Unlock secure access: 6 best practices to protect your customers online

From digital banking and health portals to online retail and loyalty accounts, the digital customer landscape has exploded. But poor password habits put both your customer and your business at risk, with many customers reusing passwords across different sites. Even multi-factor authentication (MFA) using mobile based authenticators such as SMS, OTP and push notification apps are easily breached and don't offer the best user experience. Ensuring customer security isn't just about securing customer information databases. It also necessitates offering the highest security to your customers to access their digital accounts safely and stop attackers from gaining access to their personal and financial information.

Secure customer accounts and drive trust with modern FIDO security

If you are considering a new account security strategy for your end customers, 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 one-time passwords or SMS messages—both of which are vulnerable to being hacked—FIDO2 hardware passkeys such as YubiKeys are phishing resistant, delivering robust security and ease of use.

yubico

Choose the right method and maximize adoption by following these best practices:

1. 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. Additionally you can add mitigating controls and additional fraud monitoring for these clients.

2. Use a multi-channel approach to educate customer

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.

3. 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.

4. 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.

5. 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.

6. 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.

Read our white paper, 'What is FIDO and why is it important for business security', to learn the fundamentals of modern FIDO authentication that you can incorporate into your customer facing digital services.

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for secure, simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone's reach. Learn more at www.yubico.com.

© 2025 Yubico

Contact us
yubi.co/contact