yubico

5 ways financial services

organizations can get started with highest-assurance multi-factor authentication

More than 60% of all leaked records in 2019 were exposed by financial services organizations.

The financial services industry is one of the highest value targets for cyber criminals due to its massive store of financial and personally identifiable information (PII), and the potential for quick payoffs through fraudulent money transfers. The 2019 Financial Breach Report: The Financial Matrix found that while financial services organizations accounted for just 6% of breaches in 2019, more than 60% of all leaked records in 2019 were exposed by this industry[1].

Financial services organizations should no longer rely simply on username and passwords for authentication to systems and applications as these can be easily breached. While two-factor authentication (2FA) in the form of security questions, SMS codes, and OTP are becoming more prevalent, these 2FA methods offer little to no protection against account takeovers, phishing, malware, and man-in-the-middle attacks. Requiring mobile-based authentication can also make companies liable for employee mobile costs.

Commercial and retail banks, insurance firms, brokerage and trading firms, investment banks and other financial services organizations need to implement security best practices such as phishing-resistant MFA that does not rely on employee mobile devices, to keep employee and customer accounts safe and secure.

The following are five ways financial services organizations can get started with highest-assurance MFA:

---

1 Protect privileged accounts from phishing attacks and account takeovers

Privileged users are prime targets for cybercriminals as they have greater access to sensitive company and customer information.

The security landscape continues to evolve and new threat vectors emerge everyday. The vast majority of big security breaches involve the misuse or escalation of privileged credentials and gaining ready access to valuable information such as intellectual property, business plans, and financial data—resulting in crippling consequences for the business.

A privileged user is any employee that has higher authorization levels to access sensitive customer, company and financial information. Financial services organizations should strengthen privileged access management, and ensure authentication security best practices are followed by all privileged users including network and database administrators, security and systems administrators, application developers, C-suite employees, and employees in finance, accounting and human resources.

Requiring privileged users to authenticate with phishing-resistant hardware security keys to securely access services and applications will help stop targeted attacks and prevent account takeovers.

2 Secure remote workers against cybersecurity threats

It is imperative for organizations to set processes and systems in place that secure remote workers without hindering productivity.

Hackers are taking advantage of the rise in remote work with targeted phishing attacks. Advancements in technology make it possible for employees to work from anywhere, but also introduce a new set of challenges for IT. Unsecured WiFi networks, unmanaged personal mobile devices, and phishing scams make it easy for cybercriminals to steal user credentials and difficult for IT teams to securely manage geographically dispersed teams.

Financial services organizations need to develop business contingency plans that include protecting their remote workforces, so employees can securely access systems without introducing new risks and vulnerabilities. Enabling MFA should be one of the top requirements for a work from home policy. For highest-assurance MFA, hardware security keys should be used with identity access management systems and identity providers to log into computers, secure VPN access, step up authentication for password managers, and even to securely generate one-time time-based passcodes.

3 Step-up authentication security for high-risk, high-value transactions

Account takeovers and data breaches net cybercriminals high profits

Employees that perform high-risk, high-value transactions on a daily basis are often the target of cybercriminals. MFA-resistant phishing, spear phishing, and business email compromise (BEC) use social engineering lures to trick employees to give up their account credentials, install malware or ransomware on their device, or pay a falsified but realistic invoice to the criminal's bank account.

Passwords are too easily guessed, brute-forced, breached, compromised, or even copied from a post-it note attached to the user's laptop/desktop. Access to high-risk systems needs to be strengthened by requiring strong and modern MFA using hardware security keys, to ensure only authorized account access and authorized high-value transactions.

4 Roll out highest-assurance security to branch workers using shared access terminals

Shared access terminals/workstations open up attack vectors to admin accounts through keystroke logging and pass-the-hash.

Employees who work on shared workstations are common in banks and call centers. Tellers move from one station to another and supervisors move to authorize transactions. Users in these environments are often part-time employees that are associated with high turnover and a minimal commitment to the organization, increasing the insider threat.

Financial services organizations need to double down on security across shared access terminals and shared workstations, to prevent unauthorized access to high-value systems and resources. Authentication via usernames and passwords does not offer high security—passwords can be breached using keystroke logging. A hardware security key offers highest-assurance MFA security for shared terminals/workstations and offers a frictionless and easy user experience.

5 Protect personal and financial information across call centers

Call center agents need fast, secure, and regulation-compliant access to important customer, account, and financial data

In 2019, Aite Group interviewed 25 executives at 18 of the top 40 largest U.S. financial institutions, and found that 61% of fraud can be traced back to the contact center2. With high employee churn, seasonal peaks, and other challenging business dynamics, call center environments need a secure, yet simple approach to verify agent identities before providing access to critical systems and data.

Financial services call centers can deploy hardware security keys to deliver stronger security that can securely verify the identity of call center agents before they are given access to PII and other sensitive data, or make any changes to a customer account, such as raising a credit limit. As mobile phones can capture images of customer and financial data such as account numbers, card expiration dates, and numerous other details that might violate customer privacy, a hardware security key offers a much more secure authentication solution.

Prevent fraud, account takeovers, and achieve highest-assurance authentication security with the YubiKey

Hardware security keys such as the YubiKey, offer a modern, highly secure, easy to use, and cost-effective approach to MFA security. The YubiKey is a multi-protocol hardware security key that offers highest-assurance authentication security over and above usernames and passwords by stopping account takeovers, phishing attacks and man-in-the-middle attacks. By providing only authorized highest-assurance MFA to sensitive and PII data with the YubiKey, financial services organizations can stay compliant with existing and emerging regulations including SOX, PSD2, PCI, FIPS, and GDPR. Unlike SMS codes and mobile push authentication, YubiKeys do not require a cellular connection, batteries, or any other external dependency to operate-instead, employees can simply plug the YubiKey into a USB port on a computer or other system and touch to authenticate.

Learn more here.

1. 2019 Financial Breach Report: The Financial Matrix
2. www.pindrop.com/blog/61-of-fraudtraced-back-to-the-contact-center/

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

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088