MISIÓN 3 · LA BÓVEDA BAJO ATAQUE

Seguridad Cripto y Defensa Anti-Estafas

El manual que más dinero ahorra en todo el curso: cómo operan realmente las estafas modernas en Web3 (phishing, firmas maliciosas, falsos soportes, envenenamiento de direcciones) y el sistema práctico de higiene digital para blindar tu capital.

NIVEL	SIMULADOR ASOCIADO	DESBLOQUEO HOTMART
Crítico · Obligatorio	**La Bóveda bajo Ataque**	**Quiz Módulo 03 → 04**

Qué vas a dominar al terminar este manual

- Detectar en segundos sitios de **phishing**, anuncios patrocinados falsos y mensajes de ingeniería social.
- Leer ventanas de firma Web3 (`Approve` , `setApprovalForAll` , `Permit`) y revocar permisos viejos.
- Implementar un **respaldo físico offline** de tu frase semilla resistente a robos digitales y accidentes domésticos.
- Separar tu operativa en **billetera de uso diario (Burner)** vs. **bóveda de ahorro**.

SECCIÓN 01 · INGENIERÍA SOCIAL

Casi nadie «hackea» la blockchain: hackean a las personas

Romper la criptografía de Bitcoin o Ethereum es matemáticamente inviable hoy. Por eso, más del 90% de las pérdidas ocurren por **ingeniería social**: engañar al usuario para que entregue su frase semilla o firme una autorización engañosa.

Modalidad de ataque	Cómo te atrapan	Defensa inmediata
Phishing por dominio clonado	Anuncios pagos en Google o links en Telegram con letras parecidas (`rn` por `m`, `l` por `I`).	Guardar sitios oficiales en marcadores y nunca entrar desde links de terceros.
Falso soporte técnico	Un «agente» te escribe por DM en Discord/Telegram pidiendo «sincronizar tu wallet» con tus 12 palabras.	Ningún soporte real te escribe primero ni pide jamás tu frase semilla.
Airdrop / NFT trampa	Aparece un token «gratis» en tu billetera que te invita a un sitio a «reclamar $500».	Ignorarlo por completo; al intentar canjearlo te hacen firmar un drenador.
Envenenamiento de historial	Un atacante te manda $0.001 desde una dirección con los mismos 4 primeros y 4 últimos caracteres que un contacto tuyo.	Nunca copiar direcciones desde el historial reciente sin revisar el medio y el contacto original.

SECCIÓN 02 · QUÉ FIRMÁS REALMENTE

Entender `Approve` y `Permit` antes de tocar Confirmar

Cuando interactuás con una app descentralizada (como un exchange DeFi), no siempre hacés un envío directo: muchas veces firmás un **permiso (Approve)** para que un contrato inteligente pueda gastar tus tokens en tu nombre.

El peligro aparece cuando firmás un permiso **ilimitado** en un contrato malicioso: aunque en ese instante tu saldo no baje, el atacante puede vaciar todos tus USDC un minuto o tres semanas después sin volver a pedirte firma.

✓ Buenas prácticas al firmar

Aprobá solo el **monto exacto** que vas a usar hoy. Usá billeteras modernas con simulador previo de transacción (como Rabby) que muestran en rojo si tu saldo va a bajar.

🧹 Limpieza mensual (Revoke)

Herramientas públicas auditadas como `revoke.cash` permiten ver qué contratos tienen permisos abiertos en tu billetera y revocarlos en un clic.

⚠️ Regla de la doble billetera (Bóveda + Bolsillo)

Jamás conectes la billetera donde tenés tus ahorros a sitios nuevos, juegos o pruebas. Creá una **billetera «bolsillo» (Burner)** con solo el monto justo para probar apps, y mantené tu **bóveda principal** sin conexiones externas.

SECCIÓN 03 · RESPALDO BLINDADO

Protocolo para guardar tus 12 o 24 palabras

Tu frase semilla (estándar BIP-39) es la llave maestra absoluta. Si se destruye tu computadora y tu celular en un incendio, esas 12 palabras escritas en papel o metal te devuelven acceso al 100% de tus activos en cualquier lugar del mundo.

✕ NUNCA hagas esto

- Sacar foto o captura de pantalla.
- Guardarla en Google Drive, iCloud, Notion o Notas.
- Enviarla por WhatsApp, Telegram o email.
- Escribirla en un sitio web o extensión.

✓ SÍ hacé esto

- Escribirla a mano en papel de calidad o placa de acero.
- Verificar la ortografía y el orden exacto (1 al 12).
- Guardar dos copias físicas en lugares seguros distintos.
- Probar una recuperación con $0 antes de depositar ahorros.

Protección extra para tus cuentas de Exchange

Activá siempre **2FA por aplicación autenticadora (Google Authenticator / Authy / Passkey)** y desactivá el 2FA por SMS (vulnerable a robo de chip / *SIM Swapping*). Además, habilitá la lista blanca de direcciones de retiro (*Withdrawal Whitelist*) en tu exchange.

SECCIÓN 04 · QUÉ HACER SI SOSPECHÁS COMPROMISO

Protocolo de 3 minutos si creés que firmaste algo malicioso

Si algún día cometés un error y conectás tu billetera a un sitio sospechoso, actuar rápido marca la diferencia:

🚨 **Pasos inmediatos en orden**

1. **Creá una billetera nueva limpia** (con frase semilla completamente nueva) en otro dispositivo seguro.
2. **Transferí primero los fondos sanos** hacia la billetera nueva antes de perder tiempo investigando.
3. **Revocá permisos sospechosos** en la billetera afectada y dejá de usar esa frase semilla para siempre si llegó a exponerse.

Recordá: si alguien conoció tu frase semilla, revocar permisos NO alcanza porque tiene control total de la billetera; en ese caso hay que abandonar esa semilla por completo.

SECCIÓN 05 · REFERENCIA RÁPIDA

Glosario de Seguridad Web3

Phishing
Suplantación de un sitio o soporte legítimo para robar credenciales o firmas.

Approve (Token Approval)
Permiso on-chain que autoriza a un contrato a mover tus tokens.

Drainer
Contrato malicioso diseñado para vaciar una billetera apenas firmás.

Burner Wallet
Billetera descartable con fondos mínimos usada para probar apps nuevas.

Revoke
Transacción que cancela permisos otorgados previamente a contratos externos.

SIM Swapping
Ataque telefónico que clona tu número para interceptar códigos SMS.

2FA App / Passkey
Segundo factor criptográfico local mucho más seguro que el SMS.

Address Poisoning
Envío spam desde una dirección casi idéntica para engañar tu historial.

🔓 **Desbloqueo automático en Hotmart Club**

Ingresá este código en el Quiz del Módulo 3 para habilitar el **Módulo 4: La Cooperativa Automática (DeFi y Smart Contracts)**.

`ESCUDO-SEED-2026`