Multi-Factor Authentication & Smishing

August 10, 2023

Agenda

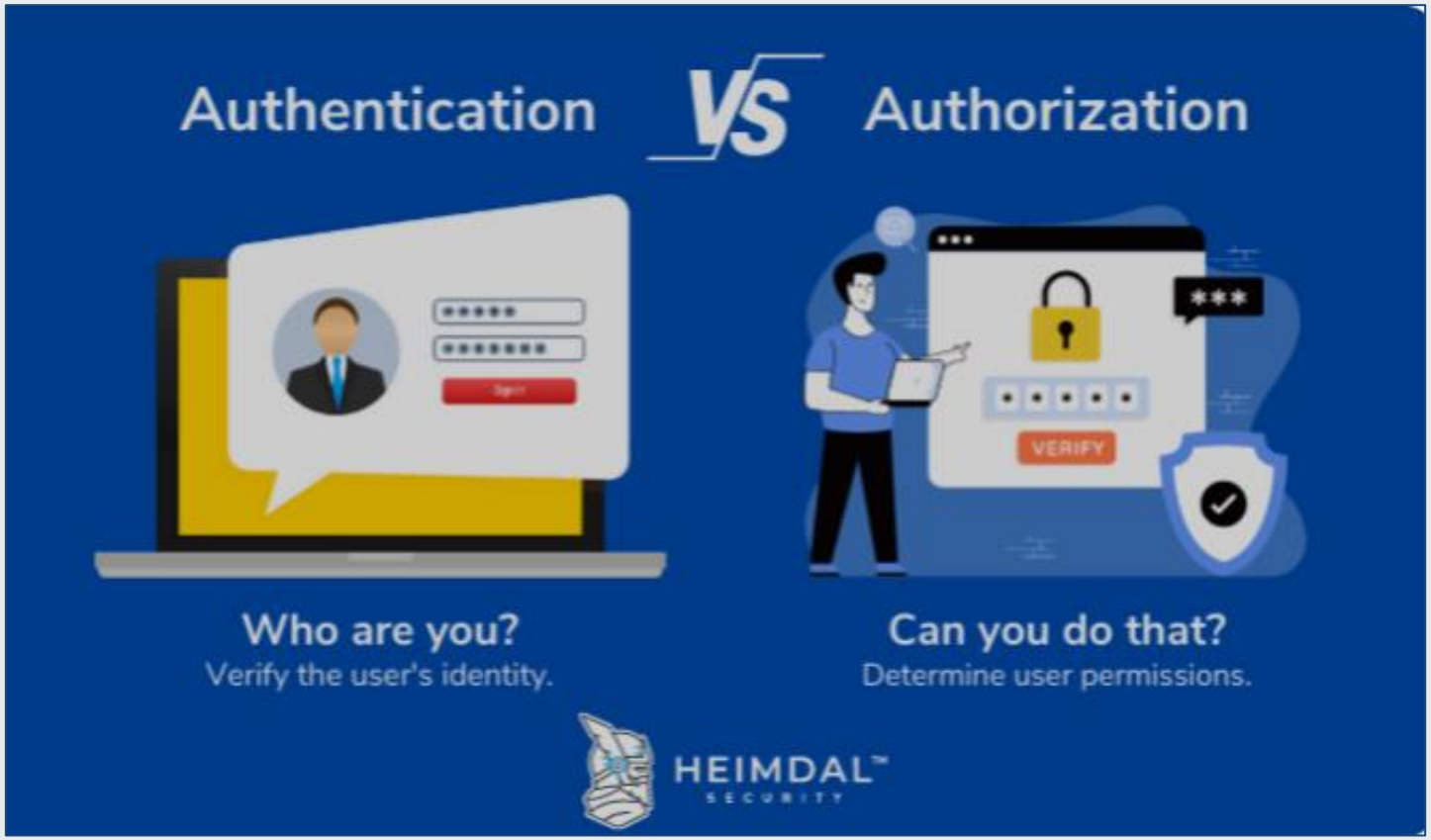
- Multi-Factor Authentication (MFA): An Overview
- Smishing
- Unintended Consequences of MFA
- Attack Vectors
- Threats to the Health Sector
- Recommendations
- Cybersecurity Resources
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Multi-Factor Authentication (MFA): An Overview

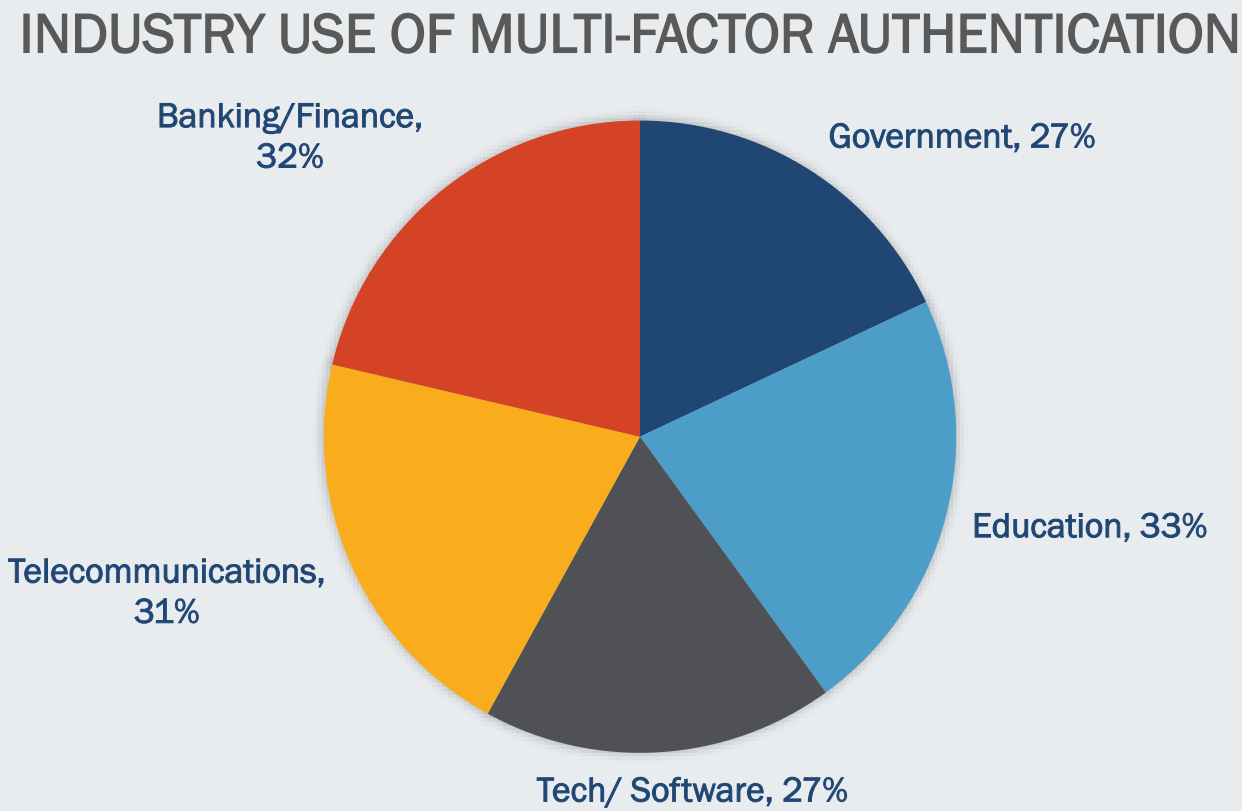


Authentication vs. Authorization in the Health Sector

What is Multi-Factor Authentication?

- *Knowledge Factor*
- *Possession Factor*
- *Inherence Factor*

Statistics on Use of MFA Report



Source: Zippia

DISCLAIMER: Per the data, percentages reflect MFA usage in each industry.

State of MFA Report

According to Prove Identity's 2023 State of MFA Report, consumers desire more streamlined authentication options.

- While MFA in the workplace continues to lag, there is some progress.
- MFA adoption rates vary significantly by service/industry.
  - When given an option:
    - 61% of consumers enable MFA for online healthcare portals and apps.
    - 60% of consumers enable MFA for online banking.
    - 70% of consumers do not enable MFA when using social media.

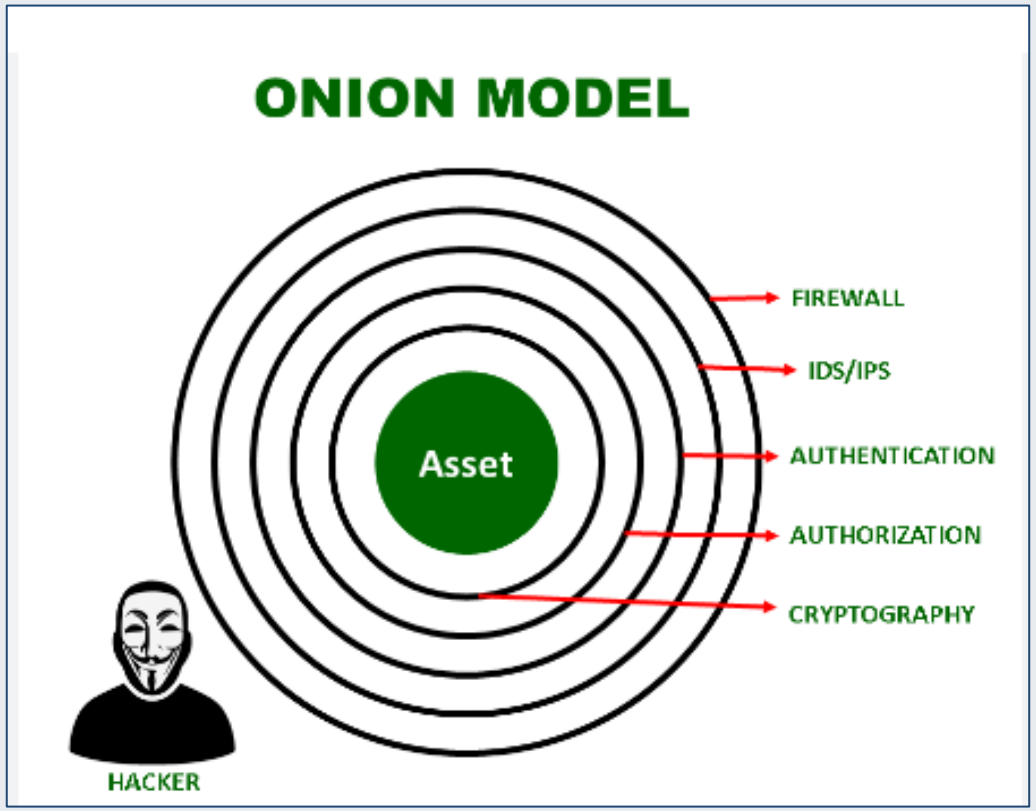
Source: Prove Identity

Security & the Onion Model in Healthcare Cybersecurity

Source: Ateam-Oracle

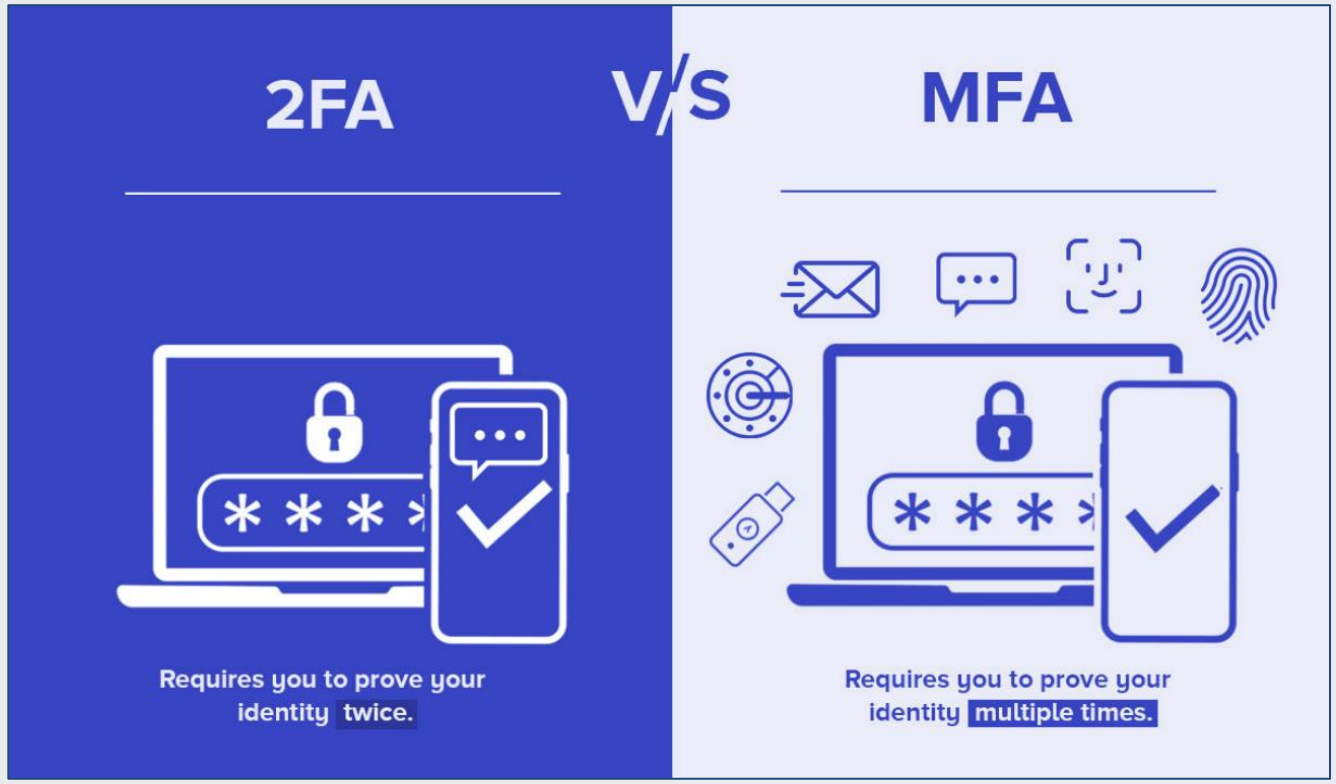
MFA vs. Onion Model

MFA is similar to the onion model, because both use a layered defense method.



2FA vs. Multi-Factor Authentication (MFA)

- 2FA – Requires two factors of authentication.
- MFA – Requires at least two or more factors of authentication.
- Multi-factor authentication is a stronger form of protection than two-factor authentication because there is an additional step of verification.

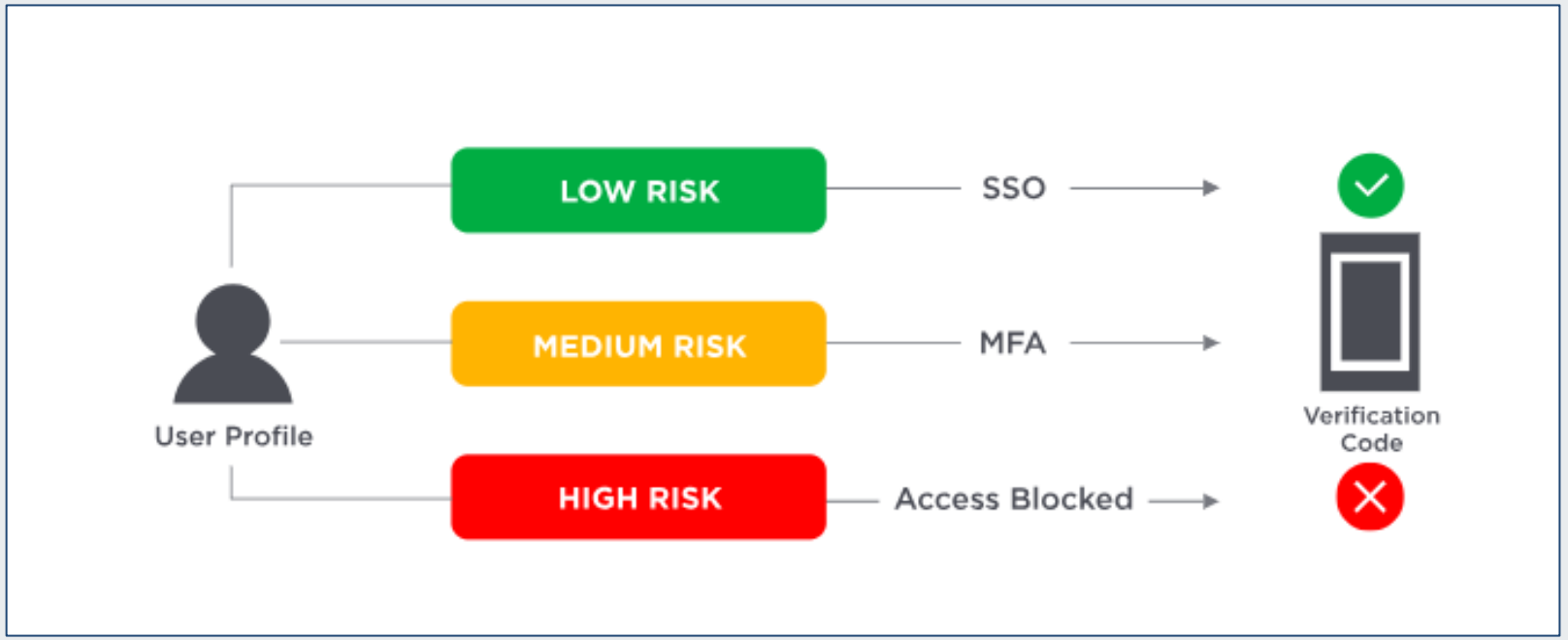


Common Types of MFA/2FA Authentication

- Hardware tokens
- SMS text-message
- Software tokens
- Push notifications
- Biometric 2FA

Authentication & Artificial Intelligence

Adaptive Authentication or Risk-based Authentication



Source: OneLogin

Biometric Authentication Technology: Everything You Need to Know

- AI & Remote Workforce
- Continuous Monitoring
- Every Action Has A Reaction Presentation Attacks
- Authentication Identity Proofing

Source: The Spotlight

AI & Remote Workforce

- Organizations that are looking to improve their security and reduce risk should consider implementing an AI-based MFA system. AI-based systems are more effective at detecting and stopping fraud and can also be used to verify the identity of users in real-time. This method will make it much more difficult for hackers to gain access to sensitive information.
- One of the most promising applications of AI for MFA is behavioral biometrics. This is a type of authentication that uses artificial intelligence to verify the identity of a user based on their behavior. Behavioral biometrics can be used to track things like how a user types, how they hold their phone, and even their unique gait.

Continuous Monitoring

A bad actor can and will look for gaps in authentication processes, such as during and even after hiring, to circumvent identity verification – even utilizing surrogates to help conceal their true identity and nefarious intentions. By using behavioral analytics with acritical intelligence (AI) to continuously monitor the attributes of individuals, organizations can detect fraudulent usage of a user's device and account. User behavioral analytics include:

- **Location:** A combination of an IP address, Wi-Fi, GPS, and cellular data can be correlated with the presented identity to check for consistency and to affirm the identity claim.
- **Device:** Attributes of a user's device, such as browser language and time zone, etc., can be correlated with the presented identity for consistency and identity affirmation.
- **Email:** Link analysis can be used to verify when the email has been used prior with the presented identity.
- **Phone number:** Cross referencing a phone number to the network operator and other dates can reveal identity data to affirm or refute an identity claim.

Presentation Attacks

In cybersecurity, every action has a reaction. As biometric technology has grown in implementation, so has the need of cybercriminals to circumvent these security controls.

One such advanced form of a biometric spoofing attack is called a presentation attack. This attack, commonly referred to as spoofs or presentation attacks (PAs), is the process of subverting a biometric system using tools called presentation attack instruments (PAIs).

There are three levels of presentation attack sophistication:

- **Level 1** - Requires little to no expertise.
- **Level 2** – Requires moderate skill and practice.
- **Level 3** - Requires extensive skill and practice.

Authentication Identity Proofing

To help protect against fraudulent authentication such as biometric spoofing attacks, it is recommended that organizations in the health sector consider utilizing the following security controls:

- **Selfie** – Similar to a photo identification; employees can use their devices such as a cell phone or webcam to capture a selfie and perform a liveness detection test.
- **Remote Fingerprinting** – Individuals can use their smartphones to capture and verify multiple fingerprints in a contactless and non-intrusive manner, which is helpful for the healthcare sector, where cyber threats are on the rise.
- **Voice** – Users can utilize voice software for authentication purposes.
- **Video Know Your Customer** – Involves live video chat between employees and employers, which provides another secure form of identity authentication.

MFA Authentication in Cloud Computing

- Connect MFA with cloud apps and services.
- Remote workers require endpoint protection.
- With the advent of cloud computing, MFA has become even more necessary.
- As companies move their systems to the cloud, they can no longer rely upon a user being physically on the same network as a security factor.
- Additional security needs to be put into place to ensure that those accessing the systems are not bad actors.
- As users are accessing these systems any time and from any place, MFA can help ensure that they are who they say they are by prompting for additional authentication factors that are more difficult for hackers to imitate or use brute force methods to crack.

Benefits of Multi-Factor Authentication

Source: Keeper Security

Smishing

What is Smishing?

- Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link, which sends the attacker private information or downloads malicious programs to a smartphone.
- Many users are already aware of the dangers of clicking a link in email messages; fewer people are aware of the dangers of clicking links in text messages. Users are much more trusting of text messages, so smishing is often lucrative to attackers phishing for credentials, banking information and private data.

How Smishing Works

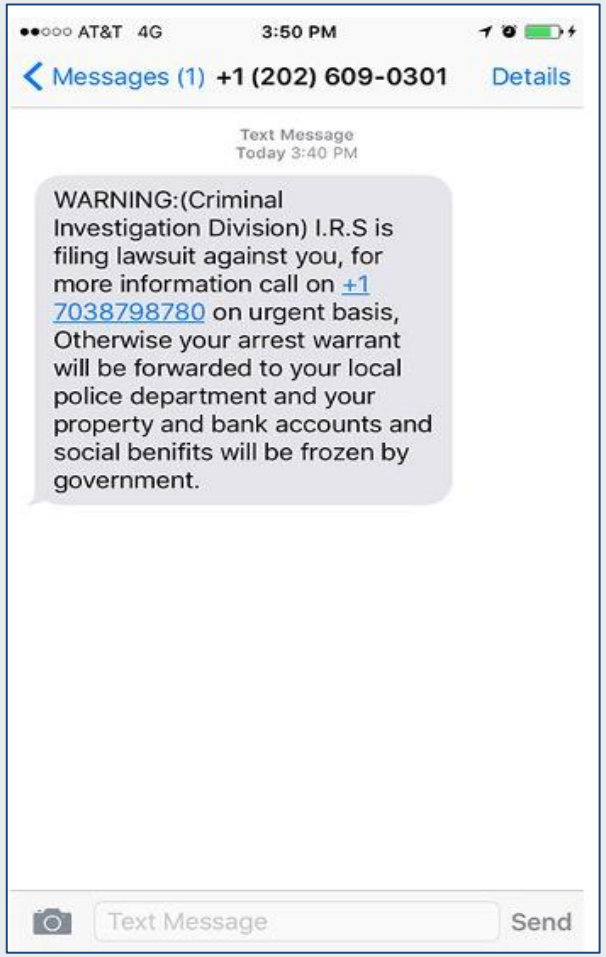
Like a phishing attack, smishing tricks us into believing that fake messages are legitimate so that we interact with them without concern. Smishing attacks work by using some or all the following features:

- Context
- Target selection
- Social engineering
- Malicious attachments
- Malicious links

Example of A Smishing Attack

The following image displays a sample smishing attack.

Here, the attacker poses as the IRS and threatens the recipient with arrest and financial ruin unless they call the number in the text. If the recipient calls, they get scammed into sending money.

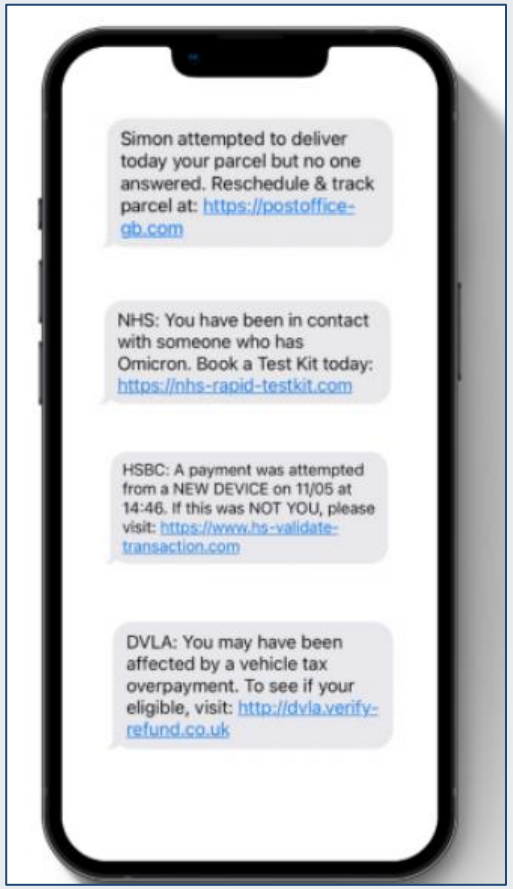


The Psychological Aspect of Smishing/Phishing

According to cybersecurity experts, using psychological tactics to get users to unknowingly compromise a device plays a significant role in smishing/phishing attacks.

How to Identify and Mitigate This Threat:

- Deadlines and time-sensitive language
- Scarcity
- A quick fix

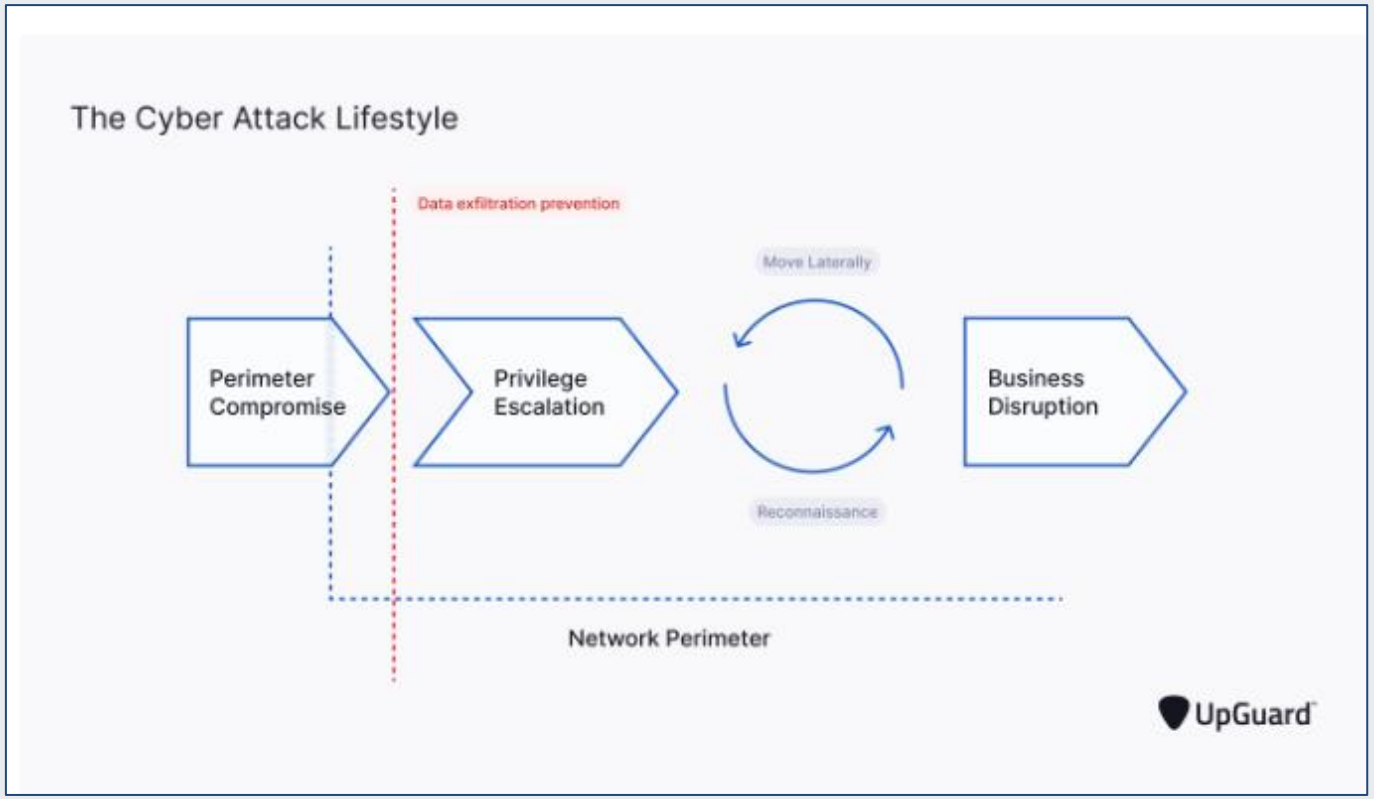


Source: Cyber Fraud Centre Scotland

Threats to the Health Sector

Top Cyber Threats in Healthcare

- Phishing/Smishing
- Ransomware Attacks
- Data Breaches
- DDos Attacks
- Info-Stealing Malware



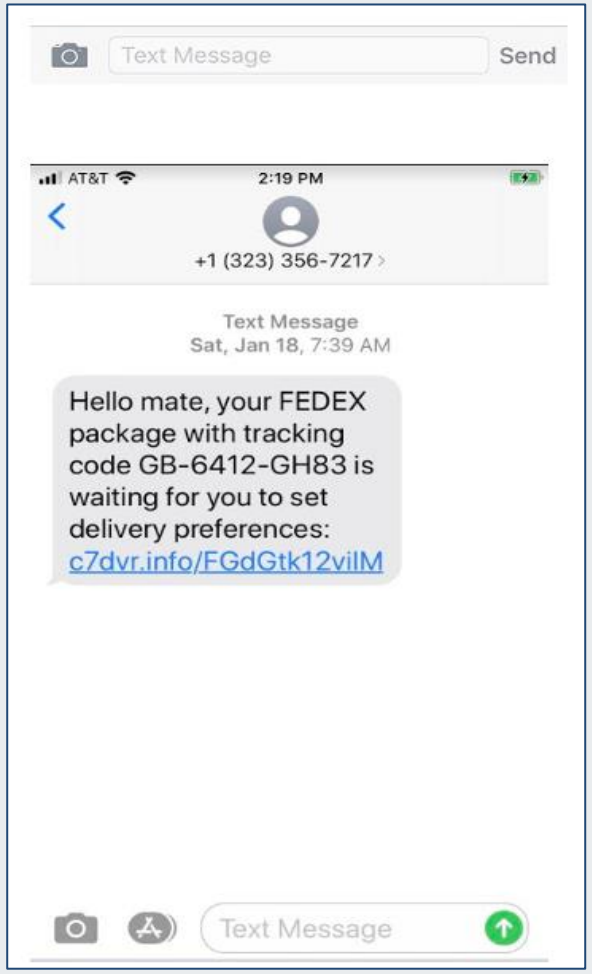
Info-Stealing Malware

According to BlackBerry's recent quarterly Global Threat Intelligence Report, the health sector and financial sector are the top two targeted industries in recent months.

- The report covers attacks logged between March—May 2023.
- During that 90-day period, BlackBerry observed threat actors deploying approximately 11.5 attacks per minute, including 1.7 novel malware samples per minute. The latter number is a 13 percent increase from the previous month.
- The last quarter of the report highlighted an increase in SEO poisoning in healthcare. This quarter focused on the rapid increase of info-stealing malware, also known as infostealers.
- Infostealers live in infected computers and gather information, allowing cyber threat actors to obtain credentials and exploit organizations.
- According to BlackBerry, the value of protected health information (PHI), as well as the high-stakes nature of the industry, are factors that contribute to healthcare being targeted often by threat actors who believe they can pressure organizations to pay a ransom.

The Threat of Smishing

- Smishing is where an attacker uses a convincing text message to trick or lure targeted recipients into clicking a link, which then sends the attacker private information or downloads malicious programs to a smartphone.
- A more common smishing attack uses brand names with links purported to be to the brand's site. Usually, an attacker will tell the user that they have won money or will provide a malicious link purported to be for tracking packages, as in the following example.



Unintended Consequences of MFA

Challenges of Multi-Factor Authentication

While multi-factor authentication is a valuable method of protection, it can also be the source of some cybersecurity problems. Two major challenges associated with MFA are email or SMS OTPs, such as:

- Friction and frustration
- Security vulnerabilities

Organizations can overcome these obstacles by considering adopting next-generation or new multi-factor authentication solutions.

MFA Notification Fatigue

MFA notification fatigue is another major challenge related to multi-factor authentication. Cyber threat actors often exploit the psychological aspect of MFA notifications, using it for their own gain, in what is called an MFA fatigue attack.

Source: Mio Dispatch

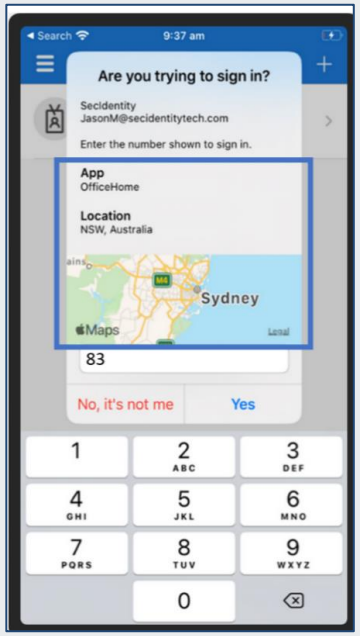
What Is an MFA Fatigue Attack?

An MFA fatigue attack, or MFA spamming, involves a threat actor bombarding an account owner incessantly with MFA push notifications until the target slips up, or is simply worn down psychologically from numerous notifications and approves the login request.

Once an MFA request is approved, the cyber threat actor will be able to gain unauthorized entry to the user's account and use this access to their advantage.

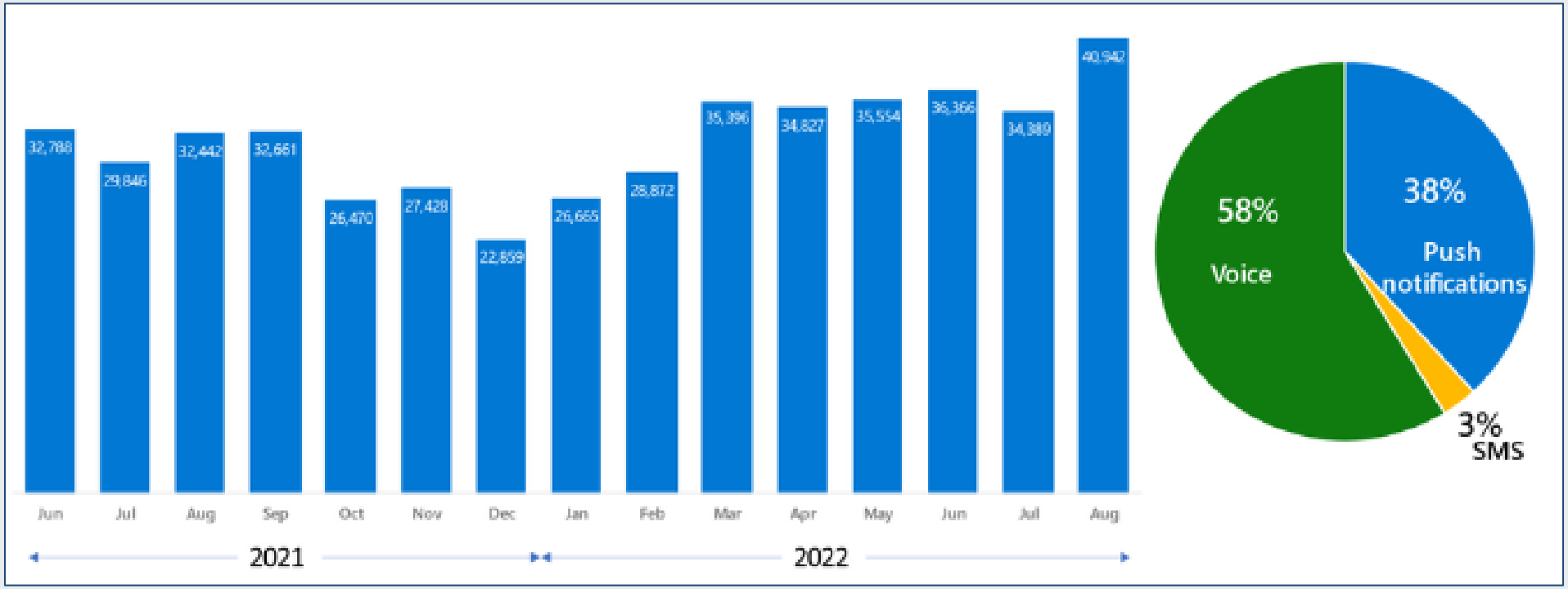
<u>How to protect against an MFA fatigue attack</u>:

- Enable Additional Context
- Adopt Risk-Based Authentication
- Implement the FIDO2 Authentication
- Disable Push Notifications as a Verification Method
- Limit Authentication Requests
- Spread Security Awareness Around MFA



Source: Microsoft

MFA Fatigue Attack Statistics

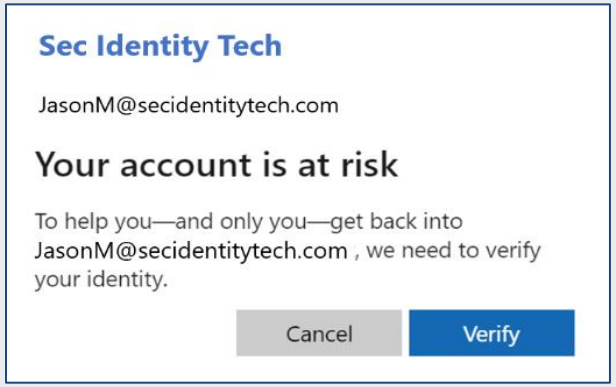


MFA Fatigue Attacks
Source: Microsoft | Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts.

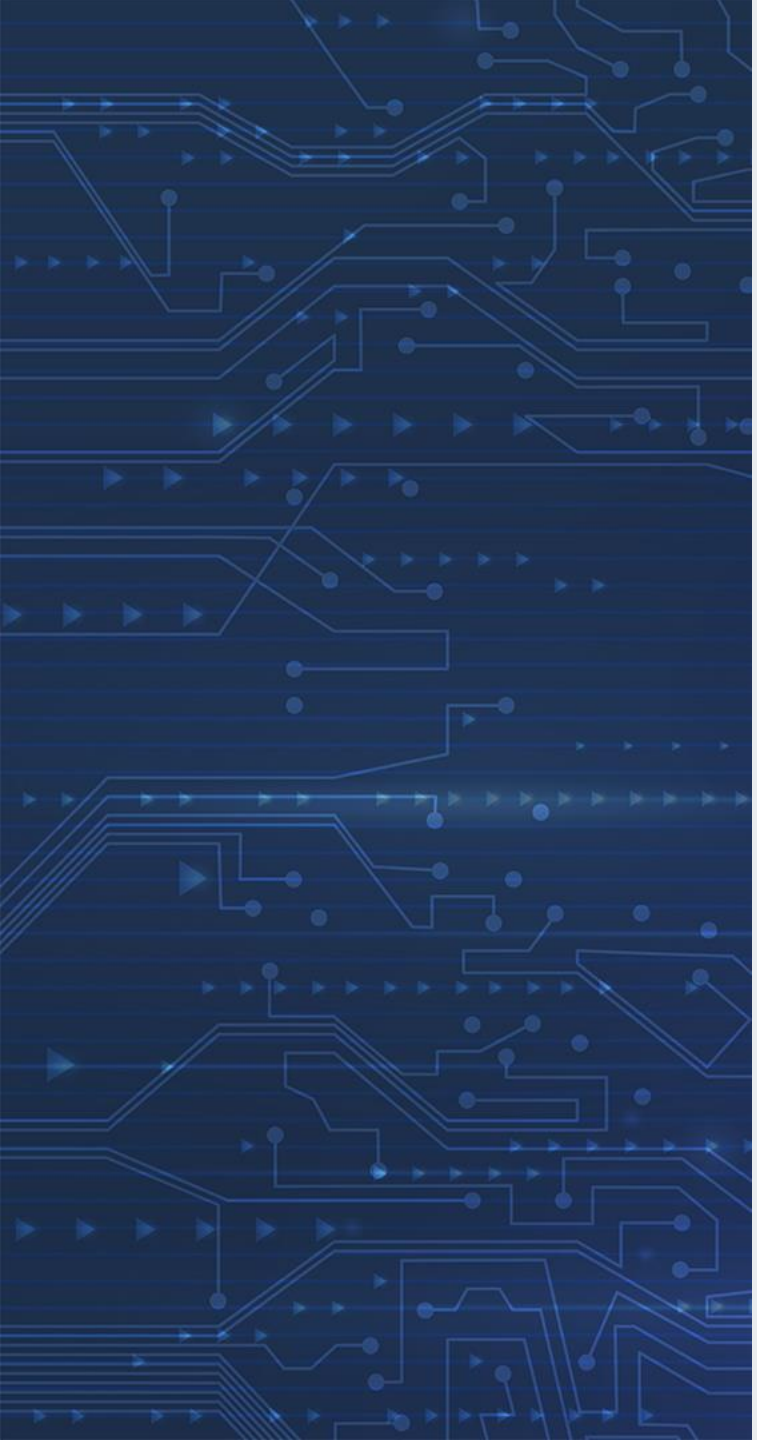
MFA Fatigue Attack Mitigations

According to Microsoft, MFA fatigue attacks or MFA spamming can be a significant problem, and with the increase in this attack vector, they recommend taking the following steps:

- Prevent good users from accidentally approving sign-ins.
- Help users make good decisions by providing them with more context.
- If your healthcare organization is still migrating to the Authenticator app, then automatically change the passwords of all at-risk users.
- Additionally, HC3 recommends conducting annual training and refresher courses.



Source: Microsoft



Attack Vectors

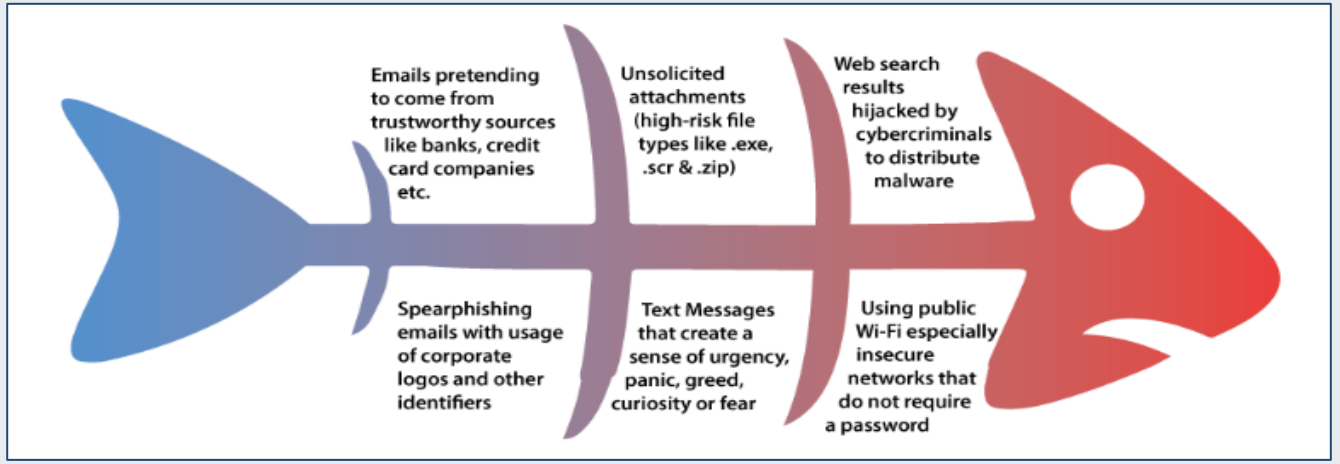
Man-in-the-Middle (MitM)

Source: Malwarebytes

Smishing

Smishing is an easy attack vector for threat actors to utilize against users who rely on text messages to communicate.

- These type of crimes can lead to security issues and privacy concerns, such as identity theft.
- While a proactive approach can prevent smishing attacks, it is also recommended for users to treat suspicious text messages with caution and implement security software to all devices.

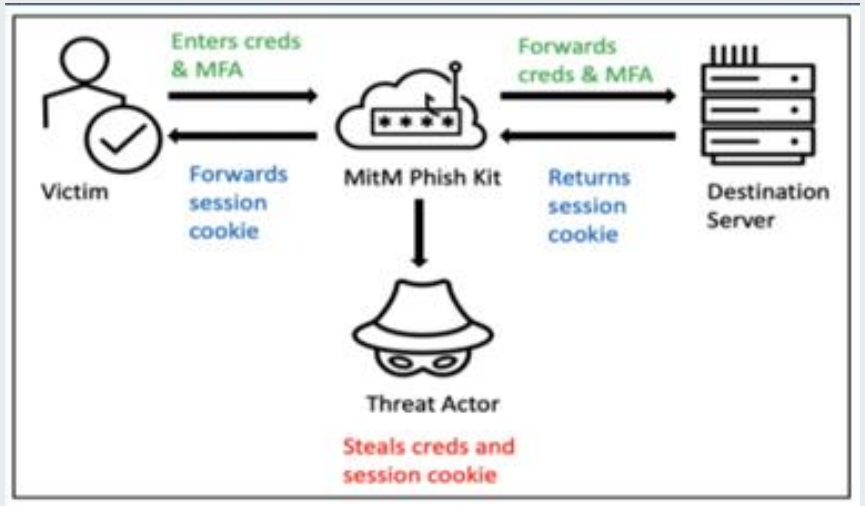


Source: E-C Council Aware

MFA Phishing Kits

MFA phishing kits pose a significant threat to the HPH sector, because this credential phishing software specifically targets MFA, which is used to protect accounts from unauthorized access.

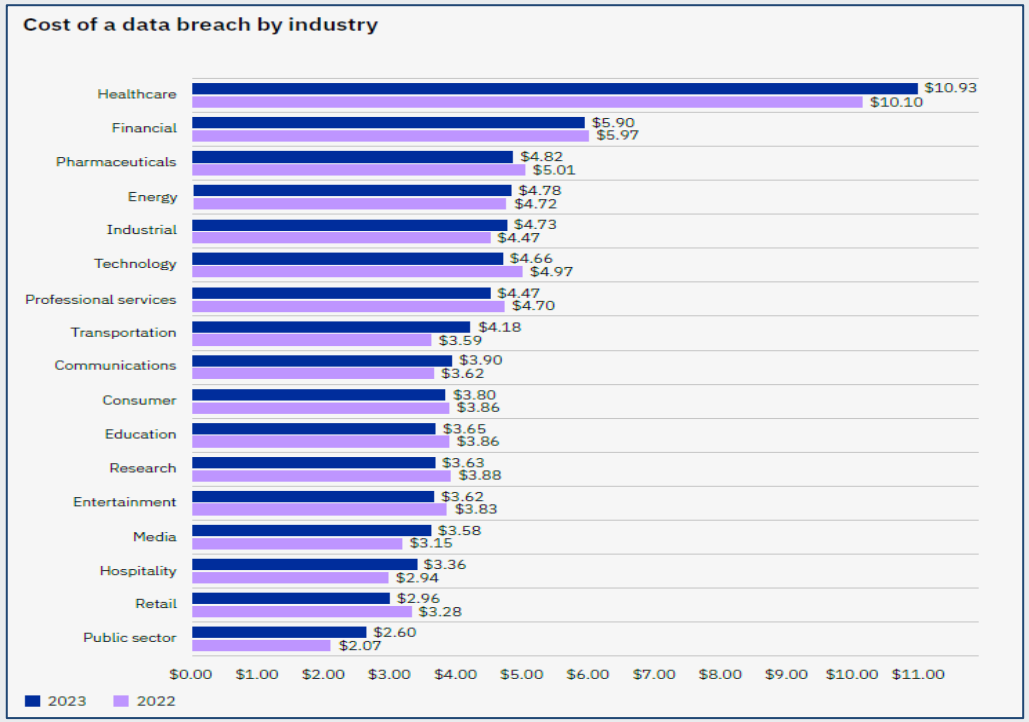
According to Proofpoint, there are numerous MFA phishing kits that range from simple open-source kits with human readable code and basic functionality, to sophisticated kits that use built-in modules and numerous layers of obfuscation, which give them the ability to steal MFA tokens, usernames and passwords, as well as credit card and social security numbers.



Source: Proofpoint

Cost of Data Breaches By Industry

According to IBM's 2023 Cost of A Data Breach Report, the cost of a data breach in healthcare increased from USD 10.10 million in 2022 to USD 10.93 million in 2023. With an 8.2 percent increase, the health sector reported the highest costs for the 13th consecutive year.



Source: IBM

Recommendations

Using MFA to Protect the Health Sector

The health sector is a top target for cyber threat actors, and it is imperative to take the necessary steps to protect sensitive information. As stated in this brief, there are benefits of multi-factor authentication, and it is recommended that health sector employees add MFA to all devices. Some benefits of MFA and protection provided to the health sector are:

- Improved Password Hygiene
- Stronger Access Restrictions
- More Secure Telehealth
- Enhanced Insurability

“Protect Ya Neck”…and Your Data from Smishing

- Beware of urgent messages
- Confirm phone numbers
- Do not respond to unknown numbers
- Avoid sharing password information
- Utilize anti-virus or anti-malware software
- Multi-factor authentication
- Avoid clicking any in-message links

Source: Forbes & 1000 Logos

How To Stop Smishing Texts

Here are some proactive steps that are recommended for users to protect work and personal devices from smishing attacks.

How to filter texts on iPhone:

1. Go to **Settings.**
2. Select **Messages.**
3. Swipe the button next to **Filter Unknown Senders.**

How to filter texts on Android:

1. Go to **Messages.**
2. Select the three dots to open **Settings.**
3. Select **Block Numbers and Messages.**
4. Activate **Caller ID and Spam Protection.**

Reducing the Cost of A Data Breach

According to IBM's 2023 Cost of A Data Breach Report, the following can help reduce the cost of a data breach in your organization:

- Build security into every stage of software development and deployment—and test regularly.
- Use MFA and modernize data protection across a hybrid cloud infrastructure.
- Use security AI and automation to increase speed and accuracy.
- Strengthen resiliency by knowing your attack surface and practicing an incident response framework.

Source: Universal Data Incorporated

Cybersecurity Resources

Free Cybersecurity Tools & Resources

HHS HC3

HHS 405(d)
Aligning Health Care
Industry Security Approaches

HHS 405(d)

CISA

CISA

Reference Materials

References

- Abed, A.A.“Stay Ahead of the Game: Top Smishing Defense Tactics You Need to Know,” LinkedIn. March 18,2023. https://www.linkedin.com/pulse/stay-ahead-game-top-smishing-defense-tactics-you-need-abed-a-a-.
- Gardiner, Sarah. “The Psychology Behind Phishing Attacks,” Cyber and Fraud Centre Scotland. Publication date. https://cyberfraudcentre.com/the-psychology-behind-phishing-attacks.
- Editorial Team. “Healthcare Cyber Attacks: The 5 Biggest Cybersecurity Threats in Healthcare 2023,” Just Total Tech. March 2,2023. https://justtotaltech.com/healthcare-cyber-attacks/#:~:text=Patient%20information%20is%20highly%20valuable,hacking%2C%20and%20unsecured%20IoT%20devices.
- Kolbasuk McGee, Marianne. “Feds Urge Healthcare Providers, Vendors to Use Strong MFA,” Bank Info Security. July 3,2023. https://www.bankinfosecurity.com/mfa-a-22434.

- Andrioaie, Andra. “Authentication vs. Authorization: the Difference Explained,”Heimdal Security. April 21, 2022. https://heimdalsecurity.com/blog/authentication-vs-authorization/
- Thakkar, Kiran. “Security - Like Layers of Onion (Defense),” ATeam-Oracle. January 3, 2023. https://www.ateam-oracle.com/post/security-layers-of-defense
- Suresh, Vignesh. “Introduction to Security Defense Models,” Geeks for Geeks. May 22, 2020. https://www.geeksforgeeks.org/introduction-to-security-defense-models/
- “What is Multi-Factor Authentication (MFA) and How Does it Work?,” OneLogin. July 4, 2023. https://www.onelogin.com/learn/what-is-mfa
- M.,Richard. “Biometric Authentication Technology – Everything You Need To Know,” ShuftiPro. November 6, 2020. https://shuftipro.com/blog/biometric-authentication-technology-everything-you-need-to-know/

- Yu, Eileen. “These medical IoT devices carry the biggest security risks,” ZD Net. April 19, 2023. https://www.zdnet.com/article/these-medical-iot-devices-carry-biggest-security-risks/.
- Benefits of Multifactor Authentication in Healthcare,” Global Data Systems. https://www.getgds.com/resources/blog/healthcare/benefits-of-multifactor-authentication-in-healthcare
- Yoneda, Yuka. “Prove Identity’s 2023 State of MFA Report Reveals Consumer Attitudes Towards Multi-Factor Authentication,” Prove. April 24, 2023. https://www.prove.com/blog/prove-identity-2023-state-of-mfa-report-consumer-attitudes-multi-factor-authentication
- McKeon, Jill. “OCR Reinforces Importance of Multi-Factor Authentication in Healthcare,” Health IT Security. July 5,2023. https://healthitsecurity.com/news/ocr-reinforces-importance-of-multi-factor-authentication-in-healthcare .

- “Top 6 Hackable Medical IoT Devices,” Critical Insight. Publication date. https://www.criticalinsight.com/resources/news/article/top-6-hackable-medical-iot-devices .
- Tsiukhai,Tatsiana. “When Innovation Hurts: IoT Vulnerabilities in Healthcare,” Soft EQ. May 17, 2022. https://www.softeq.com/blog/top-5-iot-vulnerabilities-in-healthcare.
- Palmer, Danny; Rodriguez, Robert(Art). “These Experts Are Racing to Protect AI from Hackers. Time is Running Out,” ZD Net In Depth. Publication date. https://www.zdnet.com/in-depth/innovation/these-experts-are-racing-to-protect-ai-from-hackers-time-is-running-out/.
- Trevico, Aranza. “The Benefits of Multi-Factor Authentication,” Keeper Security. December 20, 2022. https://www.keepersecurity.com/blog/2022/12/20/the-benefits-of-multi-factor-authentication/
- Stouffer, Clare. “What is 2FA? A simplified guide to two-factor authentication,” Norton. June 16, 2022. https://us.norton.com/internetsecurity-how-to-importance-two-factor-authentication.html

Questions

FAQ

Upcoming Briefing

- September 21 – North Korea and China Cybercrime Threats to the U.S. HPH

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV