CM.com

US

From Passwords to Biometrics.

The Role of Two-Factor Authentication in Retail Data Protection

Contents

Introduction

In today's digital landscape, the retail industry is confronted with a rising tide of cyber threats that pose significant challenges to the security of sensitive data and the protection of customer information. To effectively address these challenges, midsize retail, and e-commerce companies must implement robust security measures. This whitepaper serves as a comprehensive guide on the importance of two-factor authentication (2FA) and its pivotal role in ensuring the security of businesses and customers.

The Retail Industry as a Prime Target for Cyberattacks

The retail industry has emerged as a prime target for cyberattacks due to the vast amounts of customer data it handles and the inherent value it holds. A study conducted by Security Magazine highlights that the retail industry bears the brunt of cyberattacks, underscoring the imperative for businesses in this sector to adopt stringent security measures.[1] Retail industry cyberattacks can be severe, leading to financial losses, tarnished reputation, and erosion of customer trust.

Understanding Two-Factor Authentication

Two-factor authentication (2FA) is a security method that provides an additional layer of protection beyond traditional username and password authentication.[2] It requires users to provide two different types of credentials to verify their identity. This method typically involves something the user knows, such as a password or PIN, and something the user possesses, such as a mobile device or security token. Additionally, 2FA can leverage biometrics like fingerprints or facial recognition as inherent characteristics of the user.

Enhancing Security and Safeguarding Customer Data

By implementing 2FA, retail businesses can significantly enhance their security posture. It is a robust deterrent against cyber threats, as passwords alone are insufficient to ensure adequate security. The combination of two authentication factors makes it substantially more challenging for unauthorized individuals to gain access to sensitive information.

Moreover, 2FA plays a critical role in safeguarding customer data. Retail companies handle vast amounts of personal and financial information, and a security breach can have dire consequences. Implementing 2FA adds an extra layer of protection, reassuring customers that their data is handled with the utmost care.

In the following sections of this whitepaper, we will delve into a detailed analysis of two-factor authentication, exploring its various types and how it can be applied in retail businesses. We will also underscore the need for implementing 2FA in retail by examining the cybersecurity threats retail companies face and the costs associated with not implementing 2FA. Furthermore, we will provide case studies demonstrating the benefits of 2FA in retail and the consequences of failures due to the lack of 2FA. Finally, we will outline best practices for implementing 2FA in midsize retail businesses, including selecting the appropriate type of 2FA, training employees, and educating customers.

Explanation of Two-Factor Authentication

Two-factor authentication (2FA) offers an added layer of protection beyond traditional username and password authentication. It requires users to provide two different types of credentials to verify their identity. These two factors typically involve something the user knows, such as a password or PIN, and something the user possesses, such as a mobile device or security token. Additionally, 2FA can leverage biometrics, such as fingerprints or facial recognition, which are inherent to the user.[3]

How it Works

When users seek access to a system or application, 2FA prompts them for a second form of identification. The various methods for this process include:

Something you know

This commonly used form of authentication involves passwords, PINs, or responses to security queries. While familiar to many, it also poses potential risks, as cyber threats can compromise passwords, or customers may utilize a single password for multiple accounts.

Authentication app

To bolster security, users can input a unique code generated by an authentication app on their mobile device. Notably, these time-based one-time passwords (TOTPs) change regularly, providing an additional layer of security. Recognized apps in this domain include Google Authenticator, Microsoft Authenticator, Authy, LastPass Authenticator, and Duo Security. Duo Security is a favored choice for many organizations, with options like one-time passcodes, push notifications, and phone call-backs for secondary authentication.

Something you have

This authentication factor involves a physical device such as a mobile phone, smart card, or security token. Users input a code received on their device after entering their password. Usually, this code is a one-time passcode (OTP) generated by an app or sent via SMS. This method enhances security as an unauthorized individual must possess the user's device to gain access, even if the user's password is compromised.

Physical security token

Certain 2FA implementations utilize physical tokens, small devices that generate one-time passwords or codes. Users integrate the token into a device or input a code during the authentication process. Devices like YubiKey, RSA SecurID Token, or Google's Titan Security Key serve this purpose. These hardware devices create a code for authentication, bringing a tangible element to the verification process.

Something you are

This third authentication type utilizes biometric factors, unique physical or behavioral traits of the user, such as fingerprints, facial recognition, voice patterns, or retinal scans. Biometric authentication provides superior security but requires specialized hardware and software and may raise privacy issues.

Biometric scan

Biometric authentication methods use physical or behavioral characteristics unique to each user, such as fingerprints or facial recognition. The user's biometric data is scanned and compared to stored data for identity verification. Notable features include Apple's Face ID and Touch ID, Windows Hello, and various features on Android smartphones. Even if a password is breached, an unauthorized user must bypass the biometric scan to gain access, ensuring robust security.[4]

In today's highly interconnected digital environment, mid-sized retail businesses confront a critical challenge: protecting customer data while providing a seamless shopping experience. One standout solution is Two-Factor Authentication (2FA) using One-Time Passwords (OTPs) delivered via messaging. This innovative approach revolutionizes transaction security and enhances consumer trust in your brand.

Understanding 2FA and OTPs

2FA enhances the security of user accounts by necessitating two components: a password (something the user knows) and a unique verification code, also referred to as a One-Time Password (OTP) (something the user receives). The OTP, a distinctive, time-bound code, is dispatched to the user through their preferred messaging platform. This two-tier security protocol ensures that only authorized individuals are granted access.

OTP Messaging Channels: SMS, Email, and Mobile Apps

OTP messages can be disseminated through multiple channels, each with merits, allowing diverse options to accommodate customer preferences.

SMS

SMS messaging is the prevalent method for OTP delivery. Upon initiating the 2FA process, an OTP is generated and transmitted to the user's registered mobile number. Though reliant on a cellular network, its ubiquity and prompt delivery render it a dependable option.

Email

Email serves as another conduit for OTP dispatch. This alternative is useful for users who opt to retain the privacy of their mobile numbers when the mobile network is accessible.

Mobile Apps

Certain businesses employ dedicated mobile apps (like Google Authenticator or Microsoft Authenticator) for OTP delivery.

Once associated with the user's account, these apps generate OTPs that refresh every 30 seconds. This method is independent of cellular networks or email access, proving to be a boon in specific situations.

In the contemporary digital marketplace, safeguarding your customer's data while ensuring a seamless shopping experience is vital for any mid-sized retail business. Two-Factor Authentication (2FA) steps in here, employing One-Time Passwords (OTPs) and Time-Based One-Time Passwords (TOTPs), dispatched through various messaging channels. This approach is not solely about securing transactions—it's about establishing a formidable foundation of trust with your customers.

The 2FA Process in Action

Imagine a customer trying to log into their account on your retail platform. After inputting their password, they receive a prompt for an OTP or TOTP, which your system dispatches to their chosen messaging channel.

The user retrieves and enters the OTP/TOTP on your website. Your system confirms the password within a stipulated timeframe, and access is granted to the user only upon successful verification. This procedure fortifies your platform against data breaches by demanding the user's password and physical access to the chosen OTP/TOTP delivery method.

What it means for Mid-Sized Retail Businesses

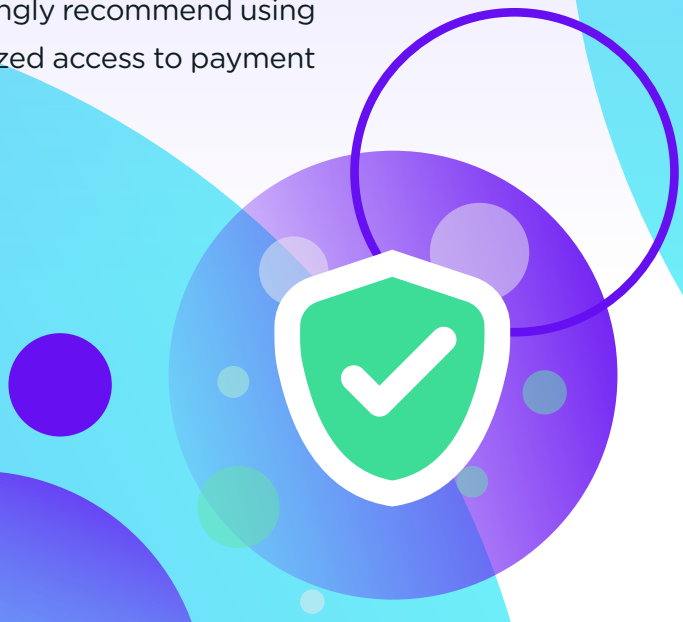
Adopting 2FA with OTPs and TOTPs places you at the forefront of data security. It safeguards your customers' confidential information while affirming their security is a priority. Additionally, it delivers a seamless shopping experience that harmonizes security with convenience.

Implementing 2FA distinguishes you from competitors yet to adopt this sophisticated security level, reinforcing your commitment to data protection and showcasing your tech-forward stance.

By introducing 2FA in retail, an extra layer of security is incorporated into the authentication process, minimizing the risk of unauthorized access and shielding against various cybersecurity threats. With passwords increasingly susceptible to hacking and phishing attacks, 2FA becomes a crucial safeguard to maintain the integrity and confidentiality of sensitive data.

According to Verizon's 2022 Data Breach Investigation Report, 81% of hacking-related breaches occur due to weak or stolen passwords.[5] By introducing an additional factor, 2FA mitigates the risk of unauthorized access even if the password is compromised. It provides an extra barrier that potential attackers must bypass, significantly reducing the likelihood of successful breaches.

Furthermore, the implementation of 2FA aligns with industry best practices and compliance requirements. Regulatory frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS), strongly recommend using 2FA to protect customer data and prevent unauthorized access to payment systems.



Importance of Two-Factor Authentication for Retail Business

To properly highlight the significance of two-factor authentication for retail, it is essential to understand the cybersecurity threats retail businesses face and the critical importance of protecting customer data.

According to the 2019 Cost of Cybercrime Study conducted by Accenture, the retail industry experiences the highest number of cyberattacks, accounting for 16% of all attacks across various sectors. This alarming statistic can be attributed to the industry's large customer base, the significant value of the data handled, and the prevalence of online transactions. The study also estimates that retail companies face an average annual cost of $12.1 million due to cybercrime.[6]

Given the extensive amount of customer information, including personal and financial data, that retail businesses handle, a security breach can result in severe consequences such as financial loss, reputational damage, and the erosion of customer trust. Implementing 2FA adds an extra layer of protection, assuring customers that their personal information is handled with the utmost care.

IBM Security's Cost of Data Breach Report reveals a compelling insight into the effectiveness of 2FA. Organizations with fully deployed 2FA solutions experience lower costs associated with data breaches than those without. On average, companies with 2FA save $1.8 million in data breach costs.[7]

Additionally, a report by Cisco highlights that the retail industry was the second most targeted sector globally for ransomware attacks in 2021, marking a 75% increase from the previous year. Furthermore, a survey conducted by Cisco demonstrates the significance of 2FA in building customer trust. Notably, 80% of consumers indicated they would trust a company more if it utilized 2FA to protect their sensitive information. By implementing 2FA, retailers can foster customer trust, enhance their brand reputation, and gain a competitive edge.[8]

Considering the current state of cybersecurity threats, it becomes evident that taking a proactive approach to security is essential. Recent research from Accenture highlights the importance of prioritizing cybersecurity right from the inception of any digital transformation effort. The study identifies a group known as "cyber transformers," comprising 30% of the respondents. These cyber transformers excel in risk management, frequently utilize cybersecurity-as-a-service, demonstrate an unwavering commitment to protecting their ecosystem, and heavily rely on automation. Consequently, they are nearly six times more likely to experience successful digital transformations than their counterparts.[9]

Implementing 2FA is a crucial step toward becoming a "cyber transformer." This additional layer of security reduces the risk of unauthorized access and aligns with industry best practices and regulatory compliance requirements. For instance, regulatory frameworks like the Payment Card Industry Data Security Standard (PCI DSS) strongly advocate using 2FA to protect customer data and prevent unauthorized access to payment systems.

Detailed Analysis of Two-Factor Authentication

In today's digital economy, data holds immense value as one of the most crucial assets for businesses. Particularly for retail and e-commerce companies, data is the lifeblood that drives customer engagement, enhances user experience, and generates revenue. However, due to the sensitive nature of the information they possess, such as credit card details and personal customer data, these companies become prime targets for cybercriminals.

As the digital presence of retail and e-commerce businesses continues to expand, so does the potential surface area for cyber-attacks. According to a report from the Internet Security Threat Report, there was a significant 56% increase in breaches in 2019, with many explicitly targeting e-commerce sites. Consequently, safeguarding digital assets becomes paramount, and one of the most powerful tools available for businesses in this endeavor is two-factor authentication (2FA).[10]

Implementing two-factor authentication (2FA) for retail and e-commerce environments is crucial to retail e-commerce security measures. It requires a careful evaluation of the customer experience. Though 2FA significantly bolsters security, it might introduce friction into the user experience, potentially leading to cart abandonment or reduced user engagement. Therefore, striking a delicate balance between security and usability is imperative.

One effective solution within the framework of retail e-commerce security measures is to incorporate adaptive authentication. This approach involves adjusting the authentication requirements based on the transaction's risk level. For example, users might only need to enter a password when browsing products. However, they could be prompted for an additional authentication factor when attempting to purchase or modify account details. This strategy enables businesses to apply robust security measures where they are most needed without causing unnecessary disruptions to the customer journey.

The choice of the second authentication factor is another important consideration. SMS-based One-Time Passwords (OTPs) are commonly used due to their ease of implementation and widespread user acceptance. However, they are susceptible to SIM swapping attacks and rely on the user having network coverage. Authenticator apps, which generate OTPs on the user's device, offer a more secure alternative but require additional software installation.

Biometric authentication is an emerging trend with significant potential to enhance the security and user experience of e-commerce platforms. Advancements in biometric technology enable users to authenticate their identity with a simple fingerprint scan or facial recognition, providing a seamless and secure user experience.

Biometric Authentication Trends in 2023

As we move into 2023, the field of biometric authentication is experiencing notable trends, as reported by Biometric Update. These trends indicate a shift towards multimodal and multi-factor authentication (MFA) alongside an increased focus on privacy regulations.[11]

Another trend to watch is the rise of post-quantum cryptography (PQC). PQC will introduce higher computational complexity and larger data sizes, necessitating the development of new hardware and software optimizations.[12]

Furthermore, interoperable digital IDs based on decentralized and blockchain technologies are expected to gain mass adoption in 2023, thereby fostering the utilization of new biometric applications. As biometric technologies become more precise, their applications expand accordingly. Anticipated growth in access control technologies relying on biometrics is driven by changes in work environments and employee habits following the impact of Covid-19.[13]

With increased regulatory efforts surrounding biometric data collection and the regulation of digital IDs, privacy and legal aspects of biometrics are becoming more localized yet consistent.
The adoption of cloud technologies relying on biometrics is set to rise, enabling support for edge-computing workloads, making existing devices compatible with cloud services, and facilitating centralized access to systems and data across multiple sites.

In 2023, passwordless authentication, especially for critical accounts, is projected to grow significantly, providing users with enhanced security for their private data.

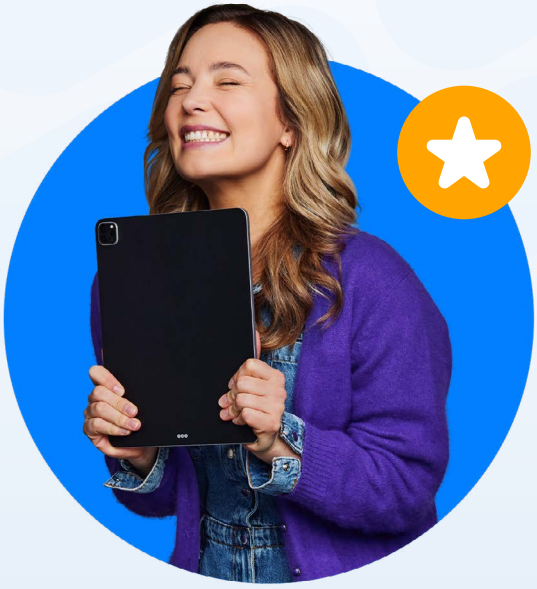
To counter the emergence of deepfakes and sophisticated fraud techniques, anti-spoofing and liveness checks are expected to gain prominence, necessitating investment in AI and machine learning anti-fraud technologies.[14]

As the security landscape for midsize retail and e-commerce businesses rapidly evolves, it is imperative for companies to respond with advanced security measures. Implementing two-factor authentication for retail is no longer optional but a necessity. By understanding the various forms of 2FA and their applications in e-commerce, businesses can make informed decisions that enhance security while ensuring a seamless user experience. Staying updated with the latest trends, such as biometric authentication and the transition towards password-less authentication, is crucial for staying ahead of potential risks and ensuring the utmost security for sensitive customer data.

How 2FA can be Applied in Retail Businesses

Two-factor authentication (2FA) is a valuable security enhancement that retail businesses can implement to provide an additional layer of protection beyond passwords. It can be applied in various ways, particularly concerning customer and employee accounts.

Customer Accounts



Integrating two-factor authentication (2FA) for customer accounts is a critical strategy for improving customer trust with 2FA. It safeguards their personal data and transaction details. When customers log into their accounts, they are prompted to provide a second form of authentication alongside their passwords. This second form could be a one-time code sent to their phone, a fingerprint scan, or facial recognition, depending on the chosen 2FA method. This means that even if a customer's password is compromised, unauthorized access becomes significantly more difficult since the attacker would need access to the second factor.

Implementing 2FA is not just about securing accounts; it's also about improving customer trust with 2FA. This implementation reassures customers that their data and transactions are protected by advanced security measures, enhancing their trust in the retailer. However, it is crucial to balance this heightened security with user convenience. The additional authentication step should be as seamless as possible to avoid creating friction in the user experience.

An excellent example of implementing 2FA in retail is demonstrated by Amazon. When customers create or sign into their Amazon accounts, they can enable Two-Step Verification.

With this feature, after entering their password, Amazon sends a one-time passcode to their phone number. The customer must enter this passcode to successfully log in, adding an extra layer of security that requires physical access to the customer's phone for account access.

Another instance is the utilization of biometrics in mobile banking applications. Banks like Wells Fargo and Bank of America allow customers to access their accounts on smartphones using their fingerprints or Face ID. This seamless integration of biometric authentication ensures a user-friendly experience while bolstering security.

Employee Accounts

2FA is equally vital for employee accounts, mainly as retail businesses handle vast amounts of sensitive data, including customer information, supplier details, and financial records. Employees, especially those with administrative access, can pose potential vulnerabilities.

Implementing 2FA for employee accounts adds an additional layer of security. Similar to customer accounts, the second factor can involve a code sent to an employee's phone, a biometric prompt, or a physical token, depending on the chosen 2FA solution. This ensures that even if an employee's primary password is compromised, unauthorized access to the system can still be prevented.

Beyond protecting sensitive data, 2FA for employee accounts aids in monitoring and auditing access to various systems, facilitating the identification of potential internal security issues.

Google is an example of 2FA for employee accounts, offering its solution called Google Authenticator. When employees log into their Google Workspace accounts, they are prompted to enter a code generated by the Google Authenticator app on their phones and their passwords. This dynamic code changes every 30 seconds, providing an added layer of security. Without the code from the Google Authenticator app, unauthorized users cannot gain access, even if an employee's password is compromised.

Another example is the use of physical security tokens for 2FA in companies dealing with highly sensitive information. These tokens generate a code that employees must enter following their passwords. Companies like RSA offer security tokens as part of their comprehensive suite of security solutions.
Implementing 2FA in retail for customers and employees significantly enhances overall security. It serves as an investment that protects the company's data while building trust with customers and stakeholders.

The Cost of Not Implementing Two-Factor Authentication

Implementing two-factor Authentication (2FA) is one of the most effective methods to mitigate the risks. Despite the benefits of 2FA in the retail industry, numerous businesses have been hesitant to adopt 2FA, citing perceived inconvenience or cost as deterrents. However, it is crucial to recognize that the potential consequences of neglecting 2FA can far outweigh any initial concerns, resulting in substantial financial losses, tarnished reputation, and a loss of trust from customers.

Financial Losses

Data breaches can result in substantial financial losses, as evidenced by a study by IBM and Ponemon Institute. In 2020, the average global cost per data breach amounted to a staggering $3.86 million. U.S. companies experienced an even higher average cost of $8.64 million.[15] This data was calculated by examining data breaches that ranged in size between 3,400 and 99,370 compromised records.

Looking ahead to 2023, the projected average cost of a data breach is estimated to reach $5 million.[16] These costs encompass various aspects, including direct and indirect expenses:

Direct Costs

Direct costs encompass activities such as identifying and rectifying the security breach, as well as implementing preventive measures to mitigate future incidents.

Indirect Costs

Indirect costs comprise factors such as lost business opportunities resulting from the breach, reputation management endeavors, and efforts to retain customer trust.

The financial repercussions of data breaches can be significant, underscoring the importance of implementing robust security measures to safeguard sensitive information.

Damaged Reputation

A data breach can have profound and enduring consequences on a company's reputation. The 2020 Cost of a Data Breach report by IBM and Ponemon highlighted the tendency of customers to distance themselves from businesses that have experienced such breaches. The report revealed that companies, on average, lost 5.6% of their existing customer base following a data breach incident.[17]

For mid-sized retail and e-commerce enterprises, the impact of a damaged reputation can be even more severe. These businesses heavily rely on their online presence and reputation to attract and retain customers. Therefore, a data breach can potentially undermine the trust they have painstakingly built, resulting in lost sales and customer attrition.[18]

While 2022 saw a decrease in lost business costs related to data breaches, totaling $1.42 million, it is essential to note that compromised credentials, such as compromised business emails and third-party data breaches, exhibited an upward trajectory. Specifically, the costs associated with third-party violations as the initial attack vector rose from $4.33 million in 2021 to $4.55 million.[19]

Furthermore, the duration of an undetected breach directly correlates with its financial impact. In 2022, the average breach remained undetected for 277 days, representing a slight reduction of 10 days compared to the previous year. However, despite this marginal decrease in detection times, average data breach costs continued to rise.[20]

Loss of Customer Trust

A data breach can profoundly impact the trust customers place in a company. Findings from a 2019 study by Ping Identity revealed that as many as 78% of consumers would discontinue their online engagement with a brand following a data breach. This statistic clearly illustrates the potential loss of customer loyalty from such a violation.[21]

For mid-sized retail and e-commerce companies, which heavily rely on repeat business, the loss of customer trust can be incredibly detrimental. In addition to potentially losing existing customers, these businesses may encounter challenges in attracting new customers as their security practices are scrutinized.

The aftermath of a data breach entails a significant investment of time and resources in crisis management, security solution upgrades, security training, and stakeholder communication aimed at rebuilding trust. The way a company handles a data breach directly impacts its reputation, and the level of customer trust it can regain post-incident.[22]

A survey conducted on 1,000 Americans revealed that people are more likely to continue shopping with a retail store following a data breach compared to other types of businesses. Notably, two well-known examples, Target and Uber, experienced significant data breaches with varying outcomes.[23]

Target's breach, which occurred in 2013 and lasted approximately three weeks, garnered criticism due to the delayed public notification. Nevertheless, Target managed to revamp its reputation in the years that followed by taking swift and comprehensive measures to enhance security and regain customer trust. Their proactive approach to bolstering safety measures and technology likely had a positive impact on public opinion. Although Target experienced a 54.6% decline in consumer perception in the year following the breach, subsequent years witnessed a steady increase.[24]

In contrast, Uber's breach occurred in 2016 and was discovered a month later. The company opted to pay hackers to delete the data and remain silent about the incident. It was only in 2017 that Uber disclosed the breach, resulting in fines, mandated security protocols, and significant erosion of customer trust. The mishandling of the breach exacerbated criticism as Uber violated laws regarding breach notification.[25]

The consequences of not implementing two-factor authentication for retail can be far-reaching, encompassing financial losses, reputational damage, and a loss of customer trust. Implementing 2FA is a crucial step in safeguarding a company's data, preserving its integrity, and upholding the trust of its customers.

Case Study: The Impact of Two-Factor Authentication

Succesful Implementation

Rite Aid's Experience with 2FA

Rite Aid, a prominent US-based pharmacy employing nearly 60,000 individuals, is a compelling example of a successful two-factor authentication (2FA) implementation within the retail industry. The company encountered a notable hurdle: the need for organization-wide authentication that did not rely on company email or SMS verification while accommodating the use of shared terminals for access. This predicament arose because retail task workers were prohibited from using personal mobile phones on-site yet required access through a single terminal.

To address this challenge, Rite Aid adopted MIRACL Trust, a highly effective multi-factor authentication solution that eliminated the necessity for mobile verification and enabled multiple logins from a single desktop. This solution proved ideal for staff members who shared terminals, offering rapid two-second logins and substantially reduced error rates compared to legacy multi-factor authentication methods. Moreover, this authentication solution did not require possessing a company email or mobile phone, as it relied on a PIN-based zero-knowledge proof mechanism. Consequently, employees could securely and conveniently access e-learning resources using shared terminals, ensuring ease of use and uncompromised security measures.[26]

The Consequences of a Lack of 2FA: Security Breaches

The absence of two-factor authentication (2FA) can have severe consequences, as demonstrated by several notable incidents in recent years involving significant security breaches.

Equifax
2017

During this incident, hackers exploited default login information based on social security numbers and birth dates to gain website access. This breach exposed the risk of 145 million records being made public, including employee records. Moreover, at least 750 employee records were utilized to file false tax returns with the IRS in the United States. The implementation of multi-factor authentication could have prevented this breach.[27]

Deloitte
2017

During this breach, a hacker gained unauthorized access to the firm's global email server using an administrator's account protected only by a single password. This breach potentially provided the hacker with usernames, passwords, IP addresses, architectural diagrams for businesses, health information, and up to five million email messages. The sensitive material stolen could have been significantly more difficult to acquire if the administrator's email account had been safeguarded with multi-factor authentication.[28]

Timehop
2018

Timehop, an application that allows users to view old photographs from social media, fell victim to a breach in which the hacker exploited compromised access credentials to their cloud computing environment. The lack of multi-factor authentication protection for the account facilitated the theft of personally identifiable data. This breach could have been prevented if multi-factor authentication had been implemented.[29]

Ring
2019

Ring, the Amazon-owned home security company, reported experiencing a data leak that compromised the personal information of 3,672 customers. This leak exposed users' emails, passwords, time zones, and names associated with specific Ring cameras. Despite the seriousness of the situation, Ring maintains that its systems have not been breached, attributing the leak to "bad actors" who utilized information from other companies' data breaches.

The leaked information has the potential to grant hackers access to a user's home address, phone number, payment details, and even live video feed from active Ring cameras. Ring has taken action by notifying affected users and enforcing a password reset. Additionally, they are urging all customers to enable two-factor authentication as a means to fortify account security.

Neiman Marcus
2021

Neiman Marcus, a distinguished American luxury department store, endured a substantial data breach that exposed the personal data of over 1.1 million customers. The breached data included details such as names, email addresses, credit card numbers, and additional payment information stemming from a vulnerability in the company's payment processing system.

Responding swiftly to this major security breach, Neiman Marcus promptly addressed the system vulnerability. Furthermore, the company offered affected customers complimentary credit monitoring and identity theft protection services as a supportive measure to mitigate potential harm.

The 2021 Neiman Marcus data breach is a stark reminder of the enduring cybersecurity threats to which even prominent and well-established corporations are susceptible. It emphasizes the importance of businesses implementing robust security measures, including strong passwords, regular software updates, and continuous employee training on cybersecurity best practices.

Regrettably, this is not the first time Neiman Marcus has faced such security concerns. The company has encountered multiple cybersecurity incidents in recent years, including a similar breach in 2013 that exposed the personal information of approximately 4.9 million customers and a hacking incident in 2017. These incidents underscore the critical necessity for ongoing investments and updates in cybersecurity measures.

3.1M
Cards Affected

Uber
2022

In 2022, Uber experienced a significant data breach, not its first, resulting from a sophisticated social engineering attack led by the notorious hacking group LAPSUS$. This attack exploited human vulnerabilities, highlighting the critical need for companies to prioritize employee education and adherence to security best practices.

This breach emphasizes the importance of practicing good password hygiene and implementing robust multi-factor authentication (MFA). Regularly changing passwords and utilizing a password manager can significantly reduce the risk of compromised passwords. Additionally, opting for the most secure 2FA methods, such as Authenticator Apps over SMS-based authentication, can provide more robust protection against social engineering tactics.

This incident serves as a reminder that cybercriminals persistently target human weaknesses amidst rapid technological advancements. It underscores the necessity for ongoing vigilance, strict security practices, and continuous employee education to prevent data breaches.

These examples highlight how the lack of 2FA allegedly made these companies and their customers vulnerable to cyberattacks, resulting in substantial data breaches, financial losses, and reputational damage. In contrast, Rite Aid's successful implementation of 2FA is a testament to the potential benefits of this security measure in the retail industry.

As a result, retail companies should seriously consider adopting 2FA to safeguard their data and maintain customer trust.

The Personal Information of

57M

Users got stolen in 2016, in another breach

Two-Factor Authentication in 2023: What to Expect

The alarming surge in cybercrime, projected to escalate by 15% annually and reach a staggering $10.5 trillion by 2025, has underscored the pressing need for robust security measures across industries. Amidst this landscape, two-factor authentication (2FA) stands out as a critical countermeasure for midsize retail and e-commerce businesses.[30]

2FA fortifies account security and has proven exceptionally effective against automated attacks and data breach prevention for retail. Both Google and Microsoft have reported that accounts utilizing 2FA are over 99.9% less susceptible to compromise.[31]

2FA is a blend of simplicity, security, and innovation designed to seamlessly integrate into your retail business, bolstering your security posture while enhancing your user experience. In the words of CM.com's Head of CPAAS R&D, Remco Magielse, Ph.D.:

> ***"When examining the 2FA markets, we find that time-based OTPs and SMS OTP primarily dominates it. These methods have gained popularity as they require only a phone number from a customer, something that people are typically comfortable providing."***

Consequently, they represent a low-effort implementation strategy to boost security significantly. SMS OTPs are appealing due to their simplicity, but other OTP options, such as WhatsApp, may require a tad more effort but offer a higher degree of safety. For example, WhatsApp OTPs provide a second layer of authentication and add an extra layer of security with their encrypted messaging system.

Various methods exist for implementing 2FA, including text messages (SMS), authentication apps, security keys, and backup codes. Each method carries its own strengths and potential weaknesses. For instance, SMS, while easy to set up and use, is relatively insecure as hackers can intercept text messages.[32]

Incorporating 2FA necessitates a careful balance between security and user experience. If the process becomes excessively complex, users may bypass or circumvent it, undermining its effectiveness. In 2023, there are several popular and effective 2FA methods that businesses can consider:

SMS-Based 2FA

The system sends a one-time code to the user's registered mobile number during login. The user must enter this code to access their account. However, this method has vulnerabilities, such as SIM swapping and interception of the SMS code.

Authenticator Apps

These applications (like Google Authenticator or Microsoft Authenticator) generate a time-sensitive code that the user must enter during login. This method avoids some of the vulnerabilities of SMS-based 2FA.

Hardware Tokens

These are physical devices that generate a code that the user must enter. While this is one of the most secure methods, it can be costly and less convenient for the user.

Biometric 2FA

Biometric 2FA includes methods like fingerprint scanning, facial recognition, or voice recognition. These methods are convenient and difficult to spoof but require more sophisticated technology.

To optimally prevent data breaches in retail, selecting a two-factor authentication (2FA) method should be carefully considered. This decision should consider the specifics of your business, the level of sensitivity of the data you manage, and the tech-savviness of your users. By tailoring your 2FA method to these parameters, you can enhance security and better protect your retail operation.

Looking to the Future: Expectations and Trends

It is crucial to maintain realistic expectations regarding the efficacy of 2FA as a tool against cybercrime. While undeniably powerful, 2FA is not infallible and should be complemented by a broader understanding of online threats. Relying solely on 2FA and becoming overconfident in its protection can potentially leave a business vulnerable to attack.[33]

The user experience of 2FA has significantly evolved over time. With the widespread adoption of smartphones, the convenience issues that users previously lamented have largely been resolved. However, it is essential to note that smartphones, while convenient, also carry their own set of risks.[34]

Conclusion

In conclusion, the significance of cybersecurity threats within the retail industry cannot be overstated, emphasizing the undeniable need for robust protective measures such as two-factor authentication (2FA). Our exploration of the intricacies of 2FA, its diverse types, and its relevance to retail establishments makes it apparent that 2FA stands as a critical defense against data breaches, phishing attacks, malware, and insider threats. The presented case studies serve as compelling reminders of the profound repercussions of neglecting 2FA, including substantial financial ramifications and the erosion of customer trust.

The successful implementation of 2FA within retail businesses, particularly those of medium size, necessitates the meticulous selection of the appropriate 2FA method, coupled with dedicated efforts to educate employees and customers regarding its functionality and significance. As we venture into 2023 and beyond, the landscape of cybersecurity threats is expected to evolve, demanding a dynamic approach to 2FA and an unwavering commitment to remaining informed and adaptable.

Customer data protection in retail hinges upon these protective measures, rendering the adoption of 2FA not merely an option but imperative for retail businesses. By embracing 2FA, retail companies can fortify their security posture, enhance customer trust, and reinforce their resilience in the face of ever-evolving cybersecurity challenges.

Citation

- [10] 2019 insider threat report - Fortinet.
  https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf.
- [21] "81% of Consumers Would Stop Engaging with a Brand Online After a Data Breach, Reports Ping Identity." Ping Identity - Last modified October 22, 2019.
  https://press.pingidentity.com/2019-10-22-81-of-Consumers-Would-Stop-Engaging-with-a-Brand-Online-After-a-Data-Breach,-Reports-Ping-Identity
- [9] Accenture. 2019. "2019 Cost of Cybercrime Study." Accenture - 2019.
  https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.
- [6] Accenture - Last modified 2023
  https://www.accenture.com/us-en
- [22] [23] [24] [25] Buckbee, Michael. "Company Reputation After a Data Breach." Varonis Systems, Inc. - Last updated May 28, 2023.
  https://www.varonis.com/blog/company-reputation-after-a-data-breach.
- [8] CISCO, 2022. "Data Transparency's Essential Role in Building Customer Trust.
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf
- [1] Crowley, Greg. 2022. "The Rising Threat of Cybersecurity for Retailers." Security Magazine. - December 14, 2022.
  https://www.securitymagazine.com/articles/98715-the-rising-threat-of-cybersecurity-for-retailers
- [30] "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine - April 27, 2021.
  cybersecurityventures.com/cyberwarfare-report-intrusion/.
- [3] [27] Fruhlinger, Josh. 2019. "What is 2FA? How Two-Factor Authentication Works and Why You Should Use It." CSO Online - 2019.
  https://www.csoonline.com/article/3239144/what-is-2fa-how-two-factor-authentication-works-and-why-you-should-use-it.html
- [4] Griffith, Eric. 2023. "Multi-Factor Authentication: Who Has It and How to Set It Up." PCMag. - March 8, 2023.
  https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up
- [28] Hopkins, Nick. "Deloitte Hit by Cyber-Attack Revealing Clients' Secret Emails." The Guardian, The Guardian - November 27, 2017.
  www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.
- [31] [32] "How to Use Two-Factor Authentication (2FA) in 2023." RestorePrivacy.
  restoreprivacy.com/two-factor-authentication-2fa/. June 27, 2023.
- [15] [17] IBM, 2020. "Cost of a Data Breach Report 2020." IBM - 2020.
  https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

- [7] IBM, 2022. “Data Breach Report.” IBM. https://www.ibm.com/reports/data-breach
- [33] [34] Jones, Brad. “Two-Factor Security Is the Best Lock for Your Digital Life, but It’s Not Perfect.” Digital Trends, Digital Trends - January 20, 2017. www.digitaltrends.com/computing/why-2-factor-security-is-flawed/.
- [-] Jones, Corrin. “Warnings (& Lessons) of the 2013 Target Data Breach.” Red River | Technology Decisions Aren’t Black and White. Think Red - October 26, 2021. redriver.com/security/target-data-breach.
- [29] Lomas, Natasha. “Timehop Discloses July 4 Data Breach Affecting 21 Million.” TechCrunch - July 9, 2018. techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/.
- [11] [12] [13] [14] Mascellino, Alessandro. “Biometrics Trends for 2023: Multimodal and MFA to Grow Alongside Privacy Regulations.” Biometric Update. - Last modified December 27, 2022. https://www.biometricupdate.com/202212/biometrics-trends-for-2023-multimodal-and-mfa-to-grow-alongside-privacy-regulations
- [16] [18] [19] [20] McKenzie, Gov. Deandrea. “What is the Cost of a Data Breach in 2023? | UpGuard.” Investguiding - June 30, 2023. https://investguiding-com.ngontinh24.com/article/what-is-the-cost-of-a-data-breach-in-2023-upguard
- [26] MIRACL. “MIRACL Case Study: Rite Aid.” MIRACL - Publication Date. https://miracl.com/casestudies/MIRACL_case_study_Rite_Aid.pdf.
- [-] Nguyen, Nicole. “You Need Two-Factor Authentication, but Some Types Are Safer than Others.” Wall Street Journal - April 3, 2022. www.wsj.com/articles/you-need-two-factor-authentication-but-some-types-are-safer-than-others-11648930708.
- [2] Rankine, 2023. “What is Two-Factor Authentication and How to Set It Up.” - Textr. June 23, 2023. https://textrapp.com/team/blog/tech-solutions/how-to-set-up-two-factor-authentication
- [5] Verizon, 2022. “2022 Data Breach Investigations Report.” - Verizon, 2022. https://www.verizon.com/business/resources/Tc0e/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
- [-] Wallen, Jack. “How to Get Users on Board with Two-Factor Authentication.” TechRepublic - August 7, 2017. www.techrepublic.com/article/how-to-get-users-on-board-with-two-factor-authentication/.

CM.com (AMS: CMCOM) is a global leader in cloud software for conversational commerce that enables businesses to deliver a superior customer experience. Our communications and payments platform empowers marketing, sales and customer support to automate engagement with customers across multiple mobile channels, blended with seamless payment capabilities that drive sales, gain customers and increase customer happiness.