yubico

How to best secure your call center environments against modern cyber threats

Call centers are a rich source of sensitive personal information—particularly financial information such as credit card details and social security numbers—that hold great financial value and are often bought and sold on the dark web by cyber criminals. Because of this, call centers are constantly exposed to both internal and external data security threats. In addition to ensuring high security, the impetus to get call center employees productive quickly is of utmost importance due to high employee churn, seasonal peaks, and other challenging business dynamics.

Call center environments can greatly benefit from a secure, yet simple approach to verify the identity of their agents before providing access to critical systems so they can quickly provide excellent customer service, and achieve key call center success metrics such as minimal customer time in call queue, first contact resolution, and average handle time.

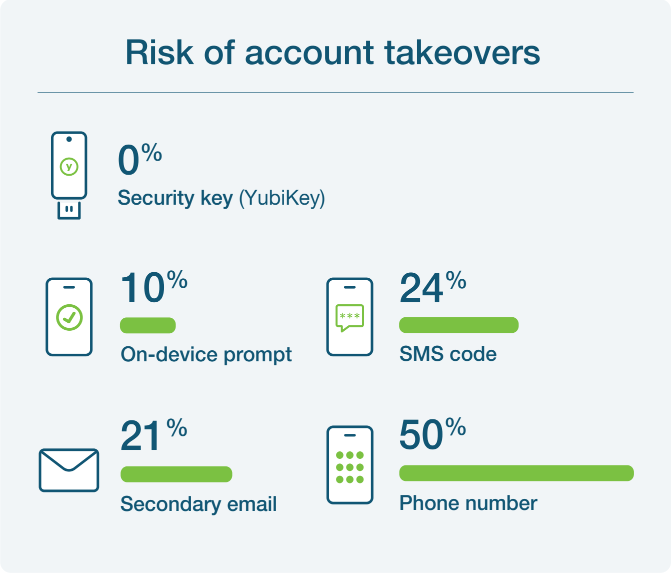
Key considerations in choosing the ideal authentication solution

Any authentication solution that serves a call center environment must balance the two poles of security and usability. Where this balance rests will depend on user access needs and particular industry requirements and standards. But a good rule of thumb is to ask how much "hassle-factor" your users can withstand before they begin not complying with procedures or start looking for shortcuts. Use the following as a checklist to see if the authentication solution you're considering can meet the critical requirements of your call center environment.

- **Deliver strong security**
  It is important to enable safety nets against increased sophisticated attacks that are growing increasingly bold and capitalizing on human errors. A solution should stay ahead of malicious innovation, employing anti-phishing policies or authentication to provide a backstop against any ransomware or malware attacks. The solution must also ensure high trust for the authentication mechanism itself. High trust comes from ensuring that the vendor has a secure supply chain and manufacturing process. If your vendor's security team can demonstrate strong security across their supply chain and follows proper code-signing protocols, you can rest a bit easier.
- **Be adaptable for shared workstations**
  Shared workstations are common across call center environments and those stations may have special login and logout requirements. In the past companies have relied on physical security procedures in these environments, but for more robust security, physical protocols should be supplemented with phishing-resistant authentication on workstations as well before granting users access to sensitive and confidential applications and data.
- **Deliver an easy user experience**
  Users often get overlooked in a search for a solution. Make sure you create an internal rollout plan to train and prepare users for the change well ahead of time. Making this a usable system has to be just as important as making it a secure system, as one can't be realized without the other.
- **Work in cellular-free zones**
  The use of cellular devices in a call center environment creates a security risk allowing users to take photos of customer data, but can also lower employee productivity if employees use their phones to make phone calls, send texts, or check their social media accounts while they're on the clock. In order to maximize productivity, the use of mobile devices should only be allowed off the call center floor.
- **Meet evolving compliance regulations**
  Future compliance requirements are always something leaders should keep a close watch on. Looking into the future, increasing compliance regulations will dictate that organizations move towards phishing-resistant MFA approaches, in all environments. There will be a move away from OTP-based approaches which are vulnerable to phishing, in favor of PIV (smart cards) and FIDO2/WebAuthn-based MFA approaches which are highly phishing-resistant.

Why YubiKeys are an ideal solution for call center environments

The YubiKey from Yubico provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale. The hardware authenticator protects the private secrets on a secure element that cannot be easily exfiltrated, preventing remote attacks. YubiKeys are the only solution proven to stop 100% of account takeovers in independent research[1].


Risk of account takeovers

YubiKeys do not require client software to be installed and they require no batteries. So someone working in a call center environment can just plug it into a USB port and touch the button, or in case USB ports are blocked for security reasons, can just tap-n-go using NFC for secure authentication.

By supporting multiple authentication protocols on a single YubiKey, such as OTP, OpenPGP, and strong authentication protocols such as smart card, FIDO U2F and FIDO2/WebAuthn, the YubiKey offers organizations the flexibility to deploy strong authentication using a single key across a variety of legacy and modern infrastructures, to support organizations no matter where they are on their passwordless journey.

For regulated environments, YubiKeys are also available in FIPS-validated form factors that meet the highest authenticator assurance level 3 (AAL3) requirements from NIST SP 800-63B.

Easily procure and distribute YubiKey authentication at scale

Yubico helps organizations easily procure and distribute YubiKeys to employees wherever they work, anywhere in the world—at the office or even at home.

With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys. This enables organizations to rapidly procure the latest YubiKeys in a way that meets their technology and budget requirements. This service also makes it easy to choose form factors, access customer support, and more.

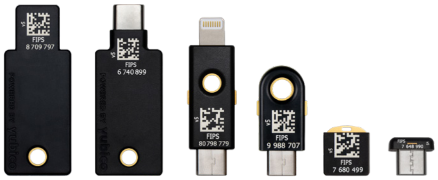
With YubiEnterprise Delivery, organizations receive turnkey service with shipping, tracking, and returns of Yubico products—all securely handled by logistics experts. It also helps with inventory management with delivery of keys as needed by the business.

Choose the trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO Alliance. Yubico is also the first company to produce the U2F security key and a multi-protocol FIDO2 authenticator.

YubiKeys are produced in the USA and Sweden, which ensures a high level of security and quality control over the entire manufacturing process.

The YubiKey 5 Series



The YubiKey 5 FIPS Series

WATER RESISTANT

CRUSH RESISTANT

MADE IN US & SWEDEN

[1] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088