Token

eBook

The CISO's Guide to Stopping Ransomware and Credential-Based Attacks with Phishing-Resistant MFA

Contents

1 Executive Summary

In today's high-risk threat environment, phishing-resistant, Next-Generation MFA solutions are no longer optional but necessary for network and data security. By integrating advanced technologies, including biometrics, hardware security keys, and FIDO2 compliance, organizations can thwart phishing attempts, neutralize SIM swapping, mitigate MFA prompt bombing, and substantially reduce the risks of data breaches and ransomware attacks.[1]

Over the past five years, the cybersecurity landscape has grown increasingly hostile, with both global enterprises and smaller organizations facing a substantial rise in bypass attacks that exploit the weaknesses of legacy Multifactor Authentication (MFA).[2]

With nearly 90% of successful cyber attacks coming from phishing campaigns, legacy MFA methodologies have proven incapable of effectively mitigating the threat.[3] These attacks cost organizations dearly, with phishing incidents averaging nearly $5 million per breach and MFA prompt bombing alone leading 62% of victims to grant unauthorized access inadvertently.[4,5]

As the threat landscape evolves, techniques like SIM swapping have exposed the weakness of SMS-based authentication. The 2023 FBI Internet Crime Report indicates that more than “$48 million in losses were reported due to port jacking or SIM swapping scams over the previous calendar year.”[6]

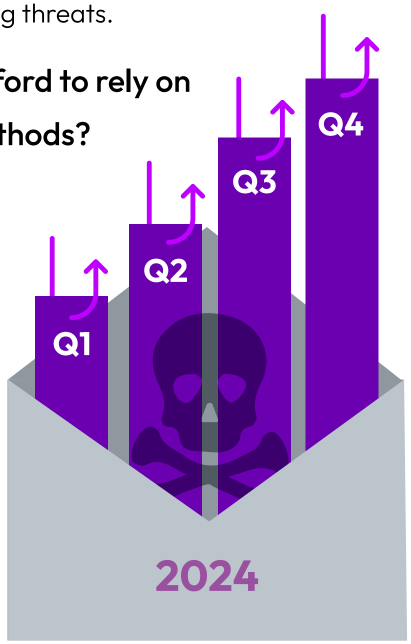
Concurrently, phishing attacks driven by MFA bypass have matured from rudimentary spam into precise, targeted campaigns, and ransomware attacks—often fueled by compromised credentials—carry average recovery costs exceeding $1.85 million.[7]

The escalation in MFA bypass attacks has impacted a broad and diverse range of targets. From financial institutions and healthcare providers to SMEs and retail, every organization with poorly secured massive data sets has historically been a target of attack.[8] While ransomware attacks have surged to prominence, with an estimated 1.5X increase in the first half of 2024, phishing continues to be the most dangerous threat vector, with an estimated 202% rise in overall phishing messages in the second half of 2024.[9, 10]

Modern methods to mitigate MFA Bypass, like dongle-based authentication have proven to block 99.9% of account attacks, while biometric methods can cut phishing success by up to 95%.[11, 12]

As cybercriminals continue to refine their methods, prioritizing Next-Generation MFA becomes a mission-critical element in safeguarding sensitive data, maintaining stakeholder trust, and ensuring operational resilience in an era of escalating threats.

Can your organization afford to rely on outdated legacy MFA methods?



202%
rise in phishing
messages in the
second half
of 2024.

2 The Prevalence of MFA Bypass Attacks

Multifactor authentication (MFA), a multi-step login process requiring users to enter additional information beyond a password, has long been a cornerstone of any effective cybersecurity strategy.[13] However, as cybercriminals and global threat actors have grown more sophisticated, MFA bypass techniques have developed in kind.

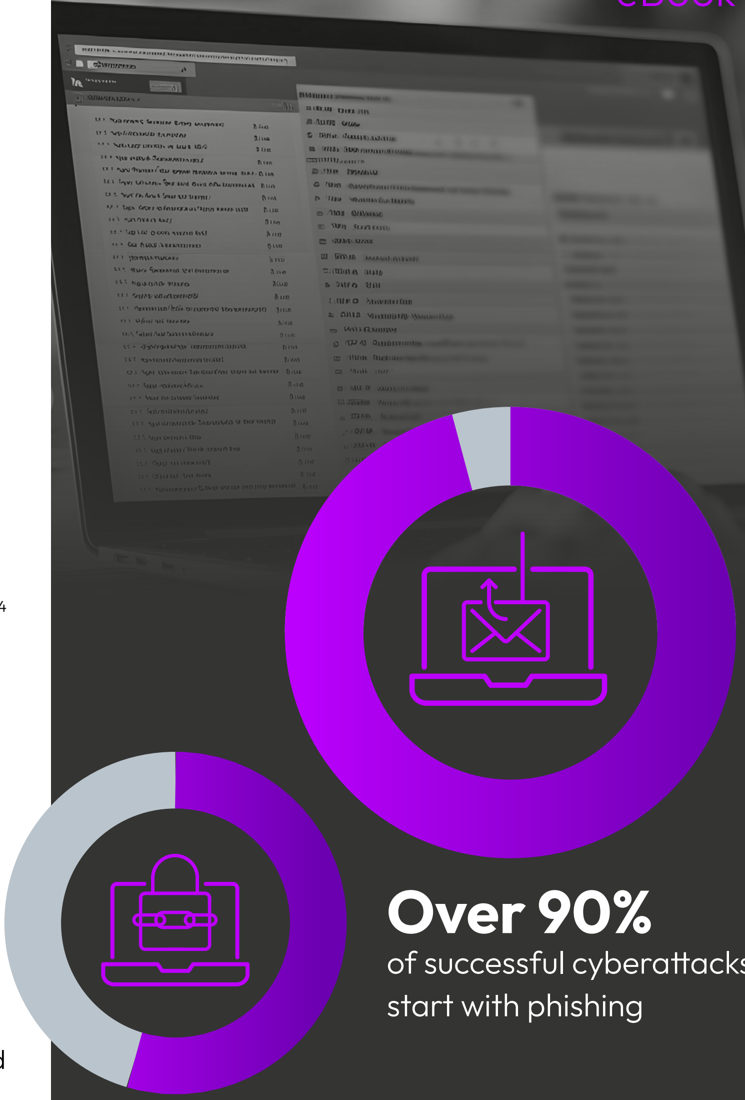
The prevalence and severity of MFA bypass attacks have dictated headlines and become a topic of conversation at shareholder meetings. According to the 2024 Verizon Data Breach Investigations Report, 83% of breaches involved external actors, with credential theft remaining a primary method.[14]

From financial institutions and healthcare providers to government agencies and Fortune 500 companies, every organization with massive data sets has historically been a target of attack.[15] **While ransomware attacks have surged to prominence, with an estimated 56% increase in the first half of 2024, phishing continues to be the most dangerous threat vector, with over 90% of successful cyber-attacks starting with phishing.**[16, 17]

Over the first half of the 2020s, phishing and social engineering attacks, such as business email compromise (BEC), became increasingly prevalent, emerging as key enablers of data breaches.[18]

The Democratization of Cybercrime

As the cyber risk landscape has intensified, MFA bypass techniques have become more democratized and accessible. The democratization has resulted in affordable malware kits and stolen credential marketplaces on the dark web. More damning, attackers are no longer limiting themselves to enterprise-level businesses or multinational organizations, rather increasingly focusing on all organizations regardless of size to provoke maximum damage and induce incident payouts, currently rising by 500% year-to-year.[19]



Over 90%
of successful cyberattacks start with phishing

56% increase
in rasomware attacks in the first half of 2024

Token

3 Key Limitations of Legacy MFA & Real-World Consequences

Legacy MFA has significant structural weaknesses that compromise data security, erode brand trust, and expose organizations to financial loss.[20] From phishing attacks to SIM swapping, these well-established vulnerabilities have made legacy MFA inadequate for modern threat landscapes.

Susceptibility to Phishing

Legacy MFA systems rely on static credentials like SMS codes such as email or mobile-based one-time passwords (OTPs). These are highly susceptible to phishing tactics, where attackers deceive users into sharing authentication codes. Phishing attacks have accounted for significant financial losses, costing organizations an average of $4.91 million per incident, as reported by IBM.[21]

Methods of Attack

With so many permutations for attack, the cyber battlefield can often feel overwhelming and confusing. To clear the haze, in the following section, we will define some of the most significant attack vectors and how they can bypass legacy MFA.

Man-in-the-Middle Attacks

A cyberattack in which a hacker steals sensitive information by eavesdropping or illegally accessing communications between two or more online targets, such as a user and a web application.[22] Man-in-the-Middle attacks provide direct access to user files enabling attackers to simply copy and paste emailed passcodes or limited-time pass keys.

Prompt Bombing Vulnerability

Prompt bombing is a technique where users are overwhelmed with repeated MFA approval requests.[23] Prompt bombing exploits human error and fatigue to facilitate data compromise.

SIM Swapping Risks

SMS-based MFA is especially vulnerable to SIM swapping, where attackers hijack phone numbers to intercept authentication codes.[24]

High Costs of Breach

The financial impact of breaches tied to legacy MFA is severe. Organizations persistently face ballooning costs from ransomware payments, lost revenue, the expenses of restoring operations, increased cyber insurance premiums, as well as the loss of customer trust.

Recent findings from IBM's 2024 Cost of a Data Breach Report revealed that the average cost of a data breach globally is $4.8 million.[25]

From ransomware payments and costly cyber insurance premiums to the loss of customer confidence and declines in stock valuations, the immediate damages and long-term recovery efforts stemming from an MFA-bypass-focused attack can destabilize business operations.[26]

4 Ineffective MFA: A Key Contributor to Failures

Traditional MFA methods, from email and SMS authentication to one-time passwords and security keys, have all proven highly susceptible to cyberattacks. Recent data indicates that "90% of ransomware attacks occur using user credentials, and the vast majority of those now include a legacy MFA hack as well."[27]

While once the foundational element of any defense-in-depth strategy, legacy MFA is increasingly proving inadequate.[28] Consequently, industry experts and cybercriminals alike have realized that the perceived benefits of legacy MFA actually present ample opportunities for data compromises and the execution of ransomware attacks.[29]

The SolarWinds attack of 2020 [30] remains one of the most significant cyber incidents, with widespread operational and financial impacts. In this devastating, multinational cyber bonanza, hackers used stolen credentials to infiltrate government agencies and major corporations, causing massive losses in 'secure data,' company valuations, and operational capacity across diverse sectors.

According to most reports, the estimated cost of the SolarWinds attack was over $40 million with an additional $20 million allocated to software redesign as of 2024.[31]

Prompt bombing continues to represent another critical failure point of legacy MFA. By inundating victims with repeated MFA prompts, attackers rely on users to mistakenly approve fraudulent access attempts out of fatigue or confusion.[32] MFA's weakness was notably exploited during the Uber breach of 2022, where attackers used the tactic to infiltrate internal systems.[33] The resulting data leak has led to over $148 million in settlements for Uber while compromising the data of over 100,000 drivers.[34]

74% of breaches cite human factor as having played a role in the cyberattack

According to Duncan Greatwood, CEO of Xage **"The Uber breach appears to be a result of an MFA fatigue attack, also referred to as an MFA bombing attack, in which hackers send multiple authentication approval requests to a secondary device like a mobile phone, in hopes that a user unintentionally provides access or grows so frustrated that they eventually approve a request."**[35]

The FBI estimates that SIM-swapping scams cost U.S. victims tens of millions of dollars annually.

SIM swapping has similarly exposed potentially critical vulnerabilities in SMS-based authentication enabling attackers to reroute authentication codes and take control of accounts. The FBI estimates that SIM-swapping scams cost U.S. victims tens of millions of dollars annually.[36]

With so many distinctive routes to bypass legacy MFA, businesses of all sizes have begun to realize the urgent need for modern authentication solutions that mitigate costly vulnerabilities while bolstering organizational defenses.

A Call for Phishing Resistant MFA Solutions

The rise of increasingly sophisticated and easily deployed cyber threats has laid bare the limitations of legacy MFA.[37] Effectively mitigating vulnerabilities such as phishing susceptibility, SIM-swapping risks, and prompt bombing tactics requires transitioning to Next-Generation MFA solutions.

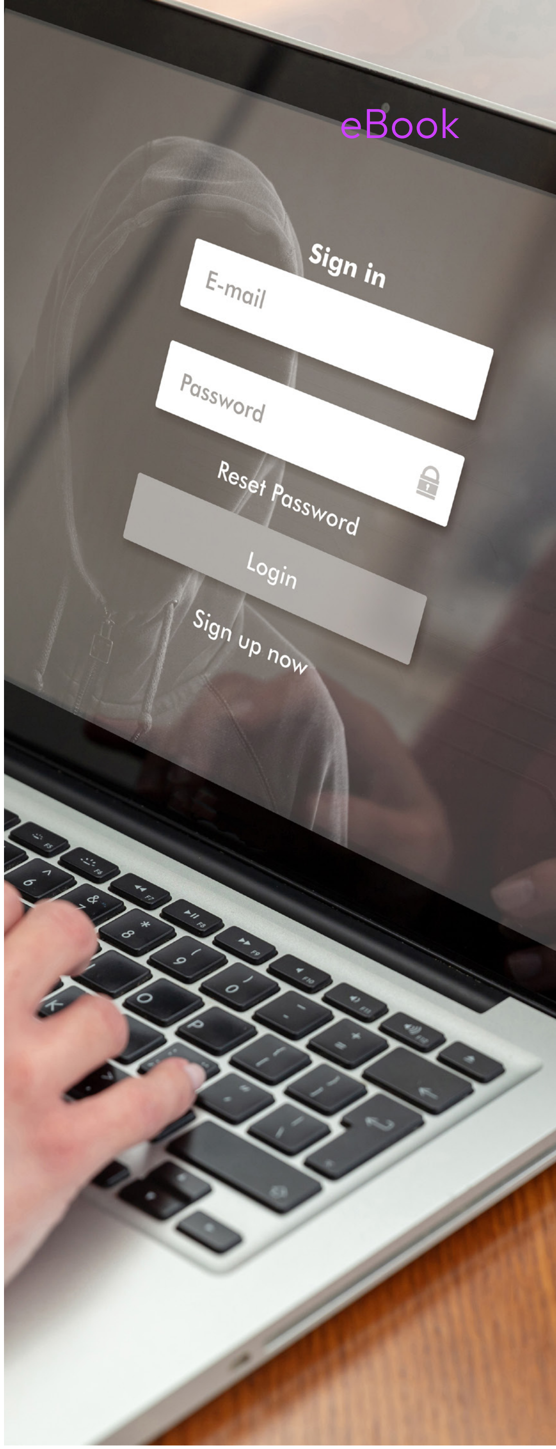
Only through the integration of advanced technologies like biometrics, hardware keys, and FIDO2 compliance can a reborn and revitalized MFA provide stronger defenses, eliminating reliance on outdated methods to reduce user friction.[38] By storing biometrics on the hardware itself (such as a wearable or security key) the device is inherently phishing-resistant. Further protecting users, the biometric data never leaves the device and isn't transmitted or stored externally on a server or in the cloud.

Due to their unique and individually linked methods, biometrics and hardware keys cannot be shared and are not at risk through the cloud. Whereas FIDO2 compliance provides passwordless authentication to facilitate greater security and privacy, user-friendly experiences, and improved scalability.[39] These advanced MFA solutions facilitate phishing-resistant solutions immune to password theft and replay attacks.

This is not a pie-in-the-sky idea, but rather an empirical reflection of the realities of an ever-expanding and complex cyber threat environment. Industry data reflects that phishing-resistant and Next-Generation MFA are effective and market-ready solutions to decrease the structural limitations of legacy MFA.

The implementation of dongle-based authentication solutions are shown to mitigate 99.9% of attacks on accounts protected by MFA. Concurrently with biometric MFA systems, such as Token Ring Biometric Authentication, Next-Generation MFA tools, can stop phishing attacks without the use of passwords or OTPs.[40, 41]

As cybercriminals continue to evolve their methods, organizations must embrace Next-Generation MFA as a critical component of their security strategy.



5 Democratization of Cyber Attacks

The democratization of cybercrime, largely driven by Ransomware-as-a-Service and the prevalence of stolen credentials on various dark web marketplaces, has expanded the threat landscape.[42] The broadening of cyber targets has impacted a broad range of industries and, most critically, lowered the barriers for entry by enabling cybercriminals without programming skills to execute devastating cyberattacks.

Advanced tools and services, once available only to the most skilled hackers, are now accessible to anyone willing to pay. This shift has reshaped how cyberattacks are planned, purchased, and executed.

Sectors Most Affected

From retail and financial services to healthcare, technology, and even SMEs, everyone is at risk and the stakes are growing by the minute.

- ### Healthcare

  Plagued by limited IT budgets and enormous quantities of Personal Protected Information (PPI) stored in their systems, the healthcare sector has increasingly become a beacon for cybercriminals worldwide. 2024 laid witness to many of the most costly cyberattacks the sector has seen. The Change Healthcare Ransomware attack disruption forced patients to pay out-of-pocket for medications and threatened the financial stability of healthcare providers, with some losing up to $100 million per day.[43] The attack was attributed to the ALPHV/BlackCat ransomware group, and UnitedHealth reported losses from the attack that exceeded $2 billion.

  More reflective of the consequences of MFA bypass and data pilfering, a recent AHA survey in the Lancet revealed that many medical practices faced potential closure because of lost revenue from unpaid claims, putting patient access to medical services at risk."[44]

  Due to the high risks associated with maintaining secure personal data, financial institutions must be on the cutting edge of innovative data security solutions or risk customer backlash and regulatory penalties.[45]

- ### Retail

  According to the 2024 Verizon Data Breach Investigations Report, overall cyber incidents in retail surged by 25% compared to the previous year, with credential theft cited as a leading attack vector.[46] Often stemming from phishing, password pilfering, and the resulting ransomware attacks that follow, the retail sector has experienced the shortcomings and consequences of ineffective legacy MFA firsthand.

  With over 80% of retailers reporting at least one ransomware attack in the past calendar year, it is evident existing security protocols are not providing adequate protection to retail establishments.[47]

Cyberattacks by the Numbers

2024 laid witness to many of the **most costly cyberattacks the healthcare sector** has seen.

64% of technology firms reported at least one ransomware attack in 2024.

80% of retailers reporting at least one ransomware attack in the past calendar year.

SMEs have experienced a **38% increase in breaches** over the past two years.

Nearly 70% of financial companies reported at least one if not multiple ransomware incidents in the past year.

Organizations persistently face ballooning costs from ransomware payments, lost revenue, the expenses of restoring operations, increased cyber insurance premiums, as well as the loss of customer trust.

Recent findings from IBM's 2024 Cost of a Data Breach Report revealed that **the average cost of a data breach globally is**

$4.8 million.

- **Financial Institutions**

  Cyberattacks targeting the financial sector have escalated markedly in 2024, as cybercriminals capitalize on the high value of banking and investment data and the significant losses that organizations in the sector suffer. For financial institutions, 2024 witnessed a 30% uptick in reported breaches compared to the previous year, with credential theft and social engineering emerging as dominant attack vectors for attack.[48]

  Much like within retail, nearly 70% of financial companies reported at least one if not multiple ransomware incidents in the past year.[49]

- **Technology**

  Technology firms saw a 35% increase in reported breaches compared to the prior years, with credential theft and sophisticated phishing campaigns emerging as primary entry points for attackers.[50] The technology sector repeatedly experienced breaches linked to advanced social engineering techniques, signaling that human factors remain a significant vulnerability resulting from the inadequacies of legacy MFA.

  With 64% of technology firms reporting at least one ransomware attack in 2024, new methods to insulate cyber risk are crucial to the sector's long-term viability.[51]

- **SMEs**

  Small and medium enterprises (SMEs) are another rapidly growing target in this increasingly complex threat environment. Historically not prioritized by attackers due to the lower ransomware payments available from SMEs, this group has experienced a 38% increase in breaches over the past two years.[52]

  The upswing in SME-focused attacks is largely a result of the democratization of cyberattacks driven by the affordability and accessibility of malware kits on the dark web, simplifying attacks and increasing the scale and scope of potential victims.[53]

Where Do Users Purchase Attack Services?

The growth of dark web marketplaces has revolutionized how cybercriminals procure tools and services.[54] The dark web has created an accessible marketplace for cybercriminals worldwide, streamlining illicit cyber services, networks of hackers for hire, and previous complex tools into centralized depositories for criminal exploits.

Notable platforms include:

Alphabay and WhiteHouse Market:
These marketplaces feature ransomware-as-a-service (RaaS), credential dumps, and botnets presented in a user-friendly and customer service-oriented platform. Equalizing the playing field, pricing can range from as little as $50 for basic phishing kits to thousands of dollars for custom-built ransomware.[55]

Telegram Channels:
While some marketplaces require complex entry procedures, more often than not, encrypted messaging apps, such as Telegram or WhatsApp, have become central hubs for cybercriminal activity to enable the direct sales of malware and stolen data at the swipe of a finger.[56]

Dedicated RaaS Websites:
Specialization in the marketplace has also enabled ransomware developers to operate professional websites with high levels of customer support and a broad range of subscription options especially as malware-as-a-service. Dedicated RaaS platforms offer user-friendly interfaces, allowing even novice attackers to deploy ransomware.[57]

> The democratization of cybercrime has drastically lowered operational costs for attackers while significantly expanding risks and costs for victims. Breaches involving tools sourced from the dark web result in recovery costs 17% higher than average.

IBM Cost of a Data Breach Report 2024

Trends in Dark Web Cyberattack Kits

The dark web has become the most critical and strategically important marketplace for cyberattack kits, offering tools and services that are more accessible, affordable, and effective than ever before.[58]

Shifts in the centralization and broad accessibility of malware kits and MFA bypass-based attacks have empowered a diverse range of attackers. From opportunistic amateurs to organized crime syndicates, everyone is now able to expand their reach, increase attacks, and drive to compromise as much data as possible.

As a result, the dark web has become a key hub for cybercriminals, providing tools and resources to enable sophisticated attacks, and linking criminals with every tool and resource imaginable to inflict maximum damage, data loss, and economic compromise.[59]

Some of the most significant methods for data compromise in recent years have included:

Modular Attack Kits: Modular attack kits allow attackers to customize their operations and create bespoke attacks on targeted victims. One of the most well-known phishing kits, 16Shop, provides advanced functionality such as pre-built templates targeting platforms like PayPal, Apple, and Amazon to streamline the attack process.[60] Modular attack kits often include step-by-step setup guides, making them accessible even to non-technical users.

AI-Powered Tools: Dark web offerings incorporate AI to increase the effectiveness and customization of MFA bypass-based attacks.[61] Tools such as DeepLocker (a proof-of-concept malware demonstrated by IBM) have proved that AI can evade detection and deliver payloads only when specific conditions are met (e.g., facial recognition of a target).[62]

Subscription Models: The rise of Ransomware-as-a-service (RaaS) has introduced subscription-based models for malware distribution.[63] Platforms like LockBit 3.0 provide a professional interface where affiliates can rent ransomware for a percentage of their profits. Subscribers receive updates, detailed analytics dashboards, and customer support to optimize their campaigns. LockBit alone has been credited with nearly 1,000 ransomware attacks since 2022 while generating millions in ransomware payments worldwide.[64]

Lower Costs: The most critical trend in dark web marketplaces has been the plummeting costs of malware kits and their newfound accessibility to virtually anyone. While in the past cyberattacks could cost thousands or even tens of thousands of dollars, today basic phishing kits are available for as little as $20 on marketplaces like *Genesis Market*.[65]

Meanwhile, high-end ransomware kits (such as those provided by *REvil* before its takedown) were sold for under $100.[66] The lower costs of attacks have democratized cybercrime, enabling even low-budget attackers to launch sophisticated campaigns.

These trends represent how the dark web has become a hub for innovation in cybercrime, offering tools that lower the barriers to entry while increasing the scale and sophistication of attacks.

Impact on Costs and Risks

The democratization of cybercrime has drastically lowered operational costs for attackers while significantly expanding risks and costs for victims. According to IBM's Cost of a Data Breach Report 2024, breaches involving tools sourced from the dark web result in recovery costs 17% higher than average.[67]

6 How Next-Generation MFA Mitigates Risk

Next-Generation Multifactor Authentication (NGMFA) addresses the vulnerabilities of legacy MFA solutions by leveraging advanced, user-friendly technologies. By replacing outdated methods like passwords and SMS codes, Next-Generation MFA provides phishing-resistant protection against modern cyber threats.

Core Features of Next-Generation MFA

95% effective against account attacks

Biometric Verification

Biometrics utilize unique physical traits such as fingerprints, facial recognition, or voice patterns to verify identity. Unlike legacy MFA methodology, biometric data is inherently tied to the individual, making them immune to phishing and interception. Furthermore, Biometric data is securely stored on the device itself and never transmitted or shared, ensuring user privacy and reducing exposure to potential breaches.

From fingerprint-based authentication (which has been shown to reduce phishing success rates by up to 95%) to facial, voice, and even vein pattern identification, Next-Generation MFA provides iron-clad solutions to mitigate legacy threats.[68]

99.9% effective against account attacks

Hardware Devices (FIDO2- Compliant)

Hardware devices provide another effective means to mitigate previous MFA bypasses. By providing physical security keys that generate unique cryptography for each session, users incur notable resistance to phishing and SIM-swapping attacks.

Hardware keys eliminate reliance on vulnerable SMS or email-based authentication methods, ensuring a secure and streamlined login process. A study by Microsoft found that security key-based authentication mitigates 99.9% of account attacks.[69]

99.9% effective against account attacks

Wearable Authentication

Devices (like the Token Ring) combine biometric capabilities with hardware keys that provide seamless, always-available authentication.[70] Integrating wearables, users experience fast, frictionless logins with a simple tap, reducing user effort while maintaining the highest level of security.

By addressing legacy vulnerabilities and leveraging cutting-edge technologies, Next-Generation MFA enables organizations to significantly reduce network intrusions, secure digital assets, protect highly sensitive data, and reduce financial risks.

Legacy MFA vs. Next-Generation MFA

Aspect	Legacy MFA	Next-Generation MFA
Authentication Method	Static methods like SMS and OTP	Dynamic methods like biometrics and hardware devices
Phishing Resistance	Limited; prone to social engineering	High; eliminates shared secrets and user errors
Susceptibility to SIM Swapping	High; SMS-based codes easily intercepted	None; uses non-SMS methods
User Experience	Friction-heavy; frequent prompts and delays	Seamless and adaptive, reducing fatigue
Cost of Breach	High; average breach costs $4.8 million	Significantly reduces the likelihood of a network intrusion
Wearability	Digital elements remain on the cloud or device, thus susceptible to theft	Worn on the body, with biometric data directly linked to the device.

Key takaways

Enhanced Security:

Next-Generation MFA eliminates costly vulnerabilities in legacy systems, dramatically mitigating risks like SIM swapping, and prompt bombing while implementing a range of phishing-resistant solutions to protect user data.

User-Friendly Experience:

Biometric and wearable solutions reduce friction, making authentication seamless for end users while providing industry-leading network and data security. Because the device is on the user's body, it's less likely to be lost or forgotten.

Cost Efficiency:

By preventing breaches and implementing new secure methodologies, Next-Generation MFA lowers all the costs associated with a network intrusion including intrusion detection, system recovery, lost revenue, regulatory penalties, ransomware payments, and expenses associated with class-action lawsuits.

Future-Ready:

Next-Generation MFA solutions defend against emerging threats, ensuring the highest level of security while meeting the evolving cyber risks faced by enterprises and SMEs alike.

Explore Your Options Today

As cyber threats evolve, organizations must adopt proactive strategies to stay ahead. Legacy solutions can no longer provide the protection required in today's landscape. By moving to Phishing-Resistant, Next-Generation MFA, businesses can safeguard sensitive data, maintain stakeholder trust, and ensure operational resilience—avoiding the risks and challenges associated with breaches or ransomware incidents.

Organizations of all sizes can efficiently secure their networks and protect their data against MFA bypass attacks by implementing Next-Generation MFA solutions, like Token Ring.

To learn more about Next-Generation MFA solutions and how they can transform your security strategy **Request a Demo**.

Resources for CISOs

Generative AI and Token Ring

Stop Phishing with Token Ring

Ransomware Protection with Next-Gen MFA

Biometric Authentication with Token Ring

Footnotes

1. https://www.cyberdefensemagazine.com/why-legacy-mfa-is-doa/
2. https://cisoseries.com/join-us-11-08-24-for-hacking-mfa-super-cyber-friday/
3. https://www.cisa.gov/about/2024YIR
4. https://www.ibm.com/reports/data-breach
5. https://www.microsoft.com/security/blog/2023/03/13/attacker-innovation-evolves-phishing-and-beyond/
6. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
7. https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/
8. https://securityintelligence.com/articles/decade-global-cyberattacks-where-they-left-us/
9. https://securityintelligence.com/news/research-finds-56-percent-increase-active-ransomware-groups/
10. https://www.infosecurity-magazine.com/news/2024-phishing-attacks-double
11. https://www.tokenring.com/biometric-authentication-ring
12. https://www.microsoft.com/security/blog/2019/08/20/why-you-should-use-multi-factor-authentication/
13. https://aws.amazon.com/what-is/mfa/
14. https://www.verizon.com/business/resources/reports/dbir/
15. https://securityintelligence.com/articles/decade-global-cyberattacks-where-they-left-us/
16. https://securityintelligence.com/news/research-finds-56-percent-increase-active-ransomware-groups/
17. https://www.cisa.gov/about/2024YIR
18. https://www.csis.com/the-hub/threat-matrix-report-access
19. https://www.sophos.com/en-us/content/state-of-ransomware
20. https://www.cyberdefensemagazine.com/why-legacy-mfa-is-doa/
21. https://www.ibm.com/reports/data-breach
22. https://www.ibm.com/think/topics/man-in-the-middle
23. https://my.uq.edu.au/information-and-services/information-technology/cyber-security/cyber-security-uq/mfa-prompt-bombing-scam
24. https://www.kaspersky.com/resource-center/threats/sim-swapping
25. https://www.ibm.com/reports/data-breach
26. https://www.securitymagazine.com/articles/99553-ransomware-attacks-affect-consumer-behaviors
27. https://www.cyberdefensemagazine.com/why-legacy-mfa-is-doa/
28. https://csrc.nist.gov/glossary/term/defense_in_depth
29. https://www.knowbe4.com/hubfs/KB4-11WaystoDefeat2FA-RogerGrimes.pdf
30. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
31. https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion
32. https://oit.utk.edu/security/learning-library/article-archive/two-factor-authentication-2fa-prompt-bombing/
33. https://www.wired.com/story/uber-hack-mfa-phishing/
34. https://blog.24by7security.com/the-real-cost-of-that-uber-ride
35. https://www.darkreading.com/cyberattacks-data-breaches/uber-breach-external-contractor-mfa-bombing-attack
36. https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf
37. https://www.tokenring.com/hubfs/Collateral/How%20to%20choose%20the%20best%20MFA%20-%20Token%20Ring%20-%20eBook.pdf
38. https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2
39. https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2
40. https://www.microsoft.com/security/blog/2019/08/20/why-you-should-use-multi-factor-authentication/
41. https://www.tokenring.com/biometric-authentication-ring
42. https://thehackernews.com/expert-insights/2024/06/the-democratization-of-cyberattacks-how.html
43. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
44. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(24)01074-2/fulltext
45. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm
46. https://www.verizon.com/business/resources/reports/dbir/
47. https://www.sophos.com/en-us/content/state-of-ransomware
48. https://www.verizon.com/business/resources/reports/dbir/
49. https://www.sophos.com/en-us/content/state-of-ransomware
50. https://www.verizon.com/business/resources/reports/dbir/
51. https://www.sophos.com/en-us/content/state-of-ransomware
52. https://cybersecurityventures.com/cybersecurity-almanac-2023/
53. https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/news/smes-must-do-more-to-combat-the-growing-threat-of-cyber-attacks/
54. https://www.researchgate.net/figure/List-of-all-dark-web-marketplaces-together-with-their-specialization-and-a-brief_tbl3_343441854
55. https://krebsonsecurity.com/2023/04/inside-alphabay-dark-marketplace/
56. https://blog.checkpoint.com/2023/02/28/cybercrime-on-telegram-how-cybercriminals-exploit-the-messaging-platform/
57. https://news.sophos.com/en-us/2023/07/19/the-state-of-ransomware-2023/
58. https://www.msspalert.com/analysis/ai-now-a-staple-in-phishing-kits-sold-to-hackers
59. https://www.secureworld.io/industry-news/dark-web-marketplaces-threats
60. https://www.trendmicro.com/en_us/research/23/i/revisiting-16shop-phishing-kit-trend-interpol-partnership.html
61. https://dfi.kaspersky.com/blog/ai-in-darknet
62. https://research.ibm.com/publications/deeplocker-concealing-targeted-attacks-with-ai-locksmithing
63. https://news.sophos.com/en-us/2023/07/19/the-state-of-ransomware-2023/
64. https://www.weforum.org/stories/2024/02/lockbit-ransomware-operation-cronos-cybercrime/
65. https://securityintelligence.com/articles/cyber-crime-cheap/
66. https://www.sisainfosec.com/blogs/revil-ransomware-aka-sodinokibi-raas/
67. https://www.ibm.com/reports/data-breach
68. https://www.researchgate.net/publication/286147681_A_brief_review_Fingerprint_authentication_system
69. www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
70. https://www.tokenring.com/

Token

tokenring.com | (866) 328-7464

About Token

In a world of stolen identities and compromised user credentials, Token is changing the way organizations secure access to their digital realms by providing passwordless, biometric, next generation multifactor authentication solutions. To learn more, **visit www.tokenring.com**.

Homepage

Try Token

Talk to an Expert