Unlock Secure Banking: 6 Best Practices to Protect Customers from Banking Scams

Digital banking has revolutionized how customers select and interact with financial institutions, but it also increases the risk of cyberattacks, data breaches, and fraud.

$6.08 million

The average cost of a data breach in the financial services sector in 2024[1]

80%

of banking customers would consider switching financial institutions if their data was compromised[2]

only 31%

of financial services organizations feel confident in their ability to mitigate emerging cyber risks[3]

Secure customer accounts and drive trust with modern FIDO security

The stakes are higher than ever with regulators such as the Payment Systems Regulator (PSR) in the United Kingdom and others mandating banks to reimburse fraud victims under new rules. This is why an increasing number of financial institutions are moving customers away from legacy account security such as relying on passwords alone or insecure multi-factor authentication (MFA) such as SMS and OTP, and offering customers modern phishing-resistant account security using FIDO hardware security keys.

If you are considering a new account security strategy for your end customers across commercial and retail banking, it is important to choose the right form of authentication to prevent successful phishing attacks and account takeovers. FIDO2 technology offers phishing-resistant credentials that work across common devices. Unlike OTP or SMS messages—both of which are vulnerable to being hacked—FIDO2 hardware-backed passkeys such as YubiKeys are phishing resistant, delivering robust security and ease of use.

[1] ABA Banking Journal, Average Data Breach Cost for Financial Sector Tops $6M 2024

[2] HYPR, Customer Identity Security in Finance Report 2024

[3] McKinsey & Company, The Cyber Clock Is Ticking: Derisking Emerging Technologies in Financial Services 2024

Choose the most secure authentication and maximize adoption by following these six best practices:

Put your customers first but be prepared for resistance

Strong security is vital but so is a seamless customer experience (CX). Frictionless MFA increases adoption and decreases customer frustration and churn. Make a decision of whether to make this mandatory or optional. Making this mandatory may seem harsh from a customer standpoint, but in reality most end customers are not tech savvy and may not understand the full benefit of modern FIDO authentication. In case your organization decides to make it optional, ensure that you create clear customer legal opt-outs. You can also add mitigating controls and additional fraud monitoring for these clients.

Use a multi-channel approach to educate customers

Effective communication is crucial to a successful rollout. Educate your customers through an omnichannel approach using email, videos, and webinars and other client outreach channels—explain what you're doing and how it will better protect them. Answer common concerns upfront and offer step-by-step instructions to make adoption as simple as possible.

Prepare your contact center and client interfaces

The more enablement and collateral you provide upfront to your contact centers and client interfaces, the less strain they'll face during go live. But even with stellar education efforts, some customers will need extra support and technical documentation and education is invaluable for contact centers. Equip your representatives with FAQs and troubleshooting guides, and consider adding extra staff during deployment. Understand and document all support issues for future rollouts. A train the trainer model may be beneficial across regional locations.

Testing is key to a successful rollout

Testing is key for any new customer-facing implementation and especially for this because you are changing the way that users are authenticating. Start small by testing internally, then proceed to small user populations such as friends and family before considering moving ahead with large-scale rollout across production environments.

Save your highest-risk customers for last

Roll out in waves, starting small, getting learnings and then expanding to your most valuable clients once all kinks have been removed from the roll out process. This may seem counterintuitive, but deploying to your customers comes with more blind spots than a traditional employee deployment where you have full visibility into devices and networks. Your highest-risk customers are also your highest net worth customers, so refine your deployment with other customer segments first to ensure a smoother experience for these critical accounts.

Choose a partner, not a product

Successfully deploying and managing MFA involves more than technology—it also requires strategy, logistics and ongoing support. An experienced partner ensures you're covered from launch to long-term optimization.

yubico

WHITE PAPER

Secure *customer access* to retail and commercial banking with phishing-resistant authentication

Stop account takeovers, mitigate risk and deliver frictionless customer experiences

Explore the different types of technology that protect against modern cyber threats and discover which one is best for your organization by downloading our whitepaper **Secure customer access to retail and commercial banking with phishing-resistant authentication.**

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com