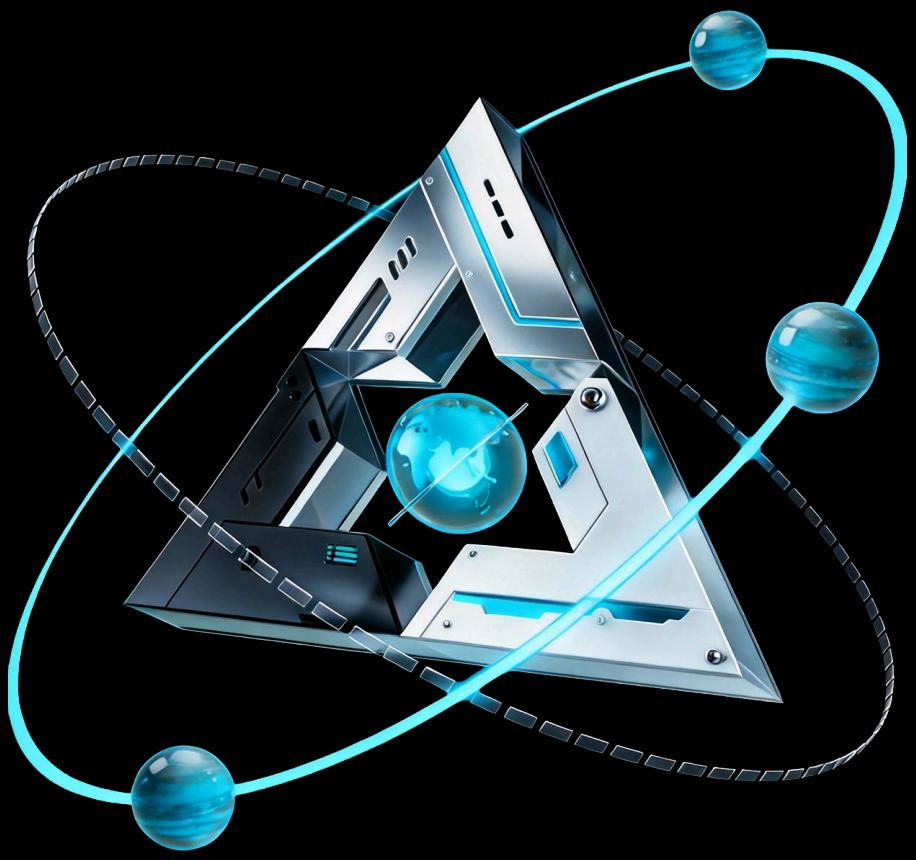
Bitget

UEX

Security Standards Report

2026



Bitget x BLOCKSEC

The UEX Security Standard:
From Proof to Protection

Executive Summary

As crypto exchanges evolve into Universal Exchanges (UEX), security must evolve with them. UEX platforms no longer protect a single asset class or settlement model. They operate across crypto, tokenized assets, and traditional markets, expanding the security perimeter to include custody, pricing, settlement, identity, compliance, and infrastructure, all within a unified account environment.

This shift introduces new systemic risks. Account-level permission failures can escalate into cross-asset liquidation events. TradFi-style data flows raise the stakes for privacy, compliance, and auditability. Volatility or pricing anomalies in one market can propagate across products through shared margin, settlement timing, or tightly coupled infrastructure. These risks cannot be addressed with asset-specific or reactive security controls.

This report, jointly authored by Bitget and BlockSec, defines a system-level security framework for the UEX era. It outlines five core standards designed to deliver continuous assurance across the full asset lifecycle: verifiable solvency, multi-asset risk isolation, high-standard data protection, AI-driven dynamic security, and resilient application and infrastructure defense.

Bitget anchors this framework in measurable safeguards, including a 163% Proof of Reserves ratio and a Protection Fund averaging $580 million. In collaboration with BlockSec, these foundations are reinforced through real-time monitoring, offensive security testing, incident response readiness, and compliance-grade controls such as AML screening and fund tracing.

Together, the framework moves UEX security beyond disclosure toward resilience, where correctness can be verified, risks can be contained, and trust can scale with complexity.

Table of contents

Background & Evolution: From Crypto Exchange to UEX

01

1.1/ Defining the Evolution of UEX: Crypto Security Combined with TradFi

UEX represents a fundamental redefinition of trading infrastructure. Early crypto exchanges were designed around a narrow security perimeter; on-chain assets, private key custody, and smart contract risk. In contrast, UEX platforms must securely support crypto-native assets alongside stocks, ETFs, commodities, Forex, and tokenized representations of off-chain value, all accessed through unified accounts and shared risk systems.

This convergence radically expands the security boundary. Once off-chain assets are introduced, platforms must prove not only cryptographic correctness, but economic correctness. That assets exist, records reconcile, settlement pathways function as intended, and pricing mechanisms remain consistent across jurisdictions and market hours. Off-chain dependencies such as brokers, custodians, registrars, clearing systems, cloud infrastructure, must be hardened against adversaries accustomed to exploiting Web3 systems at speed and scale.

UEX security therefore cannot be modular or asset-specific. Crypto-native protections must be integrated with TradFi-style isolation, governance, and auditability. Gaps between systems are no longer benign, they become attack paths. A unified exchange remains safe only when protection logic is consistent across domains and resilient under adversarial stress, not merely compliant under normal conditions.

1.2/ Common and Major Security Crises in Recent Years

Recent industry failures reveal a consistent pattern. Large-scale losses rarely originate from a single technical flaw. Instead, they emerge from structural weaknesses where governance, permissioning, and asset boundaries were assumed rather than enforced.

In crypto markets, incidents often stem from smart contract vulnerabilities, bridge design failures, private key compromise or misconfigured permissions, leading to immediate asset loss. In traditional finance, failures more commonly arise from account takeover, operational errors, compliance breakdowns, or internal control failures. As platforms evolve toward UEX models, these risks no longer remain isolated, they amplify each other. What these cases illustrate is that single-layer security models do not fail gracefully in UEX environments. When boundaries blur, failure propagates.

- **Case 1: FTX**

The core cause of FTX's bankruptcy was not market risk, but systemic misappropriation of user funds and governance failure by a centralized exchange. The platform failed to separate user assets from its own funds for an extended period, and used system-level permissions to grant affiliated trading entities risk control exemptions and unlimited leverage, masking real risk exposure. When market volatility and mass withdrawals hit, liquidity gaps were rapidly exposed, ultimately leaving user assets unpaid and triggering full bankruptcy. This became a textbook failure of centralized exchanges in fund segregation, risk control checks, and transparency.

https://arstechnica.com/tech-policy/2022/11/sam-bankman-frieds-32-billion-ftx-crypto-empire-files-for-bankruptcy/

FTX collapsed not because of market volatility, but because user assets were systematically commingled with platform and affiliate funds. Internal permissions bypassed risk controls, masking leverage and exposure until withdrawals exposed insolvency. This was not a trading failure — it was a governance and boundary failure, demonstrating how centralized trust without technical constraints collapses under stress.

- **Case 2: Ronin Network Bridge Attack**

In 2022, the Ronin Network cross-chain bridge was breached, and attackers stole about 624 million USD in assets. It became one of the largest blockchain thefts at the time and highlighted weak trust boundaries in cross-chain and DeFi infrastructure.

https://www.blocktempo.com/ronin-cross-chain-bridge-encounters-mev-attack/

These bridge exploits highlighted how weak trust boundaries and insufficient value verification allow local vulnerabilities to escalate into systemic losses. They remain cautionary examples for any UEX platform relying on cross-domain settlement and mapping logic.

1.3/ Complex Evolution of Security Threats

UEX transforms the attack surface from linear to systemic. Security must now contend with interactions across identity systems, pricing engines, settlement cycles, custody models, compliance logic, and infrastructure dependencies. The question is no longer “where can attackers break in,” but “how far can risk travel once something breaks.”

1.3.1 Account-Layer Risks

In UEX, accounts function as permission hubs rather than access credentials. They encode asset eligibility, leverage rules, compliance attributes, and cross-system authorizations. This makes identity bypasses and permission drift especially dangerous. A single compromised account can become a launch point for multi-asset liquidation cascades if controls are misaligned or monitoring is delayed.

Unified margin systems improve efficiency, but also compress risk. Differences in volatility profiles, liquidity windows, and trading hours can be exploited to create blind spots where permission abuse transitions into systemic exposure.

1.3.2 Data and Privacy Layer

UEX platforms inevitably process more sensitive data — identity verification, suitability assessments, AML signals, and third-party financial interactions. This data traverses multiple systems and jurisdictions, increasing the cost of misclassification or overexposure. Without strict minimization, classification, and auditability, privacy failures can escalate into regulatory and reputational crises.

1.3.3 Asset-Layer Risks

Asset security expands beyond wallet custody into off-chain settlement, clearing cycles, and the authenticity of mapped assets such as tokenized stocks and RWAs. Settlement delays, corporate actions, and counterparty failures introduce scenarios where execution and asset availability diverge. In these environments, solvency is not enough — assets must be custodial, settleable, reconcilable, and redeemable.

1.3.4 System Coupling Risks

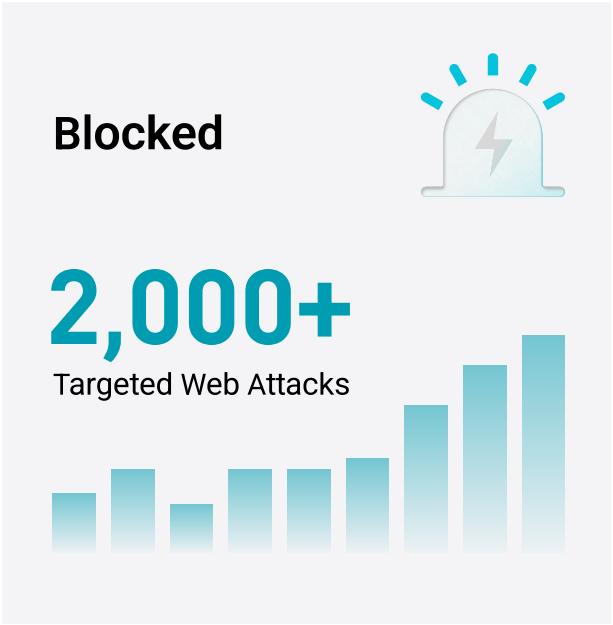
UEX platforms are tightly coupled ecosystems. Market data feeds influence pricing; pricing drives margin; margin triggers liquidation; liquidation interacts with external venues. A degraded API or delayed feed can ripple across the system. Unified collateral models intensify this coupling, making isolation and degradation strategies critical architectural concerns rather than operational afterthoughts.

Bitget's Security Philosophy: Building the Foundation for Industry Trust

02

2.1/ Review of User Protection Milestones

Bitget approaches security as an always-on operational discipline. Over the past year, its security operations processed more than 8,000 daily alerts spanning abnormal logins, suspicious transaction patterns, and anomalous on-chain activity — prioritizing early interception over post-incident remediation. In parallel, over 2,000 targeted attacks, including phishing infrastructure and impersonation attempts, were neutralized to protect user access and platform availability.



Transparency is treated as a protective layer. Monthly Proof of Reserves reports maintain an overall reserve ratio of 163%, supported by Merkle tree verification that allows users to independently confirm balances. The Protection Fund maintained average valuations near $577 million, with peaks exceeding $608 million, reinforcing financial resilience through volatile market conditions.

Latest reserve ratio

Snapshot time 2026-01-21 06:00:00 (UTC+8)

The reserve ratio is calculated by dividing the platform's assets by user assets. A ratio of 100% or higher means the platform can fully cover all user assets.

Merkle root hash

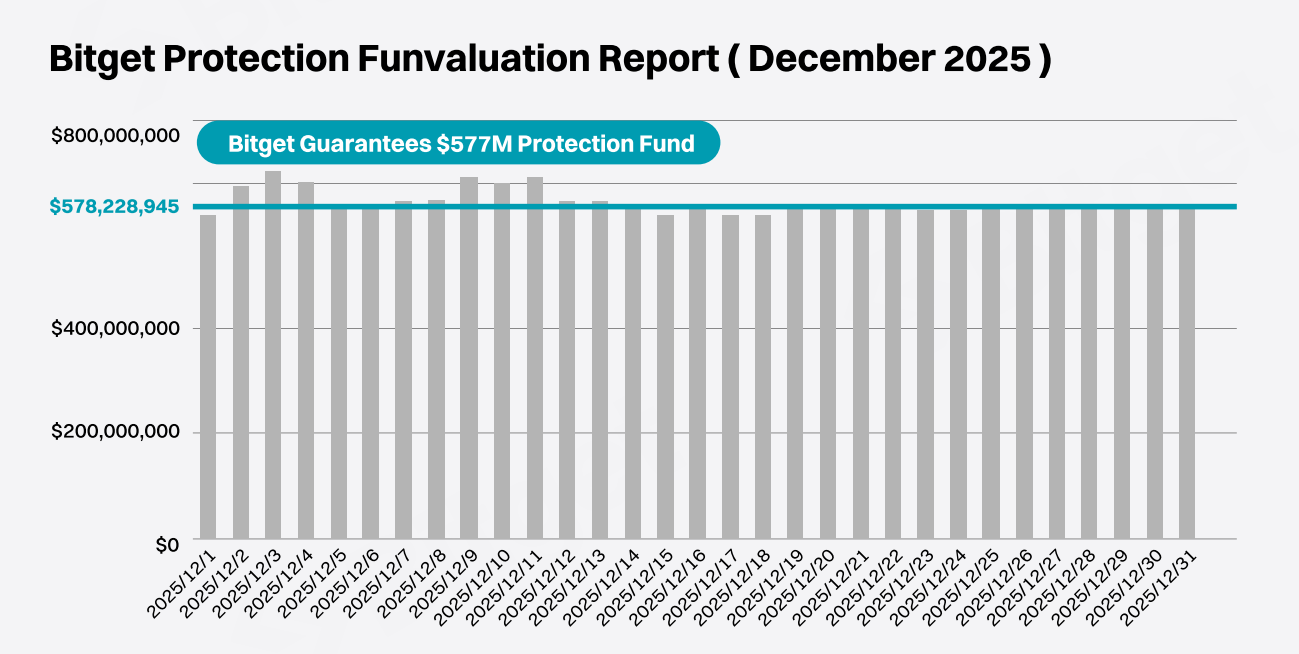
The Merkle tree, generated from all user balances, has 26 layers and 44,325,666 records.

00795643f17d7588

Total reserve ratio

Bitget holds more than 100% of user assets in BTC, ETH, USDT, and USDC.

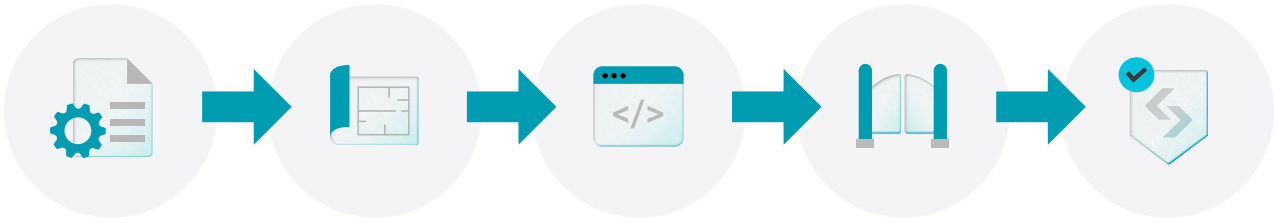
163%



Together, these measures translate security from promise into proof.

2.2/ Security Architecture DNA

Bitget's security architecture is UEX-native by design. Shift-left security embeds threat modeling, compliance constraints, and data governance at the earliest stages of development. Automated scanning, dependency controls, and security gates prevent high-risk artifacts from reaching production, while operational feedback loops ensure real-world attack patterns inform continuous hardening.



Risk isolation is engineered into account and product design. Unified trading accounts support efficiency while preserving isolation through configurable margin modes and sub-accounts. TradFi products operate within separate structures to reduce cross-domain contagion. Bitget's execution model avoids opposing user positions, collaborating with liquidity providers to diversify exposure and maintain stability.

Privacy governance is systemic. Encryption, access minimization, auditability, and third-party due diligence ensure confidentiality and integrity as data complexity grows.

Five Core Standards: Defining the Security Benchmark for the UEX Era

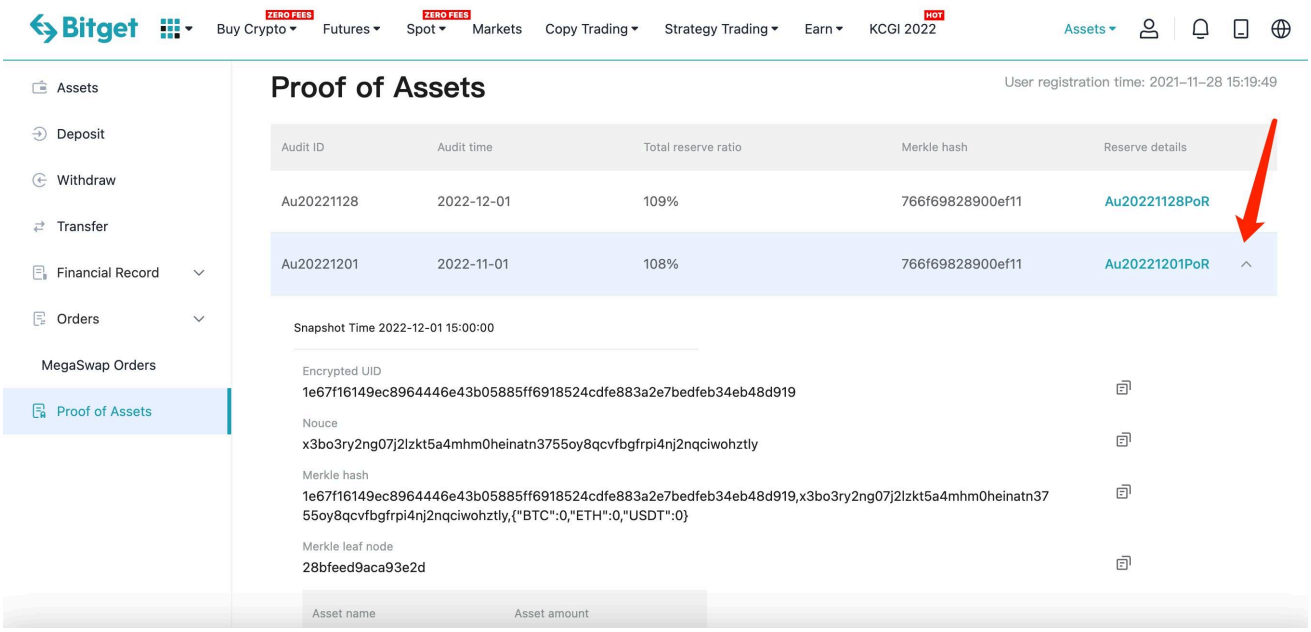
03

3.1/ Asset Protection and Solvency

UEX security begins with solvency that can be independently verified. Bitget's Proof of Reserves framework replaces trust statements with cryptographic evidence, ensuring immediate redemption confidence even during stress events. The Protection Fund provides an additional buffer for abnormal loss scenarios, with publicly verifiable reserves.

Monthly PoR Summary (December 2025)

Asset	Lowest reserve ratio	Highest reserve ratio	Average reserve ratio
BTC	260%	426%	339%
USDT	100%	173%	115%
ETH	147%	224%	179%
USDC	121%	281%	177%
Total	172%	213%	187%



Liquidation safety complements solvency. Segmented execution and staged liquidation logic reduce market impact, ensuring that localized risk does not escalate into systemic disruption.

3.2/ Multi-asset Risk Isolation

UEX requires isolation by design. Bitget applies tiered risk logic that respects the characteristics of each market while maintaining consistent protection intent. Concentration limits, exposure caps, and liquidity-aware liquidation strategies prevent single-asset shocks from propagating across the platform.

3.3/ Data Security and Privacy Standards

Data protection in UEX is driven by classification, minimization, and auditability. Controls are applied based on sensitivity rather than system origin, ensuring consistent protection across complex architectures. Cross-border access is tightly governed, supported by localized processing and shared oversight between security, legal, and compliance teams.

3.4/ AI-Driven Dynamic Security Practices

AI enhances security without becoming a new source of opacity. Bitget applies AI to anomaly detection and monitoring while constraining data usage, enforcing de-identification for external models, and retaining explainable decision paths for high-impact outcomes. AI augments human judgment rather than replacing it.

3.5/ Defensive Mechanisms for Applications, Cloud, and Infrastructure

Infrastructure resilience underpins UEX trust. Secure development lifecycle practices, zero-trust principles, multi-cloud deployments, and disaster recovery drills ensure continuity under extreme conditions. Third-party and supply-chain governance is treated as a security boundary, with continuous monitoring and strict integration controls.

Collaborative Protection: User Security and Risk Prevention Education 04

Users are part of the security model. Bitget integrates education, tooling, and verification mechanisms to reduce exposure to phishing, impersonation, and social engineering. Anti-phishing codes, official verification channels, and guided remediation workflows empower users to detect and respond to threats before losses occur.

Transparency Commitment: Emergency Mechanisms and Trust Assurance 05

Security is proven under pressure. Bitget operates a standardized incident response lifecycle spanning detection, containment, remediation, and recovery validation. Regular drills and red–blue exercises test readiness, while transparent disclosure balances accountability with responsible non-disclosure of exploitable details. Coordination with regulators and partners ensures consistent response across ecosystems.

The Next Step in UEX Security: Future Outlook 06

UEX security is entering a new phase defined by continuous, system-level assurance rather than isolated safeguards or periodic audits. As trading platforms expand across crypto-native and traditional financial assets, the benchmark for security shifts from incident avoidance to system resilience: the ability to contain loss, preserve correctness across markets, and produce verifiable, auditable evidence under adversarial conditions.

Bitget and BlockSec converge in this direction. As asset coverage, infrastructure complexity, and external dependencies grow, security architectures must evolve in parallel. Integrating differentiated risk models, hardened off-chain dependencies, and always-on monitoring across the full asset lifecycle. In this environment, security becomes an operating system rather than a feature set, where protection logic remains consistent across asset classes and responsibility boundaries are explicit and enforceable.

In the UEX era, security ultimately safeguards more than capital. It protects confidence, the assurance that users can trade, allocate and move value across markets without questioning whether the underlying infrastructure can keep pace with innovation, scale, and real-world financial complexity.

About Bitget

Bitget is the world's largest Universal Exchange (UEX), serving over 125 million users and offering access to over 2M crypto tokens, 100+ tokenized stocks, ETFs, commodities, FX, and precious metals such as gold. The ecosystem is committed to helping users trade smarter with its AI agent, which co-pilots trade execution. Bitget is driving crypto adoption through strategic partnerships with LALIGA and MotoGP™. Aligned with its global impact strategy, Bitget has joined hands with UNICEF to support blockchain education for 1.1 million people by 2027. Bitget currently leads in the tokenized TradFi market, providing the industry's lowest fees and highest liquidity across 150 regions worldwide.

For more information, visit: Website | Twitter | Telegram | LinkedIn | Discord

For media inquiries, please contact: media@bitget.com

Risk Warning: Digital asset prices are subject to fluctuation and may experience significant volatility. Investors are advised to only allocate funds they can afford to lose. The value of any investment may be impacted, and there is a possibility that financial objectives may not be met, nor the principal investment recovered. Independent financial advice should always be sought, and personal financial experience and standing carefully considered. Past performance is not a reliable indicator of future results. Bitget accepts no liability for any potential losses incurred. Nothing contained herein should be construed as financial advice. For further information, please refer to our Terms of Use.

About BlockSec

BlockSec delivers a full-suite Web3 security and compliance solution, spanning smart contract auditing, a real-time monitoring and threat-blocking platform, as well as crypto AML and forensic investigation platforms. Through Phalcon Compliance, customers can screen wallets and transactions for compliance risks, monitor suspicious activities in real time, and automate risk controls to meet regulatory and internal policy requirements. MetaSleuth enables fund-flow analysis to trace illicit proceeds and support investigations. Our 500+ customers include crypto exchanges, wallets, OTC desks, and financial institutions, along with regulators and law enforcement across 50+ jurisdictions.

Appendix

Recommended list of user security education articles

Account login and identity security

- Enable two-factor authentication (2FA), prioritize using Google Authenticator, and securely store backup information.
  Reference: https://www.bitget.com/en/support/articles/12560603821828
  Reference: https://www.bitget.com/en/academy/bitget-two-factor-authentication-2fa-guide
- If your device supports it, enable passkey to strengthen login security (usually after completing 2FA setup).
  Reference: https://www.bitget.com/en/support/articles/12560603821289
- Use a strong password and update it regularly. Avoid reusing it on other platforms. After changing your password, pay attention to any security protection restriction prompts on the platform.
  Reference: https://www.bitget.com/en/support/articles/12560603819255

Funds and trading security

- Set a fund code for secondary verification of critical actions such as withdrawals and 2FA modifications.
  Reference: https://www.bitget.com/en/support/articles/12560603821838
  Reference: https://www.bitget.com/en/support/articles/12560603821839
  Reference: https://www.bitget.com/en/support/articles/12560603821841
- Set a PIN code for additional verification during transactions/payments, reducing the risk of accidental operation and unauthorized use.
  Reference: https://www.bitget.com/en/support/articles/12560603819255
- Enable security features for withdrawals: Withdrawal address whitelist, cross-device withdrawal confirmation, and a buffer period that allows cancellation after initiating a withdrawal.
  Reference: https://www.bitget.com/en/support/articles/12560603820641
- Enable passkey for critical actions
  Reference: https://www.bitget.com/en/support/articles/12560603821290

Anti-phishing and official verification channel

- Set up an anti-phishing code to verify official emails and text messages. Watch out for fake notifications and impersonated customer support.
  Reference: https://www.bitget.com/en/support/articles/12560603821296
  Reference: https://www.bitget.com/en/support/articles/12560603816158
- Improve phishing awareness: Do not click links from unknown sources, and never share sensitive information such as verification codes, 2FA codes, passwords, or private keys with anyone.
  Reference: https://www.bitget.com/en/support/articles/12560603821287
  Reference: https://www.bitget.com/en/academy/guide-against-phishing-scams
- Use the official verification channel to verify authenticity and report suspicious accounts, links, or promotion information. Be vigilant against social engineering scams.
  Reference: https://www.bitget.com/en/support/articles/12560603826152

Devices and daily habits

- Regularly review trusted devices, logged-in devices, and account activity. If you spot anything unusual, remove the device promptly and update your security settings.
  Reference: https://www.bitget.com/en/academy/bitget-advanced-account-security-guide
  Reference: https://www.bitget.com/en/academy/an-advanced-security-guide-on-bitget
- On mobile, enable an app lock and other system security features to help prevent unauthorized account actions if your device is lost or borrowed.
  Reference: https://www.bitget.com/en/academy/an-advanced-security-guide-on-bitget