NUNCA	Tu broker **te llama urgentemente** para "resolver una alerta". Tú llamas a ellos.
NUNCA	Tu broker **te pide instalar software remoto** (TeamViewer, AnyDesk, etc.) en tu equipo.
NUNCA	Tu broker **te escribe primero** por SMS con un link para que actúes "ya".
SIEMPRE	Cuando dudes, **cuelga y llama tú** al número oficial del Capítulo VI.

05 • SIM SWAP

Protección contra SIM swap.

Un criminal convence a tu carrier de transferir tu número a su SIM. **Desde ese momento todos tus SMS y llamadas van a su teléfono** — y tu 2FA por SMS deja de protegerte.

Verizon

Activa **Number Lock** + **SIM Protection** en Security Settings de la app My Verizon.

T-Mobile

Activa **Port Out Protection** en T-Life app. PIN de 6–15 dígitos obligatorio.

AT&T

Activa **Wireless Account Lock** en la app myAT&T. Bloquea ports y cambios.

- **PIN único de carrier** — 6 a 8 dígitos, no es tu cumpleaños ni tu SSN
- **Migra todo tu 2FA** de SMS a app o llave física
- **No publiques tu número** en redes sociales ni en sitios públicos

IV

CAPÍTULO

Cobertura y responsabilidad.

Qué cubre SIPC, qué cubre tu broker, y dónde termina la responsabilidad de ambos.

Qué cubre y qué NO cubre la SIPC y tu broker.

SIPC

NO CUBRE FRAUDE

$500K

POR CUENTA · INCLUYE $250K EN EFECTIVO

SIPC solo protege si tu broker quiebra. Garantiza que recuperes tus valores y efectivo si la firma fracasa.

Pero la SIPC **no cubre**: pérdidas por fraude, hackeo, ingeniería social, ni decisiones de inversión. Tampoco cubre crypto no registrada con la SEC.

Para activarla, debes haber operado con un **broker miembro SIPC** (la mayoría lo son — verifica en sipc.org/list-of-members).

Broker

POLÍTICA PROPIA · CONOCE LA TUYA

Varía

POR BROKER · REVISA TU CLIENT AGREEMENT

Cada broker tiene su propia política. **Schwab y Fidelity** ofrecen garantías explícitas de reembolso por actividad no autorizada. **TradeStation, IBKR y Robinhood** evalúan caso por caso, sin garantía pública.

La condición común: reportar a tiempo (30 a 60 días desde el estado de cuenta) y que la actividad no se haya originado en tu negligencia — compartir contraseña, dar acceso remoto, autorizar a un tercero.

Conoce la política **antes** de necesitarla. Está en tu Client Agreement.

V

CAPÍTULO

Auditoría en 5 minutos.

Diez verificaciones para confirmar que tu cuenta está protegida. Si fallas una, eso es tu siguiente acción.

Checklist de auditoría de seguridad.

Tómate cinco minutos. Una marca por cada respuesta afirmativa.

- [ ] Mi **2FA** es por app o llave física — no por SMS.
- [ ] Tengo **alertas de login** activas (push o email).
- [ ] Mi **carrier** tiene port-out lock o Number Lock activado.
- [ ] Tengo guardados los **códigos de respaldo** de 2FA.
- [ ] Revisé las **sesiones activas** — todas son mías.
- [ ] Mi **contraseña** de broker es única y de 16+ caracteres.
- [ ] Tengo **alertas de retiro** y de wire activas.
- [ ] Mi **email de finanzas** es distinto al personal.
- [ ] Mi **SO y navegador** tienen actualizaciones automáticas.
- [ ] Tengo guardado el **número de fraude** de mi broker.

VI

CAPÍTULO

Números de emergencia.

Los cinco brokers más usados, con sus líneas de fraude verificadas. Guárdalos antes de necesitarlos.

01 • BROKER

Interactive Brokers

CLIENT SERVICES · 24/7 ENTRE SEMANA

+1 877-442-2757

DIRECTO +1 312-542-6901

REPORTE SEGURO

MÁS SEGURO Mensaje desde Client Portal

WEB ibkr.com/help

NOTA IMPORTANTE

IBKR no tiene una garantía pública de reembolso.

El reclamo se evalúa caso por caso. Reporta de inmediato vía Client Portal (canal más seguro). IBKR ha advertido públicamente sobre **clones que imitan su web y empleados** — verifica siempre que estés en interactivebrokers.com.

02 • BROKER

Thinkorswim · Charles Schwab

LÍNEA DE FRAUDE · SCHWAB

+1 877-862-6352

DESDE FUERA +1 602-355-7300

OTROS CANALES

GENERAL +1 800-435-4000

PHISHING phishing@schwab.com

SCHWAB SECURITY GUARANTEE

Cubre pérdidas por actividad no autorizada.

Desde la adquisición de TD Ameritrade, **thinkorswim opera bajo Schwab**. La línea de fraude y la garantía de seguridad de Schwab aplican. No aplica si compartiste credenciales o diste acceso remoto.

03 • BROKER

Robinhood

SOPORTE · SOLO DESDE LA APP

robinhood.com/contact

Robinhood no publica teléfono. Solicita callback dentro de la app.

EMAIL

SOPORTE	support@robinhood.com
PHISHING	reportphishing@robinhood.com

CONGELAR CUENTA

El chat congela tu cuenta en minutos.

Abre el chat dentro de la app y escribe **"my account is hacked"** o **"unauthorized activity"**. El chatbot mostrará el botón "Freeze account". Cualquier "soporte telefónico" externo es fraude.

04 • BROKER

E*TRADE · Morgan Stanley

MORGAN STANLEY ONLINE SECURITY · 24/7

+1 888-454-3965

E*TRADE +1 800-387-2331

INTERNACIONAL

+1 678-624-6210

POLÍTICA

E*TRADE pertenece a Morgan Stanley.

Para fraude o robo de identidad, la línea de **Morgan Stanley Online Security** opera 24/7. La línea de E*TRADE es para actividad bancaria sospechosa. La responsabilidad está sujeta al Client Agreement.

05 • BROKER

TradeStation

CLIENT SERVICES · LUN-VIE 8AM-5PM ET

+1 800-822-0512

DIRECTO +1 954-652-7900

EMAIL

ClientService@TradeStation.com

EUROPA +31 20 214 0470

POLÍTICA DE SEGURIDAD

TradeStation nunca te contacta por SMS ni redes sociales.

Cualquier texto o DM que diga ser de TradeStation es fraude. Reporta de inmediato a Client Services. TradeStation notifica cambios al perfil — si recibes alerta de cambio no autorizado, llama ya.

abacus
EXCHANGE

La mejor inversión es la que conservas.

ABACUS EXCHANGE · GUÍA DE SEGURIDAD PARA TRADERS