ensuro

DeFi Capital for a Smarter Future.

Cybersecurity Guide for Ensuro Protocol Investors

Updated March, 2025

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Executive Summary

This cybersecurity guide provides essential information for Ensuro Protocol investors to protect their eToken investments on the Polygon blockchain. As digital assets, eTokens require specific security measures to safeguard against various threats in the cryptocurrency ecosystem.

Key security measures include:

- Implementing multi-layered wallet security with hardware wallets for significant holdings
- Protecting private keys and seed phrases using offline storage methods
- Recognizing and avoiding sophisticated phishing attempts and social engineering attacks
- Understanding smart contract security principles and transaction verification
- Implementing proper backup procedures and incident response protocols

By following these guidelines, investors can significantly reduce the risk of unauthorized access to their assets while participating in the Ensuro Protocol ecosystem.

Disclaimer: **This guide provides general information for educational purposes only and does not constitute professional security advice. The cryptocurrency landscape evolves rapidly, and new security threats emerge regularly. Consult with cybersecurity professionals for personalized guidance. Ensuro Re Limited and its affiliates do not assume liability for any security incidents that may occur.**

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Table of Content

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Introduction

The Ensuro Protocol operates as a decentralized insurance platform on the Polygon blockchain, allowing investors to provide liquidity through eTokens. This creates opportunities for returns, but it could also present security challenges that differ from traditional investments.

This guide has been developed to ensure all Ensuro Protocol investors understand the cybersecurity landscape and can implement appropriate protective measures. The information is relevant for investors from all countries except the United States and nations under international sanctions, since they cannot participate in the Ensuro Protocol.

Blockchain Security Fundamentals

The Blockchain Security Model

The Polygon blockchain, which hosts the Ensuro Protocol, utilizes distributed ledger technology to provide security through decentralization. The blockchain itself is highly secure, however, most vulnerabilities exist at the access points where users interact with the system.

Key security aspects include:

- **Immutability:** Once transactions are confirmed, they cannot be altered or reversed
- **Transparency:** All transactions are publicly visible, though wallet ownership can remain pseudonymous
- **Consensus mechanisms:** Multiple validators must agree on transaction validity
- **Access control:** Private keys provide the only means of authorization

Wallet Types and Security Implications

Your cryptocurrency wallet is the primary interface for managing your eTokens. Different wallet types offer varying levels of security and convenience:

Wallet Type	Description	Security Level	Best Use Case
Hardware Wallets	Physical devices storing keys offline	Highest	Long-term storage, large investments
Desktop Wallets	Software applications on computers	Medium-High	Regular transactions with moderate security
Mobile Wallets	Smartphone applications	Medium	Small amounts, convenience

Web Wallets	Browser-based interfaces	Lower	Small amounts, high convenience
Exchange Wallets	Custodial accounts on exchanges	Varies	Active trading only

Recommended wallet options:

Hardware wallets:(examples)

- **Ledger Nano X/S Plus:** Supports Polygon network through the Ledger Live application, offers excellent security features through a secure element chip that protects your private keys
- **Trezor Model T/One:** Comprehensive support for multiple chains including Polygon, featuring an open-source approach to security
- **KeepKey:** Larger display for easier address verification, integrates with ShapeShift platform
- **BitBox02:** Minimalist design with emphasis on simplicity and security, includes backup options

Advantages: Resistant to malware, keeps private keys offline, physical confirmation of transactions

Considerations: Requires physical security, proper backup procedures, firmware updates

2. Software wallets (examples)

- **MetaMask:** Browser extension and mobile app with Polygon network support via custom RPC configuration
- **Trust Wallet:** Mobile solution with extensive compatibility and built-in dApp browser
- **Coinbase Wallet:** User-friendly option with good security features and direct integration with Coinbase exchange
- **Alpha Wallet:** Open-source mobile wallet with focus on DeFi applications

Advantages: Easier for frequent transactions, more convenient for DeFi interactions

Considerations: Security depends on device safety, vulnerable to malware if device is compromised

Security recommendation: Use a combination approach—maintain small amounts for transactions in a software wallet while storing the majority of holdings in a hardware wallet. Consider a multi-wallet strategy that distributes assets across different security solutions based on frequency of use and amount stored.

Critical Security Practices for eToken Investors

Private Key Management

Your private key is the single most important security element. whoever possesses it has complete control over your assets.

Essential practices:

1. **Never share your private key or seed phrase** with anyone, including individuals claiming to represent Ensuro support

- No legitimate cryptocurrency service will ever ask for your private key or seed phrase
- Support staff should provide solutions without requiring access to your funds

2. **Store offline only**, preferably in a hardware wallet or written on paper/metal in a secure location
    - Paper storage: Use archival-quality paper and waterproof ink
    - Metal storage: Provides protection against fire, water, and physical deterioration
    - Hardware wallet: Stores keys in a secure element that prevents extraction
3. **Use multiple storage locations** for recovery seed phrases:
    - Primary: Fireproof safe such as SentrySafe or Honeywell security box
    - Backup: Metal storage solutions like CryptoSteel, Billfodl, or ColdTi
    - Consider geographic distribution to protect against localized disasters
4. **Consider key-splitting protocols** for significant holdings, where different portions of your key are stored in separate locations
    - Shamir's Secret Sharing: Splits your seed into multiple parts, requiring a minimum threshold to reconstruct
    - Social Recovery: Designates trusted contacts who can collectively help recover access
    - Multisignature wallets: Require multiple keys to authorize transactions
5. **Implement encryption for any digital records**
    - Use strong encryption programs like VeraCrypt or PGP
    - Store encrypted backups on multiple devices or cloud storage
    - Maintain separate passwords for encryption that differ from wallet passwords

Warning signs of compromise:

- Unexpected transactions in your wallet history
- Login notifications from unexpected locations
- Unusual website behavior when connecting your wallet

- Changes in account settings you did not initiate
- Unauthorized device authorizations
- Failed login attempts or password reset requests

Avoiding Sophisticated Phishing Attacks

Phishing attacks have evolved significantly and now include AI-generated deepfakes and highly convincing website clones specifically targeting cryptocurrency investors.

Protection strategies:

1. **Verify all URLs carefully** before connecting your wallet
    - Legitimate Ensuro URL: https://ensuro.co
    - Phishing examples: https://ensuro-protocol.co, https://ensur0.co
    - Check for SSL certificates (https://) but remember that phishing sites can also have SSL
    - Pay special attention to IDN homograph attacks that use similar-looking Unicode characters
2. **Bookmark official websites** and always access them through bookmarks
    - Create a dedicated bookmark folder for cryptocurrency services
    - Avoid clicking links in emails, social media, or messaging apps
    - Type URLs directly when setting up bookmarks initially
3. **Verify communications through multiple channels**
   Official announcements will appear on the Ensuro Blog, Twitter, and Telegram almost simultaneously
    - Be especially suspicious of "urgent" requests or time-limited offers
    - Contact Ensuro through official channels if you receive suspicious communications
    - Remember that legitimate services never ask for your seed phrase or private keys
4. **Watch for advanced deception tactics:**

- Deepfake videos of Ensuro team members
- Fake "security alerts" claiming your account needs attention
- Impersonation of community managers in chat groups
- Fraudulent emails announcing "airdrops," "rewards," or "exclusive opportunities"
- Counterfeit mobile applications mimicking legitimate wallet apps

5. **Set up dedicated devices** for high-value transactions when possible
   - Consider using a separate computer exclusively for cryptocurrency management
   - If using a dedicated device isn't feasible, use a separate browser profile
   - Consider boot-from-USB secure operating systems for critical transactions
6. **Implement email security best practices**
   - Use a separate email address for cryptocurrency-related accounts
   - Enable advanced security features on your email provider
   - Be suspicious of attachments or unexpected PDF documents
   - Implement DMARC, SPF, and DKIM on personal domains if applicable
7. **Monitor community channels for reported scams**
   Follow security threads on the Ensuro community forum
   - Subscribe to Ensuro's security notification channels
   - Report suspicious activity to help protect the community

Common phishing scenario: Be wary of messages claiming to be from Ensuro support that request "wallet verification" due to security updates. These are typically phishing attempts designed to gain access to your wallet.

Smart Contract Security Awareness

The Ensuro Protocol operates through smart contracts on the Polygon network. Understanding their security model helps investors make safer decisions.

Smart contract security factors:

1. **Code audits:** Ensuro's smart contracts undergo regular security audits by firms such as Quantstamp:https://github.com/ensuro/ensuro/blob/main/audits/Quantstamp-Ensuro-Final-Report-2022-11-09.pdf
    - Audit reports are published at https://docs.ensuro.co/ensuro-docs/audits
    - Review dates of audits and severity of any identified issues
2. **Contract verification:** Only interact with verified contracts on the Polygon blockchain
    - Verify contract addresses through the official Ensuro documentation
    - Check contract verification status on PolygonScan (look for the green checkmark)
3. **Permission awareness:** Understand what permissions you grant when approving contracts Use approval tools like Revoke.cash to manage contract permissions
    - Consider approving only the specific amount needed for a transaction rather than unlimited approvals
4. **Stay informed about upgrades:** Smart contract updates can change functionality
    - Follow the Ensuro Blog and Social Media for announcements about protocol upgrades
    - Be wary of unofficial announcements about contract changes

Secure Transaction Practices

When transacting with eTokens, follow these verification procedures to prevent errors and fraud:

1. **Address verification protocol:**
    - Always copy addresses directly from official sources
    - Verify the first 4 and last 4 characters manually
    - Send a test transaction with a minimal amount before large transfers
    - Use the address book feature in your wallet for frequently used addresses
2. **Gas fee management on Polygon:**

- Typical transaction costs: $0.01-0.05 (significantly lower than Ethereum)
- Keep sufficient MATIC tokens for gas fees (approximately 1-5 MATIC is sufficient for numerous transactions)
- Check current gas prices at https://polygonscan.com/gastracker
- Consider transaction priority needs when setting gas prices

3. **Transaction signing safety:**
   - Review all transaction details before signing, especially:
     - Recipient address
     - Transaction amount
     - Network fees
     - Smart contract interactions
   - Verify transaction details on both your wallet interface and hardware device when using a hardware wallet

Multi-Factor Authentication Implementation

Implement multiple layers of authentication to prevent unauthorized access to your accounts and wallets.

Recommended MFA approaches:

1. **Authenticator apps** (preferred):
   - Google Authenticator
   - Authy
   - Microsoft Authenticator

   Benefits: Not vulnerable to SIM swapping, works offline

2. **Hardware security keys:**

- YubiKey
- Thetis FIDO2

Benefits: Phishing-resistant, requires physical possession

3. **Avoid SMS-based authentication** whenever possible due to SIM swapping vulnerabilities

Implementation points:

- Enable 2FA on exchange accounts, web wallets, and email accounts associated with cryptocurrency
- Store backup 2FA recovery codes securely with your seed phrase
- Consider a separate device specifically for authentication (old smartphone without SIM card)

Software and Firmware Maintenance

Outdated software often contains security vulnerabilities that can be exploited by attackers.

Update protocol:

1. **Wallet software updates:**
   Set automatic update notifications for desktop/mobile wallets
   - Verify update authenticity by downloading only from official websites
   - Schedule monthly update checks on your calendar
2. **Hardware wallet firmware:**
   Check for updates every 2-3 months
   - Follow the official update process exactly

- Verify the authenticity of update prompts through the manufacturer's website

3. **Operating system and browser security:**
   - Keep your operating system updated with security patches
   - Use browsers with security features (Firefox, Brave)
   - Install reputable antivirus/anti-malware software
   - Consider a dedicated device for cryptocurrency transactions

Additional Security Considerations

Security Implications of Network Interactions

Understanding how the Polygon network interfaces with the Ensuro Protocol can help you identify and mitigate potential vulnerabilities:

1. **Remote Procedure Call (RPC) endpoint security:**
   - Use trusted RPC endpoints when configuring your wallet for Polygon
   - Be aware that malicious RPC endpoints can monitor transactions or inject fraudulent requests
   - Consider running your own RPC node for maximum security if you have technical expertise
2. **Gas fee considerations specific to Polygon:**
   Polygon's gas fees are significantly lower than Ethereum's, but this can create security considerations
   - Attackers may attempt multiple small transactions that might go unnoticed due to minimal cost
   - Monitor even small transactions and set up alerts for any unauthorized wallet activity
3. **Bridge security when transferring assets:**
   - When moving assets between Ethereum and Polygon, use only official bridges

- Understand that cross-chain transfers introduce additional security variables
- Consider using reputable centralized exchanges as an alternative bridging method for large transfers

4. **Layer-2 specific vulnerabilities:**
   - Polygon validators have different security models than Ethereum mainnet
   - Understand that finality times and confirmation requirements differ from other networks
   - Consider waiting for multiple confirmations for high-value transactions on Polygon

Customized Security Based on Investment Size

Your security approach should scale with your investment amount in the Ensuro Protocol:

1. **Small investments** (under $5,000 equivalent):
   - Software wallet with strong password and 2FA
   - Basic backup procedures with paper seed phrase storage
   - Regular device security maintenance
   - Standard phishing awareness practices
2. **Medium investments** ($5,000-$50,000 equivalent):
   - Hardware wallet for majority of holdings
   - Software wallet only for frequent, smaller transactions
   - Multiple backup methods including metal storage
   - Enhanced verification procedures for all transactions
   - Regular security audits of your setup
3. **Large investments** (over $50,000 equivalent):
   - Cold storage for long-term holdings
   - Hardware wallet with multisignature setup
   - Air-gapped device for transaction signing

- Distributed geographic backups with redundancy
- Comprehensive security protocol with regular testing
- Consider professional security consultation

Mobile Device Security for Wallet Management

Mobile wallets are convenient but require specific security measures:

1. **Device security fundamentals:**
   - Use biometric authentication (fingerprint, face recognition)
   - Enable remote wipe capabilities
   - Install only official wallet applications from authorized app stores
   - Keep your device's operating system updated
   - Consider a dedicated device for crypto management
2. **Wi-Fi and connectivity security:**
   - Avoid using public Wi-Fi for cryptocurrency transactions
   - Consider using a VPN for additional connection security
   - Disable Bluetooth and NFC when not in use
   - Be cautious with QR code scanning from untrusted sources
3. **Application isolation:**
   - Use secure folders or work profiles to isolate financial applications
   - Consider app-level passwords in addition to device passwords
   - Regularly review app permissions
   - Use privacy screens to prevent visual "shoulder surfing"

Protecting Against Emerging Social Engineering Tactics

Beyond technical measures, be aware of psychological manipulation strategies:

1. **Investment FOMO exploitation:**
    - Be skeptical of "once in a lifetime" investment opportunities
    - Verify all investment proposals through official Ensuro channels
    - Understand that legitimate opportunities don't require immediate action
    - Follow a predetermined investment strategy rather than emotional decisions
2. **Technical support impersonation:**
    - Be aware that scammers may pose as wallet or protocol support staff
    - Legitimate support will never ask for your seed phrase or private keys
    - Initiate support contacts yourself through official channels rather than responding to outreach
    - Verify the identity of support personnel through multiple factors
3. **Community infiltration tactics:**
    - Be cautious of private messages from "community members" on Discord, Telegram, etc.
    - Verify the reputation and history of users offering assistance
    - Understand that scammers often build relationships before attempting exploitation
    - Report suspicious behavior to community moderators

Comprehensive Backup and Recovery Planning

Creating Resilient Backups

A robust backup strategy ensures you can recover assets even after device failure, theft, or disasters.

Essential backup components:

1. **Seed phrase backups** (highest priority):
    - Create at least two copies in different physical locations

- Consider geographical distribution for disaster protection
- Use durable materials:
  - Metal storage solutions (CryptoSteel, Billfodl)
  - Waterproof, fireproof document bags for paper backups
- Never store digitally unless using specialized encrypted storage solutions

2. **Access information backup** (separate from seed phrases):
   - Wallet addresses
   - Recovery emails
   - 2FA recovery codes
   - Instructions for heirs/family members in case of emergency
3. **Testing recovery procedures:**
   - Practice recovery on a new device at least once to verify backup integrity
   - Document the recovery process for future reference

Inheritance Planning

Ensure your digital assets remain accessible to designated beneficiaries in case of incapacitation or death.

Inheritance considerations:

1. **Create detailed instructions** for accessing your cryptocurrency assets
2. **Implement a "dead man's switch"** or time-lock solution
3. **Consider multi-signature wallets** that allow trusted individuals to collectively access funds
4. **Consult with an estate attorney** familiar with digital assets

Incident Response Protocol

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Immediate Actions for Suspected Compromise

If you suspect your wallet or private keys have been compromised, time is critical. Follow this response protocol:

1. **Transfer remaining assets** to a new, secure wallet from a different device immediately
2. **Revoke permissions** for any approved smart contracts using Revoke.cash
3. **Document the incident** including:
    - Suspicious transactions (transaction hashes)
    - Timeline of events
    - Any phishing messages or websites encountered
4. **Report to relevant parties:**
    - Ensuro Protocol support: info@ensuro.co
    - Local law enforcement cybercrime units
    - Relevant blockchain explorers (report addresses)

Recovery After Security Incidents

After securing any remaining assets, take these steps to recover and strengthen your security posture:

1. **Perform system security audit:**
    - Malware/virus scans
    - Factory reset compromised devices
    - Change passwords on all accounts using a secure device
2. **Review and improve security practices**:
    - Identify the vulnerability that led to the compromise
    - Implement additional security measures
    - Consider consulting with a cybersecurity professional

3. **Monitor for related activity:**
    - Set up blockchain alerts for your old addresses
    - Monitor credit reports and financial accounts for suspicious activity
    - Watch for follow-up phishing attempts (compromised accounts often lead to targeted attacks)

Emerging Threats and Defensive Strategies (2025)

Current Threat Landscape

The cryptocurrency security environment continues to evolve rapidly. These are the most significant threats facing investors:

1. **AI-powered phishing campaigns:**
    - Deepfake videos of Ensuro team members
    - AI-generated voice impersonation in support calls
    - Highly personalized spear-phishing based on public blockchain data
    - **Defense:** Verify communications through multiple official channels
2. **Cross-chain bridge vulnerabilities:**
    - Attacks targeting interactions between Polygon and other blockchains
    - Smart contract exploits in bridge protocols
    - **Defense:** Use trusted bridges only, verify contract addresses, consider direct fiat on/off ramps when possible
3. **Advanced malware targeting crypto wallets:**
    - Clipboard hijackers that replace addresses during copy/paste
    - Keyloggers specifically designed to identify seed phrase entries
    - **Defense:** Use hardware wallets, dedicated devices, and verify addresses on multiple screens

4. **Quantum computing threats on the horizon:**
    - While not immediate, quantum computing advances may eventually threaten current cryptographic systems
    - **Defense:** Follow developments in post-quantum cryptography, be prepared for protocol upgrades

Building a Security-First Mindset

Developing security awareness is your strongest defense against emerging threats:

1. **Stay informed** through reputable sources:
    - Ensuro Blog (blog.ensuro.co)
    - Polygon security announcements
    - Cryptocurrency security newsletters
2. **Participate in security discussions:**
    - Ensuro Community forums
    - Security-focused Discord channels
    - Professional cybersecurity communities
3. **Practice security hygiene:**
    - Regular security reviews of your setup
    - Periodic testing of backup and recovery procedures
    - Staying current on new security tools and practices

Appendix B: Technical Security Implementation Guide

Configuring MetaMask for Secure Polygon Network Interaction

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

For Ensuro Protocol investors using MetaMask, proper configuration enhances security when interacting with the Polygon network:

Secure Polygon network configuration:

Network Name: Polygon Mainnet

RPC URL: https://polygon-rpc.com/

Chain ID: 137

Currency Symbol: MATIC

Block Explorer URL: https://polygonscan.com/

1. **Recommended security settings:**
    - Enable "Advanced gas controls" in Settings > Advanced
    - Activate "Security alerts" in Settings > Security & Privacy
    - Disable "Show incoming transactions" if not needed
    - Consider using "Auto-Lock Timer" with a short duration
2. **Hardware wallet integration:**
    - Connect your Ledger or Trezor to MetaMask
    - Follow the device-specific connection instructions
    - Verify all transactions on both MetaMask and the hardware device
    - Enable Contract Data on your hardware device for smart contract interactions

Secure Creation of Multisignature Wallets

For enhanced security of significant holdings, consider implementing a multisignature wallet:

1. **Gnosis Safe setup process:**
    - Access the official Gnosis Safe interface at https://gnosis-safe.io/
    - Select the Polygon network
    - Connect your primary wallet
    - Set required confirmation threshold (e.g., 2 of 3 signers)
    - Add owner addresses (at least one should be a hardware wallet)
2. **Security considerations:**
    - Store owner information securely and separately
    - Distribute ownership across trusted individuals or your own devices
    - Test the recovery process with small amounts
    - Document procedures for heirs or emergency access

Implementing Address Whitelisting

Restrict transactions to only trusted addresses to prevent theft even if your wallet is compromised:

1. **Hardware wallet address whitelisting:**
    - Enable in device security settings
    - Add frequently used addresses to the allowlist
    - Require physical confirmation for any non-whitelisted address
2. **Smart contract allowance management:**
    - Use Revoke.cash to review and manage token approvals
    - Limit approval amounts to only what is needed
    - Regularly audit and revoke unnecessary approvals

Secure Backup Encryption Methods

For digital backups of critical information, implement strong encryption:

1. **VeraCrypt container setup:**
    - Create an encrypted container with strong encryption (AES-Twofish-Serpent)
    - Use a complex password or passphrase (minimum 20+ characters)
    - Store the container on multiple devices or secure cloud storage
    - Include wallet recovery instructions but NOT seed phrases in the same container
2. **Paper backup encryption:**
    - Consider BIP39 passphrase (25th word) for seed phrases
    - Use basic encryption methods like code substitution for written records
    - Split critical information across multiple physical locations

Advanced Transaction Verification

For high-value transactions, implement a rigorous verification process:

1. **Self-verification checklist:**
    - Verify recipient address on at least two different devices
    - Check transaction details under different screen brightness/angles
    - Confirm gas settings are appropriate but not excessive
    - Verify token types and amounts multiple times
    - Wait a predetermined "cooling period" before confirming
2. **Transaction simulation:**
    - Use blockchain explorers or tools like Tenderly to simulate transaction effects
    - Verify expected outcomes before signing
    - For complex smart contract interactions, understand all potential state changes

3. **Out-of-band verification:**
    - For transactions to exchanges or services, verify addresses via alternative communication channels

- Consider video calls for large peer-to-peer transactions
- Document verification steps for auditing purposes

Conclusion

Protecting your eToken investments requires implementing multiple layers of security and maintaining vigilance against evolving threats. No security system is perfect, however, following the practices outlined in this guide will significantly reduce your risk exposure.

Key takeaways:

1. Secure your private keys and seed phrases using appropriate offline storage
2. Implement hardware wallets for significant holdings
3. Verify all transactions carefully before approval
4. Maintain comprehensive backups with proper physical security
5. Stay informed about emerging security threats
6. Act quickly if you suspect any compromise

The Ensuro team is committed to maintaining the highest security standards, but ultimately, the security of your individual investments depends on implementing proper personal security practices.

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Appendix A: Security Resources

Wallet Security

- Ledger: https://www.ledger.com
- Trezor: https://trezor.io
- MetaMask: https://metamask.io
- Trust Wallet: https://trustwallet.com

Backup Solutions

- CryptoSteel: https://cryptosteel.com
- Billfodl: https://billfodl.com
- SentrySafe: https://www.sentrysafe.com

Ensuro Re Limited
Crawford House, 50
Cedar Ave,
Hamilton HM 11,
Bermuda

Security Tools

- Revoke.cash: https://revoke.cash
- PolygonScan: https://polygonscan.com
- Blockchain Explorer: https://explorer.matic.network

Educational Resources

- Ensuro Blog: blog.ensuro.co
- Polygon Documentation: https://docs.polygon.technology/docs/

Ensuro Support

- Ensuro Support: support@ensuro.co