fTLD
Registry Services, LLC

June 21, 2017

Approaching Cybersecurity on All Fronts: What Small Banks Need to do to Protect Themselves

During the email implementation of Summit Bank's .BANK domain, monitoring messages sent on behalf of the bank revealed emails from its own .COM domain originating in China – a clear sign of spoofing activity. This was an eye-opening moment for the Florida-based community bank, and reinforced the decision to fully implement Domain-based Message Authentication, Reporting and Conformance (DMARC) for email to eliminate spoofing entirely. With .BANK as part of the solution, Summit significantly improved its cybersecurity standards.

Summit Bank's Executive Vice President and COO, Frank Hall, shared the story as a cautionary tale: cyber threats pose significant challenges to financial institutions of all sizes (not just the large ones) and layered security is critical to managing cybersecurity and reputational risk.

It's that philosophy that has pushed Summit to incorporate cybersecurity into its brand identity. As a community bank focused on small business clients, maintaining a reputation of trust and security in the community is of the utmost importance.

During a discussion with fTLD Registry Services (fTLD), operator of .BANK, executives at Summit outlined their approach to layered bank security, which they contend is an industry-leading standard for all banks and is particularly important for community institutions:

- **Make Security Awareness a Priority**
  It's important that security awareness extends beyond the IT department. Every bank should train and test associates on email and malware threats and consider ways to educate clients – especially small businesses – on tactics to reduce risk.

- **Approach Network Security From All Sides**
  A must-have for any bank, multi-level private network security controls are critical. Among the most common security layers are firewalls, intrusion detection and protection systems, anti-virus and anti-malware software, email scanning, vulnerability scanning and patching, and VPN controls for remote access.

- **Use a Trusted Domain**
  Summit switched to a .BANK domain recently. fTLD mandates all financial institutions using its domain names adhere to a strict set of security requirements that include a range of robust cybersecurity practices and technologies – including email authentication, strong encryption, Domain Name System Security Extensions (DNSSEC)

and ongoing registrant verification. In addition, fTLD monitors for compliance with these security requirements and notifies registrants of any issues that are identified. This is particularly important for community banks that often don’t have the resources or expertise to implement these safeguards on their own. Landy Dutton, Summit Bank’s VP and Internal Audit Manager, noted “Community banks who do not have the depth of knowledge in this area can benefit and further secure their transaction streams by implementing these security requirements developed by banking industry and security experts for this trusted domain.”

- **Incorporate Client-Based Tools**
  Internal cybersecurity strategies only extend so far. Summit Bank recommends working directly with clients to incorporate additional tools to help identify malware and other threats as well as to provide a secure browser session for financial transactions. These tools provide a way for banks to assist clients with threat identification while mitigating attacks such as man-in-the-middle, man-in-the-browser and key logging.

- **Employ the Personal Touch**
  While large banks process huge volumes of transactions, community banks have a distinct advantage. They can (and should!) watch every single transaction to ensure there is no criminal or unusual activity. This personal approach introduces a human factor to spotting cyber-fraud and reinforces the importance of direct client relationships. At Summit Bank, this approach includes a phone call to any client requesting a wire transaction unless it was made in person. It’s also a useful time to further educate customers on the latest fraud and malware techniques.

For Summit Bank, a multi-layered approach has proven to be the best way to safeguard client accounts and business activities while also serving to bolster its image as a security-centric banking brand. As Hall put it, “There is no greater reputational risk to a community bank these days than a major cyber attack.”