Cybersecurity Best Practices

How Protocol Wealth protects information and how clients can help protect accounts.

Effective September 3, 2026 - Version Date September 3, 2026

Protecting client information is central to Protocol Wealth's operations. This disclosure summarizes safeguards we maintain and steps clients can take to reduce the risk of account compromise, fraud, and data exposure. It supplements our Privacy Policy and Client Advisory Agreement.

What Protocol Wealth Does

- Uses encryption in transit and at rest for sensitive information where appropriate.
- Applies access controls, multi-factor authentication, least-privilege permissions, and logging across core systems.
- Reviews vendors, custodians, and service providers for security and compliance posture.
- Maintains written information-security, incident-response, and identity-theft-prevention procedures.
- Uses data-minimization and supervisory controls for technology and AI-assisted workflows.
- Avoids sending client PII to public AI tools that are not authorized for that use.
- Monitors for suspicious activity and responds to incidents consistent with applicable law and firm procedures.

No technology system is perfectly secure. Cybersecurity controls reduce risk but cannot eliminate it.

What Clients Should Do

- Use multi-factor authentication on email, custodian, portal, exchange, and wallet accounts.
- Use a strong, unique password for each financial account.
- Use a password manager where appropriate.
- Verify wire, transfer, or disbursement changes by phone using a trusted number already on file.
- Be skeptical of urgent requests, unexpected links, attachments, QR codes, and payment instructions.
- Keep devices, browsers, and password managers updated.
- Avoid financial logins on public Wi-Fi or public computers.
- Do not share passwords, seed phrases, private keys, one-time codes, or recovery materials.
- Promptly notify Protocol Wealth and the relevant custodian if you suspect compromise.

Digital-Asset Security

Digital assets require additional care. Transactions are generally irreversible. Loss, theft, or compromise of private keys, seed phrases, MPC recovery materials, email accounts, devices, or wallet policies may result in permanent loss.

Protocol Wealth will never ask for your seed phrase or private key. Confirm wallet addresses and transfer instructions through a trusted channel before any transfer. Where applicable, use whitelists, dual approvals, velocity limits, and other wallet-policy controls.

Communications

Protocol Wealth will not ask for your password, PIN, private key, seed phrase, or one-time code. If you receive a suspicious communication that appears to be from Protocol Wealth, do not respond to that message. Contact us directly using a known phone number or support@protocolwealthllc.com.

Following reasonable security practices is part of the client's responsibilities under the Client Advisory Agreement. This guide is informational and does not expand or limit the liability terms of the applicable agreement.

Protocol Wealth, LLC is a registered investment adviser (CRD #335298). Registration does not imply a certain level of skill or training. Investing involves risk, including possible loss of principal; past performance does not guarantee future results. This is a disclosure, not a contract term. It states Protocol Wealth's current practice, is delivered before the Client Advisory Agreement is signed - section 5 of that Agreement records the delivery - and is superseded by a later edition rather than amended.