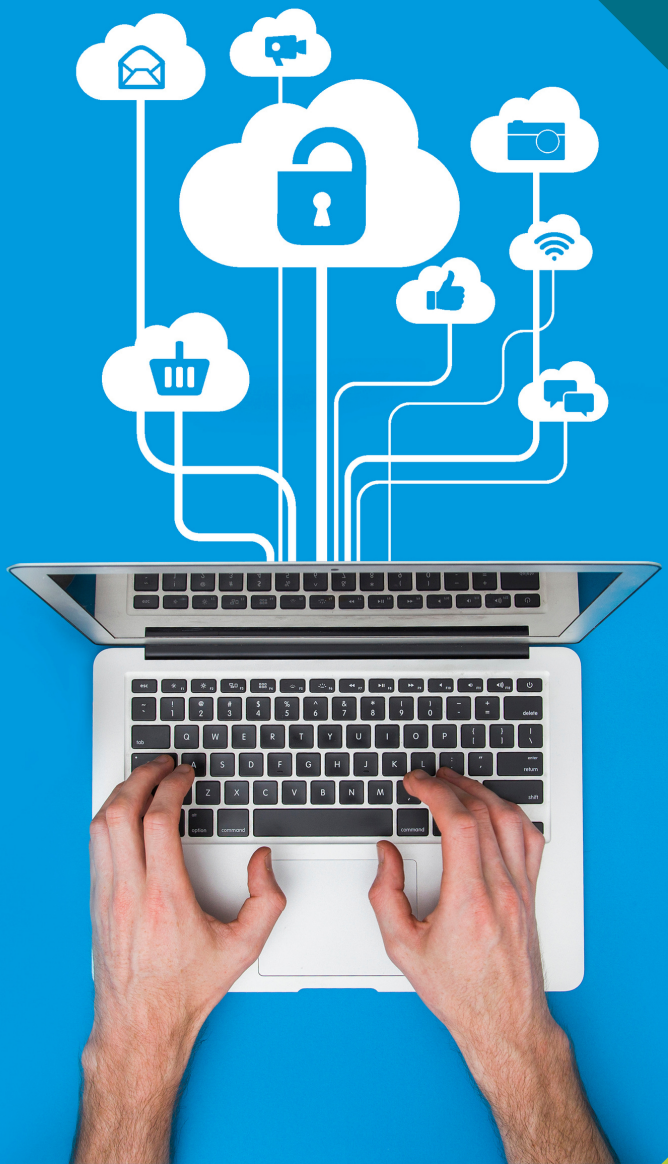
.BANK vs the Open & Unrestricted Internet



The challenge inherent in the open, unrestricted internet for banks

A near entirety of internet cyberattacks stem from the simple problem of authentication (i.e., knowing definitively who or what you're interacting with). Malware, ransomware, BEC, breaches, identity theft, and financial fraud all most commonly originate from interactions with phishing emails or spoofed websites from bad actors pretending to be someone they're not.

The overwhelming majority of the internet, banks included, operates within open, unrestricted TLDs (e.g., .com .net, .co, .org), where for just $10-$15 anyone can get any domain for any purpose. We're forced to rely on the cyber-savviness, investigative ability, and persistence of end-users to keep everyone safe, even though decades of education around cybersecurity hygiene (i.e., best practices for staying safe online) and the simultaneous rampant growth of these cyberattacks indicates a new approach to cybersecurity is long overdue.

While there is a near-constant flow of innovation attempting to solve this challenge for organizations that need to authenticate their customers, there hasn't been the same progress in the other direction, making it easy for customers, employees, and vendors to definitively authenticate their interactions with organizations.

We need a way to prevent the singular 'bad clicks' that expose organizations and individuals to cyberattacks. It's evident that people are unable, or unwilling to consistently do all that is necessary to verify who they're engaged with online via emails/websites. The process of identifying these attacks within open, unrestricted domains is a moving target, it's simply too complex to keep everyone continuously prepared and vigilant. After all, bad actors spend all of their time and resources improving their techniques, whereas the general public, and organizations like banks, simply can't dedicate as much time and resources to their own defenses.

How .BANK addresses this challenge

The banking industry decided it was time for a new approach for defending banks and their customers against cyberattacks, one simple enough to become a permanent part of everyone's cybersecurity hygiene. Interestingly a big part of the answer was first implemented when the first six TLDs were established in .com, .net, .org, .edu, .gov, and .mil. The .edu, .gov, and .mil domains have restrictions on who can get and use domains, making it clear to visitors of these domains that they are interacting with schools, government bodies, or the U.S. Department of Defense.

In 2015 the banking industry, via fTLD Registry Services, took a similar approach when it created the .BANK TLD to protect banks. The .BANK domain is restricted to verified banks (and their associations) by way of a thorough, multi-step verification process which verifies the organization is eligible, the individual requesting the domain has authority from the bank to register and manage the domain (verified through the C Suite of the bank), and that the domain name being requested matches the bank's name or a trademarked product/slogan. This process keeps out bad actors and ensures that seeing ".bank" at the end of an email address or website URL means you are in fact interacting with a bank (or bank association).

However, the banking industry, responsible for the governance of .BANK, decided to take their cybersecurity a step further and developed Security Requirements that banks must comply with to use their .BANK domains. These continuously monitored Security Requirements add multiple layers of cybersecurity, including email authentication which ensures that only the bank, and the organizations it 'whitelists', can send email as the bank.

.BANK's verification and authentication process, which restricts the domain to banks (and their associations), combined with its Security Requirements, enables website visitors and email recipients to easily authenticate their interactions with their bank(s) by simply 'looking for the ".bank"'. Importantly, the simplicity of using .BANK to authenticate all website and email interactions with banks is easy enough to become a permanent, repeatable part of everyone's cybersecurity hygiene. This makes .BANK an easy, big win for banks in preventing the singular 'bad clicks' that lead to the most common, most expensive cyberattacks.

Registering a .BANK Domain

To register a .BANK domain you must first complete fTLD's verification process which begins with a Verification Application. Upon completing verification, approved registrants are sent a digital registration token to use with an Approved Registrar to purchase their domain(s).

Benefiting from .BANK Cybersecurity

We can meet with your technical and marketing teams to address any questions they have and to go over best practices for an easy, affordable move to .BANK that is seamless for your customers.

Schedule a .BANK Migration Consultation

Additional Resources

- Interactive Map of .BANK'ers
- Bankers on .BANK
- Podcasts | Webinars | Blogs & Press
- New Direct-to-Customers Campaign
- .BANK Security Requirements