MID-YEAR

Security Checklist

Your partner in building a safer digital presence for banking.

As next year's budgeting and planning begin in earnest, here are seven key considerations that your bank should keep in mind to ensure a strong security stance.

.bank®

YOUR GOOD NAME, MADE STRONGER

Integrate technology, risk management, and marketing to strengthen your bank's defenses.

fTLD's Mid-Year Security Checklist includes actionable insights for bolstering:

01.
Cyber Hygiene & Operational Resilience

02.
Domain-Level Defense

03.
Advanced Encryption and Cryptographic Standards

04.
TLS Certificate Lifecycle Management

05.
Digital Fraud Protection & Identity Assurances

06.
Artificial Intelligence & Frontier Model Security

07.
Quantum Readiness & Cryptographic Agility

01.

Cyber Hygiene

& Operational Resilience

Securing the primary vector for financial fraud, business email compromise (BEC), ransomware, and phishing is critical.

01. Cyber Hygiene & Operational Resilience

- **REQUIRE** out-of-band verification for large wire transfers.
- **USE** our Domain Email Risk Assessment Tool to **check your email authentication.** Make sure it's harder for cybercriminals to spoof emails, keeping your bank and customers safe from phishing and online fraud.
- **AUDIT** email authentication across all operational domains. Move your DMARC policies to *p=reject* to **block unauthorized senders from impersonating** your domain.
  - **MTA-STS** should be enabled and set to 'enforce' on all email-enabled domains. This ensures the destination domain is valid and traffic is not being maliciously re-routed.
  - Secure non-email-enabled domains too with **DMARC** set to 'reject', and SPF of v=spf1 -all, which tells receiving mail servers that no IP addresses or services are authorized to send email for your domain, and any attempt should be rejected.
- **CHECK** that third-party platform senders (e.g., marketing automation, loan systems) are explicitly authorized within SPF records and correctly signing with 2048-bit DKIM keys.
- **CONFIRM** you're following our Email Deliverability Best Practices to keep your **bank's domain reputation** pristine.

Get Help

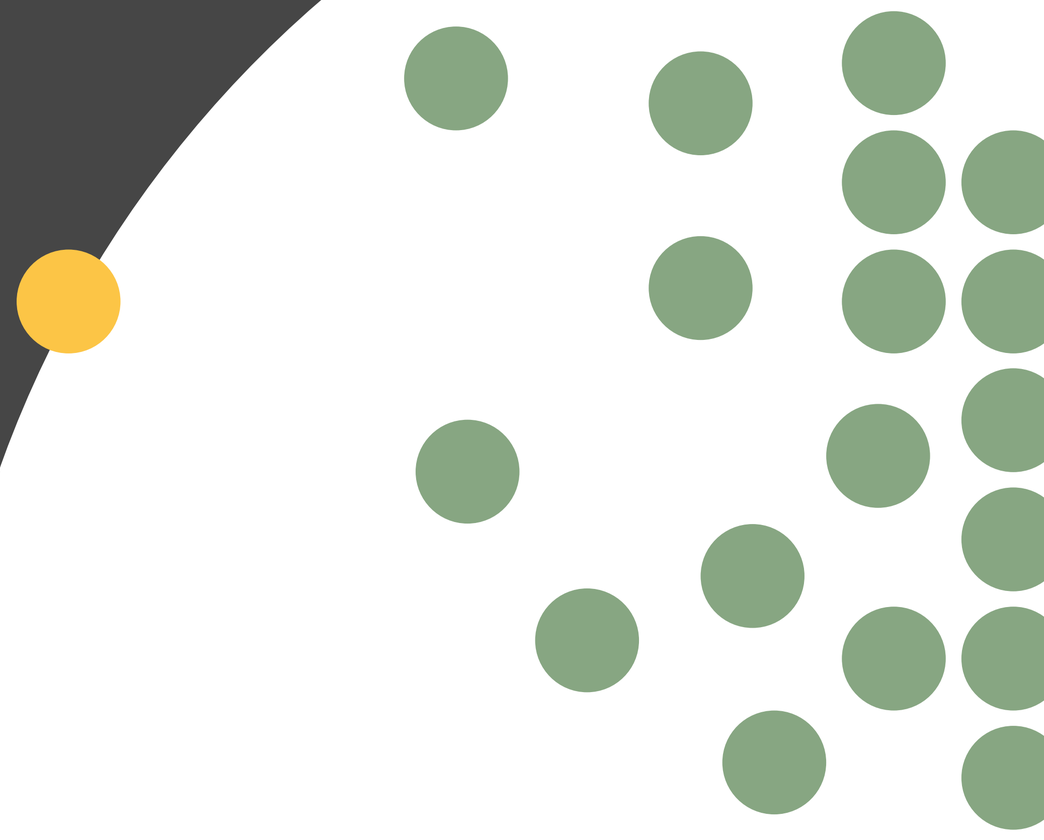
02.

Elevate Trust:

The Domain-Level Defense

Public domain extensions require manual, resource intensive monitoring. And even then, preventing lookalike domains is nearly impossible.

Moving to a verified, restricted domain —such as .Bank— mitigates this risk with mandated and monitored email authentication requirements, as well as by blocking registration of lookalike domains.



02. Elevate Trust: The Domain-Level Defense

REVIEW active remote management connections, session privileges, and updated security questionnaires for primary core providers and third-party IT managed service networks.

CHECK your domain supply chain.

- **Are you using a SOC2 or ISO 27001 certified registrar?**
  Your registrar should also be ICANN-accredited. fTLD carefully vets our registrar partners, giving you confidence and trust in them. Collect updated reports for critical vendors.

- **Web Hosting:**
  Utilize a **dedicated IP address,** rather than shared hosting for public-facing content when feasible. While more expensive, a dedicated IP isolates your server from malicious multi-tenant activity, protecting your performance, security, and sender reputation for reliable email delivery. It also avoids blocklisting or delayed remediation thanks to the exclusive IP tied to your trusted .Bank domain.

- **DNS Provider:**
  Engage your registrar or DNS provider to ensure they support **hybrid DNSSEC and certificate algorithms.** Automation is key to maintaining compliance and operational simplicity.

- **Review your domain contacts.**
  Ensure only full-time employees with the appropriate authorizations are listed for your domains.

- **Ensure Multi-Factor Authentication (MFA)**
  is comprehensively enforced across all remote access points, SaaS applications, and privileged internal accounts. Move away from SMS-based MFA wherever possible, favoring phishing-resistant methods (e.g., passkeys).

VALIDATE Brand Trust Indicators. If the login screen looks identical to a generic template, it is easy for a fraudster to clone. A website should implement dynamic, personalized, and context-aware elements that a malicious actor cannot easily predict or duplicate.
Review customer-facing visual markers of security:

- Use BIMI or a verified domain for email authenticity and trust.
- Review strict enforcement of your brand standards across your website(s).
- Give customers visual, in-context security features and alerts (such as alerting a client via a visual banner when they are adding a new wire transfer recipient).
- Add visual security features for logging in (such as last login date and location, MFA-options like a visual security indication, or in-context code requirements).

ENSURE consumer education materials on phishing are updated for current attack patterns. Consider sharing the .Bank Insight on: Phishing: A Cybersecurity Threat Overview for Banks across your social channels.

PLAN your switch to .Bank. Make cybersecurity and trust a visible feature–if it's not .Bank, it's not your bank.

Get Help

Operating within a gated, verified .Bank domain provides an instant visual trust indicator.

Let Us Help You Simplify
Your Marketing Trust Initiatives.

03. 04. 05.

Securing the Digital Banking Ecosystem

Advanced Encryption, TLS Certificate Management & Digital Fraud Protection

Strong security depends on more than a single control. Banks need resilient encryption, proactive certificate management, and layered identity protections.

Together, these safeguards help protect data in transit, reduce disruption, and maintain trust across customer-facing digital channels.

03. Advanced Encryption & Cryptographic Standards

PROTECTING data in transit against sophisticated interception capabilities is critical to your bank. By implementing the .Bank Security Requirements, you ensure your bank benefits from **industry-best protocols** for in-transit encryption, HSTS (HTTP Strict Transport Security) to prevent downgrade attacks, and strong email authentication.

- Enforce TLS 1.2 at a minimum, transitioning to **TLS 1.3** as standard.
- Review **cipher suites.** Disable weak, vulnerable cipher suites (e.g., RC4, 3DES, CBC-mode ciphers). Prioritize perfect forward secrecy (PFS) ciphers like ECDHE.

04. TLS Certificate Lifecycle Management

MITIGATE service disruptions, application dropouts, and expired certificate warnings.

- Compile an active **inventory of all TLS certificates** across consumer banking portals, websites, internal applications, and vendor APIs.
- Publicly trusted TLS server certificates are moving to shorter maximum lifetimes under CA/Browser Forum rules adopted on April 11, 2025. Prepare workflows and configuration scripts for **shortened industry-standard certificate lifecycles,** migrating toward automated renewal issuance using trusted ACME providers integrated with DNS-based validation.

05. Digital Fraud Prevention & Identity Assurances

DEFEND online banking ecosystems from account takeovers and customer-facing fraud.

- Audit MFA. **Enforce MFA** across all customer portals and employee access vectors. Transition from SMS-based verification to phishing-resistant methods.

Get Help

06.

Artificial Intelligence

& Frontier Model Security

AI has moved from an experimental technology to core infrastructure, making governance, data loss prevention, and protection against AI-driven fraud top priorities.

Artificial Intelligence & Frontier Model Security

- **MAP** the "Shadow AI" perimeter and audit your environment for **unauthorized generative AI tools.** Leverage web filters and Cloud Access Security Brokers (CASBs) to identify where employees may be pasting sensitive corporate data or customer NPI (Non-Public Personal Information) into external models.

- **ESTABLISH** Model Context Protocol (MCP) governance **if your institution uses AI agents** that connect directly to internal data silos via MCP pipelines, and ensure these connections are treated as high-security transit zones. Audit the access permissions of these agents to ensure they observe strict principle-of-least-privilege boundaries.

- **CONDUCT** a simulated deepfake drill targeting wire transfer, treasury management, or HR teams. Train staff to recognize synthetic voice or video requests and enforce out-of-band verification protocols for any high-value transactions.

- **UPDATE** secure email gateways (SEGs) with AI-driven phishing detection and behavioral analysis. Traditional rule-based indicators often miss the highly tailored, grammatically flawless phishing emails generated by threat actors utilizing LLMs.

Get Help

07.

Quantum Readiness

& Cryptographic Agility

“Harvest now, decrypt later (HNDL)” is the most immediate risk threatening your systems tomorrow. Adversaries can intercept and store encrypted bank traffic today, then decrypt it later when cryptanalytically relevant quantum computers become available.

Quantum Readiness & Cryptographic Agility

- **COMPLETE** your cryptographic inventory and document where classical public-key cryptography—specifically RSA and Elliptic Curve Cryptography (ECC)—is currently securing your perimeter, VPN endpoints, TLS certificates, and core banking APIs.
- **ESTABLISH** a crypto-agility baseline and verify whether your critical applications and network architecture can support modular cryptographic changes. Ensure your systems can transition to NIST-approved post-quantum algorithms (such as ML-KEM for key encapsulation and ML-DSA for digital signatures) without requiring complete software rewrites.
- **INITIATE** a hybrid encryption pilot and test quantum-safe hybrid encryption (combining a classical algorithm with a post-quantum algorithm) on a single, low-risk network channel or API gateway. Measure the impact on handshake sizes, network latency, and interoperability.
- **REVIEW** core provider post-quantum cryptography (PQC) roadmaps and issue specific inquiries to your core processing and critical third-party technology providers. Demand to see their documented transition roadmaps for post-quantum readiness and ensure their timelines align with federal regulatory expectations.

Get Help

Contact fTLD for email authentication vendor referral or DMARC doubts, or for a guide on how to communicate your switch to .Bank.

We're here to help your bank elevate its security.

.bank®

YOUR GOOD NAME, MADE STRONGER