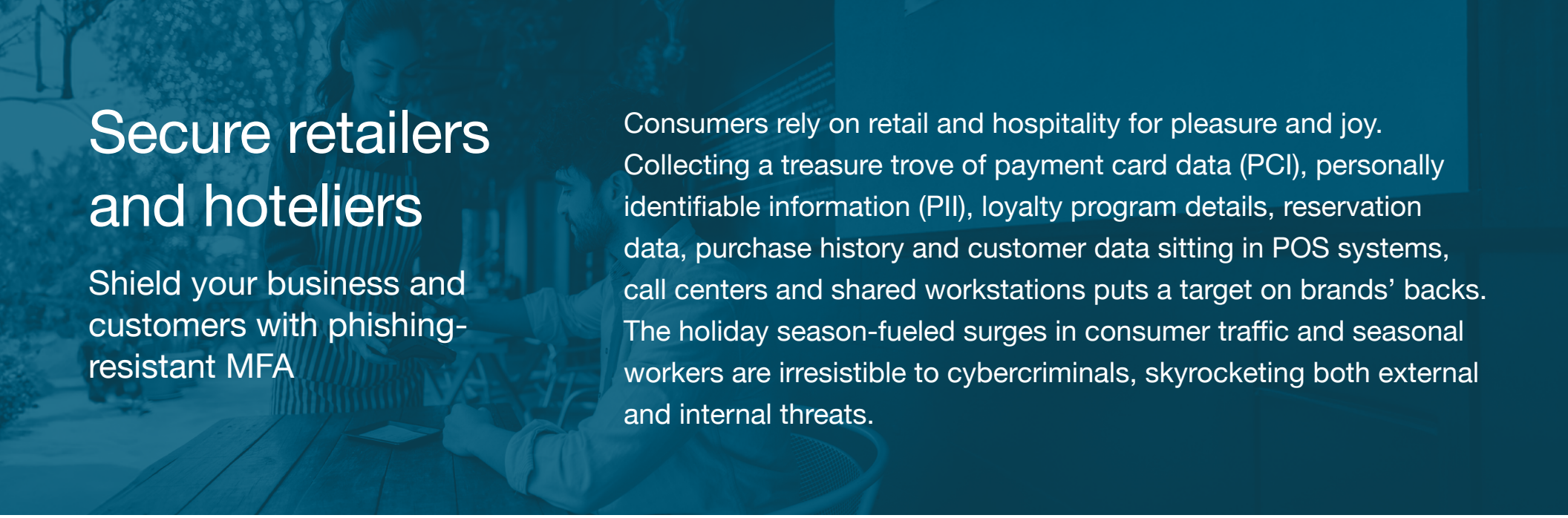

Secure retailers and hoteliers

Shield your business and customers with phishing-resistant MFA

Consumers rely on retail and hospitality for pleasure and joy. Collecting a treasure trove of payment card data (PCI), personally identifiable information (PII), loyalty program details, reservation data, purchase history and customer data sitting in POS systems, call centers and shared workstations puts a target on brands' backs. The holiday season-fueled surges in consumer traffic and seasonal workers are irresistible to cybercriminals, skyrocketing both external and internal threats.

It's the perfect storm for **phishing, ransomware and credential harvesting attacks**

$3.48 million — The average cost of a retail data breach

24% — Cyber attacks that target the retail industry

90% — Hospitality IT professionals that cite phishing as a top concern

$3.82 million — The average cost of a hospitality data breach

68% — Breaches caused by stolen credentials

176% — Increase in cyber attacks against casinos and gaming platforms from 2021 to 2022

Sources
IBM, Fortinet, Verizon, Hospitality Technology, BlackFog

yubico

Embrace a **customer-centric** MFA security solution

Multi-factor authentication (MFA) should be a first-line defense of any cybersecurity strategy. This is why, increasing cyber threats, tighter regulatory and cyber insurance requirements place tremendous pressure on these industries to strengthen authentication. **It's not a choice between security and usability, though.** From the front to the back of the house, you can prevent attacks before they happen—**all while maintaining a frictionless customer experience.**

Any MFA is better than a password, but not all MFA is created equal.

Mobile-based MFA (SMS, one-time passcodes, push notification):

- Susceptible to account takeovers and creates MFA fatigue by forcing users to re-authenticate at random intervals
- Are also unusable in mobile-restricted environments and are dependent on network and battery
- Cases where employees can't, don't, or won't use mobile authentication

Hardware-based phishing-resistant MFA, using the YubiKey:

- Reduce risk of credential theft by 99.9% and stop account takeovers while delivering 203% ROI[1]
- With multi-protocol support,[2] secure access for anyone, and from any device, to legacy and modern applications at scale
- Bridge to modern FIDO2 passwordless authentication
- Deploy the most secure passkey strategy: device-bound that is purpose-built for security, and Authenticator Assurance Level 3 (AAL3) compliant
- Drive regulatory compliance to PCI DSS v4.0.1
- Cultivate phishing-resistant users where the authentication moves seamlessly with the user across devices, platforms and systems

> "The biggest benefit that Hyatt is going to receive from deploying YubiKeys is to be able to get rid of passwords in our environment. You can't compromise what you don't have. I think we're going to have a great big party once we turn that button off and there's no more passwords anywhere in the environment."

Read the case study yubi.co/Hyatt

Art Chernobrov | Hyatt Hotels Corporation
Director of Identity, Access, and Endpoints

Contact us
yubi.co/contact

Learn more in our white paper:
yubi.co/wp-retail-hospitality

[1] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)
[2] Supports a broad range of authentication protocols: FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart card/PIV

Yubico (Nasdaq First North Growth Market 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

yubico