LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing Multifactor Authentication

OVERALL CLASSIFICATION IS

TLP:WHITE

March 19, 2020

Agenda

- Introduction
- Multifactor Authentication (MFA)
- SMS 2 Factor Authentication
- Hard Token Multifactor Authentication
- Soft Token Multifactor Authentication
- Password-less Multifactor Authentication
- Authentication Attack Matrix
- Managed Service Providers MFA
- References
- Questions

Slides Key:

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

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

Introduction

- A new report released by the World Economic Forum finds that freeing ourselves of passwords will actually make us safer and businesses more efficient.
- Cybercrime is set to cost the global economy $2.9 million every minute in 2020 and some 80% of these attacks are password-related. Knowledge-based authentication – whether with PINs, passwords, passphrases, or whatever we need to remember – is not only a major headache for users, it is costly to maintain. (World Economic Forum)

Courtesy of Cybersecurity Ventures

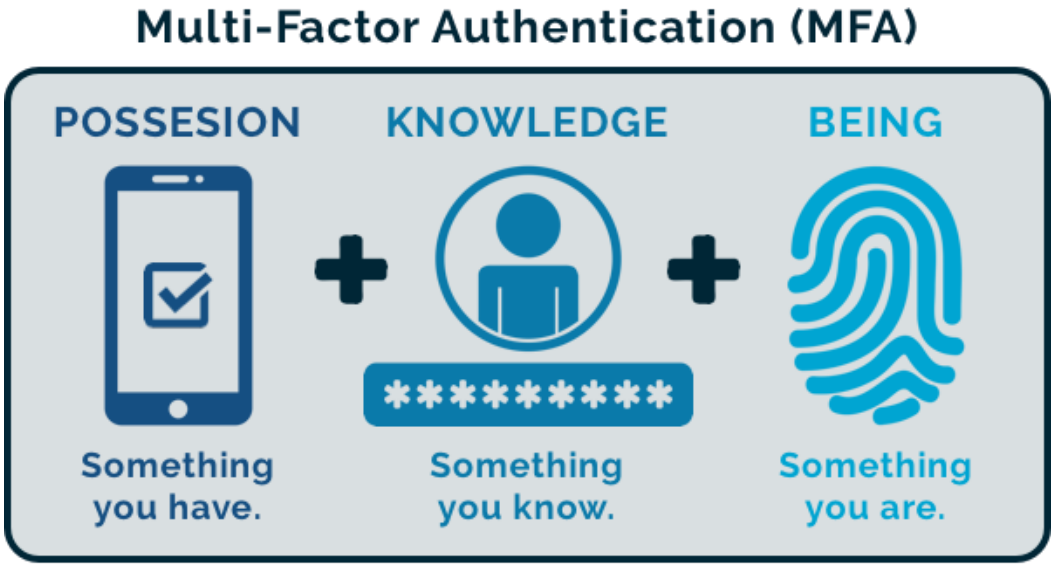
Introduction

- Over a 17-month period, from November 2017 through the end of March 2019, security and content delivery company Akamai detected 55 billion credential stuffing attacks across dozens of verticals. While some industries were more heavily targeted than others -- for example gaming, retail and media streaming -- no industry was immune.
- Multi-factor authentication has evolved as the single most effective control to insulate an organization against remote attacks and when implemented correctly, can prevent most threat actors from easily gaining an initial foothold into your organization, even if credentials become compromised.

Courtesy of INC

Multifactor Authentication (MFA)

- Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
- Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).
- The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database.
  - If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.



Courtesy of Business 2 Community

SMS 2 Factor Authentication

- Instead of generating an One Time Password(OTP) on a separate piece of hardware, a server generates the code and delivers it to the user via SMS to their mobile device.
- As most people have a mobile phone of some kind, avoiding the cost of a hardware token has led many service providers to adopt 2FA SMS for large-scale consumer use.
- It is still the most widely adopted 2FA method in use today and can be considered the “hard token equivalent” of the consumer use case - but SMS based authentication carries significant risks that have all but stalled its growth.
    - SMS messages can easily be intercepted via **SS7 (Signaling System 7) network attacks**, **SIM-Swapping** has become commonplace resulting in OTP messages being delivered to the wrong mobile phone, and the ease with which popular **keyloggers and mobile malware variants** such as Modlishka come equipped with **automated SMS OTP stealing** functions.

Courtesy of Malwarebytes

SMS 2 Factor Authentication

1

Upon signing up for a new web or mobile app, the user provides their mobile phone number.

2

The user receives an SMS message with a unique code when they first login or perform other actions such as requesting a password reset.

3

Entering the unique code into the website or app confirms their identity and allows them to complete the registration process.

mGage

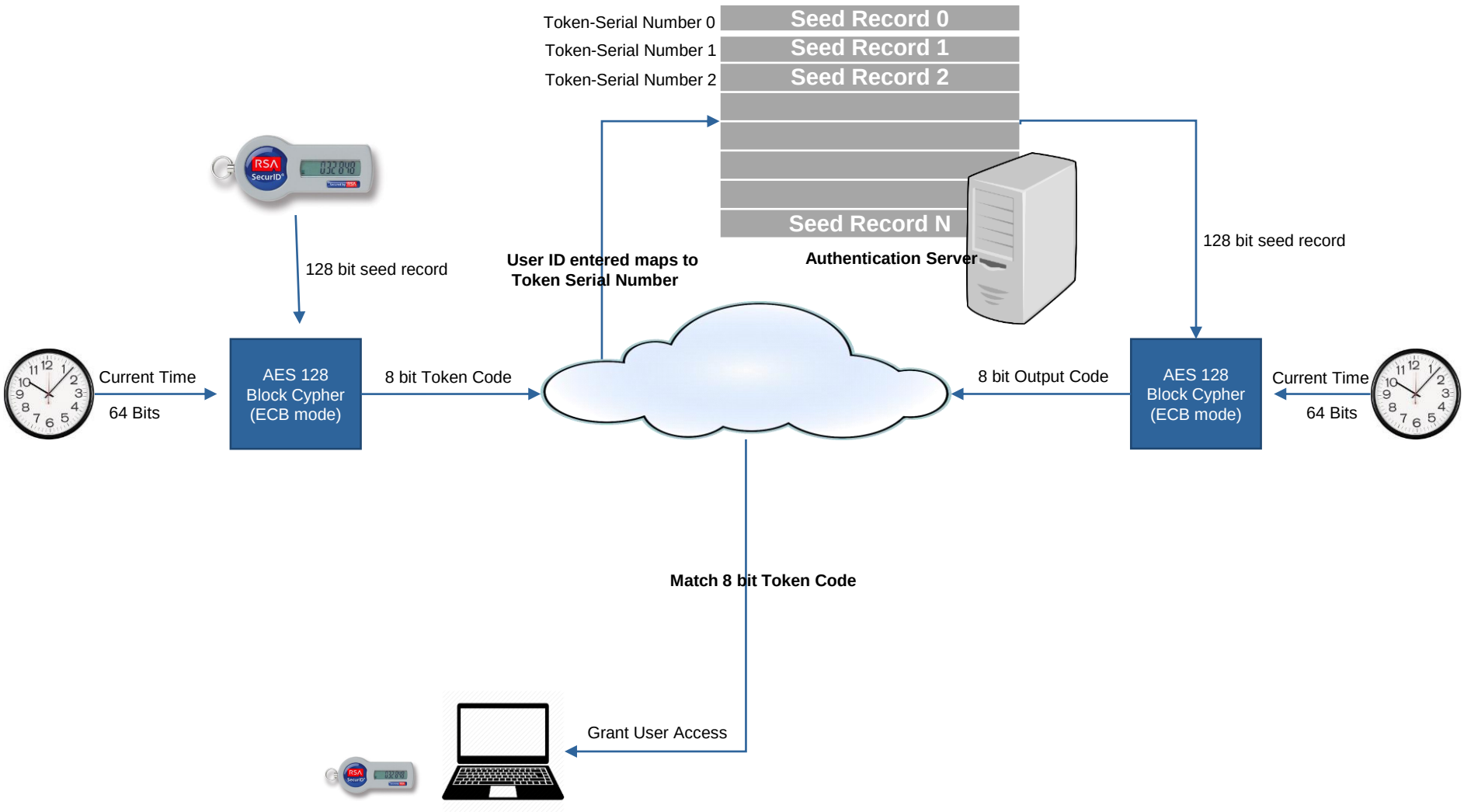
Hard Token Multifactor Authentication

- Hardware security tokens became popular they brought the world more security, using time-based one-time password (TOTP) algorithms and tamper-resistant hardware.
- Hard tokens introduced a “second-factor” to authentication (2FA) and were good at providing additional standards-based security for authentication sessions that needed a higher level of assurance.
- These devices promised to provide an additional layer of security above passwords – but over the years have been found to possess a number of user experience drawbacks as well as security vulnerabilities.

Courtesy of CDW

Courtesy of PIVKey

Hard Token Multifactor Authentication

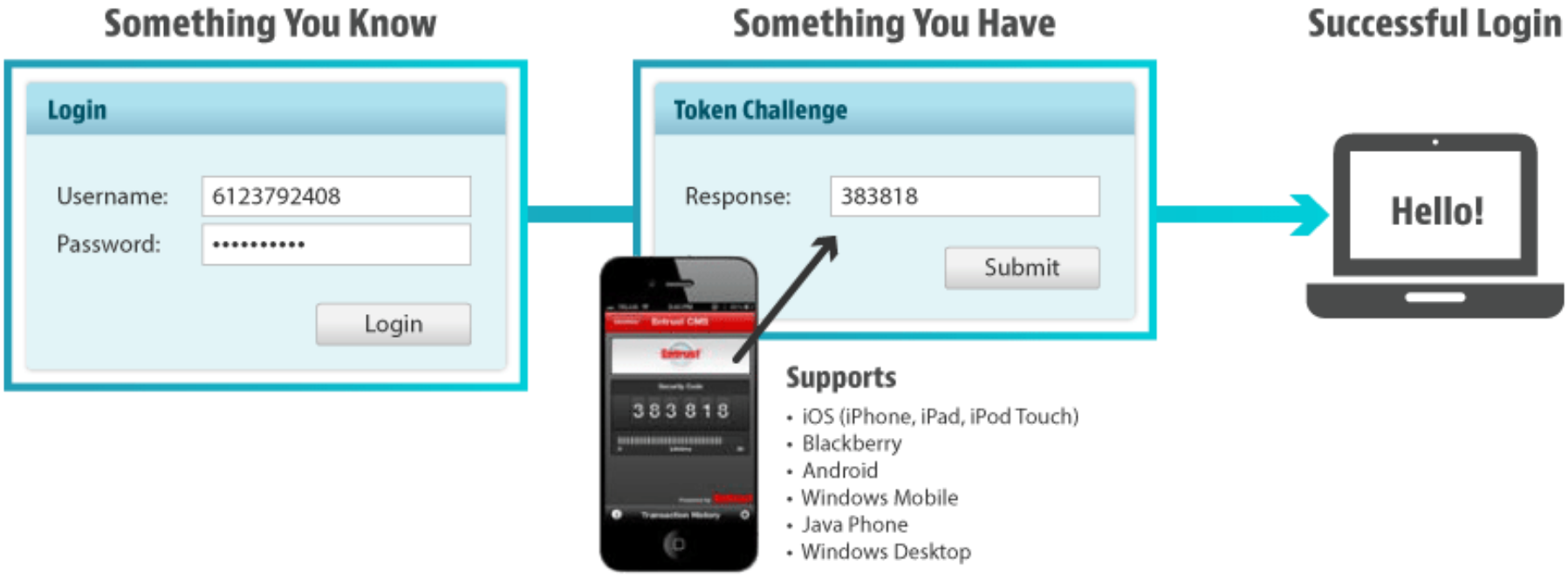


Soft Token Multifactor Authentication

- Soft token MFA went mainstream as businesses and their users shifted towards mobile devices.
- These methods popularized software-based One-Time-Passwords (OTP), and managed to replace a large segment of the hard tokens with PIN, PUSH or biometric based MFA.
- Some of the most popular authentication methods that leverage One Time Passwords (OTP) happen to rely on shared secrets - leaving users susceptible to **social engineering, mobile malware and man-in-the-middle (MitM) attacks**.

HYPR.com

Soft Token Multifactor Authentication



Courtesy of Entrust

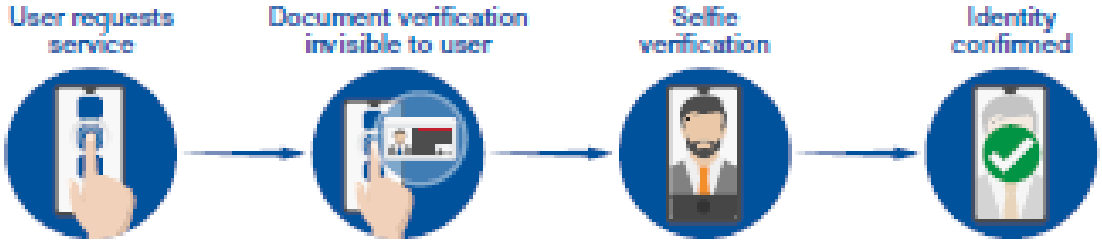
Password-less Multifactor Authentication

- Password-less authentication, is a form of multi-factor authentication that replaces the password with a secure alternative.
- This type of authentication requires two or more verification factors to sign in that are secured with a cryptographic key pair.
  - Private keys are generated by the user on their device and remain on-device at all times.
  - Biometric sensors such as Apple's Touch ID. Face ID and their Android & Windows counterparts are often used to unlock these credentials that are verified against an authentication server using public key cryptography.
  - User credentials are stored securely in the most trusted areas of smartphones and devices that are in the control of the user.

HYPR.com

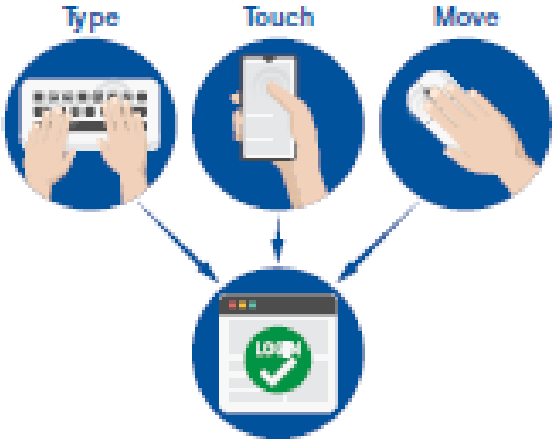
Password-less Multifactor Authentication

Facial Biometric Technology Authentication



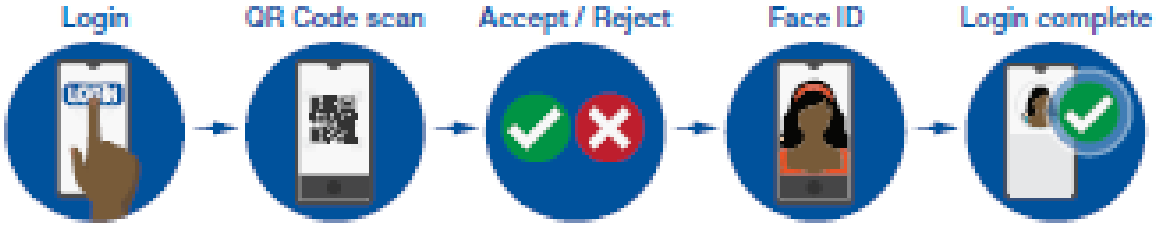
World Economic Forum

Behavioral Analysis



World Economic Forum

QR Code Authentication



World Economic Forum

Authentication Attack Matrix

	SHARED SECRETS		RELY ON SHARED SECRETS			NO
NIST 800-638 Threat Category	**Static Passwords**	**SMS 2FA**	**Phone-as-a-Token MFA**	**Hard Token 2FA**	**Smart Cards (PKI)**	**True Passwordless**
Security	**Low**	**Low**	**Medium**	**High**	**Very High**	**Very High**
Theft	•Usually Stored in one place •Users Write them down •Can Easily be Shared	•OTP Easily Stolen and Reused •Only as Secure as Mobile Device •Common SS7 Network Attacks	•Backups Are Often Made •Can Be Duplicated By Cloning Application Data	•OTP Difficult to Steal and Reuse •Not Bound to Particular User	•Card Can be Stolen and Reused •Only as Secure as PIN On Card •Attacks Are Highly Targeted	•Attacks Must Be Highly Targeted •Attackers Must Have Root Access to Mobile OS
Duplication	•Written Down and Duplicated •Backups Are Easily Made	•Backups Are Often Made •Duplicated By Cloning App Data	"•Backups Are Often Made •Can Be Duplicated By Cloning Application Data"	•Seed Backups Are Often Made (e.g. RSA Breach)	•Easily Duplicated •Highly Targeted	•Highly Targeted and Extremely Difficult Without Physical Access to Silicone on Chip
Eavesdropping	•Malware and MITM Commonly Used to Exploit	•Can Be Intercepted By Malware, MITM, and Key loggers	•OTP and MPC Can Be Intercepted By Malware and MITM	•MITM Commonly Used to Exploit	• PIN can Be Intercepted Between PC and Card Reader	• Extremely Difficult Without Physical Access to Silicone on Chip
Offline Cracking	•Hashed/Encrypted Passwords Can Be Cracked Offline	•Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	•Hashed or Encrypted Secrets Can Be Cracked Offline	•Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	•Very Difficult, Must Be Able to Decrypt and Exploit Chip	•Extremely Difficult Without Physical Access to Silicone on Chip

Authentication Attack Matrix Continued

Side Channel Attacks	**•Password Size and Complexity Can Be Established Through Side channel Analytics and Differential Power Analysis**	**•Can Be Sniffed or Intercepted By Other Apps or Malware**	**•Exposed to Credential Stuffing if Using Passwords as Alias •Can Be Sniffed or Intercepted By Other Apps or Malware**	**•Exposing Using Differential Power Analysis**	**•Possibly Exposed to Differential Power Analysis**	**•Possibly Exposed to Differential Power Analysis by a Very Sophisticated Attacker**
Phishing or Pharming	•Passwords Are The Primary Target of Phishing	•Targeted 2FA SMS 2FAPhishing (i.e. Modishka Tool)	•OTP Susceptible to Phishing •PUSH Attacks Require Social Engineering	•Targeted 2FAPhishing (i.e. Modishka Tool)	•Not Possible Since Each Authentication Request is an Unique Challenge-Response	•Not Vulnerable, as Each Authentication Request is a Unique Challenge/Response
Social Engineering	•Users and Admins Duped into Giving Password Through SE Attacks	•Attacker Retrieves MFA Code Directly from User	•Attacker Convinces User to Authenticate PUSH. Difficult Depending on Implementation	•Attacker Retrieves MFA Code Directly from User	•Extremely Difficult as User Does Not Utilize Shared Secrets	•Not Vulnerable, User Does Not Have a Shared Secret
Online Guessing	•Password Are Easy to Guess •People Reuse Password Through SE Attacks	•Difficult to Guess a TOTP	•Password-Based Alias Vulnerable to Credential Stuffing & Reuse Attack •Difficult if Based on TOTP Alias	•Difficult to Guess a TOTP	•Not Vulnerable to Guessing Due to PKI Architecture	•Not Vulnerable as Public/Private Key Pairs Are Used to Perform a Challenge/ Response Mechanism
Endpoint Compromise	•Vulnerable to Key loggers, Malware	•Vulnerable to Key loggers, Malware	•Vulnerable to Key loggers, Malware	•Vulnerable to Key loggers, Malware	•Not Vulnerable as Private Keys Always Remain On Smart Card	•Not Vulnerable as Keys Never Leave Hardware Backed Key Stone

Managed Service Providers MFA

- MFA holds particular importance when applied to Managed Service Providers (MSP). When a company purchases MSP licenses from a reseller or partners with an MSP, the partner is granted administrative privileges.
- This means that your service partners have full access to your organization's email, files, accounts and sites stored in the cloud. If one of your partners or partner's solutions are compromised, it would, in turn, mean that *you* are compromised.
    - Recently, a breach at PCM, the world's sixth-largest CSP, caused a breach at one of their client's firm when "the attackers stole administrative credentials that PCM uses to manage client accounts within Office 365".
    - Such attacks have further highlighted the vulnerabilities in the CSP world.
- Check on your third-party applications, and ensure that they support MFA. Assess that all your Cloud Service Providers (CSP) partners leverage policies such as the 'Require MFA for admins' baseline policy" to administrative users in the partner directory.

References

- Why Multi-Factor Authentication Is a Must
  - https://www.lbmc.com/blog/why-multi-factor-authentication-is-a-must/
- Multi-Factor Authentication Gains Traction In Healthcare
  - https://www.healthitoutcomes.com/doc/multi-factor-authentication-gains-traction-in-healthcare-0001
- Using SMS for Two-Factor Authentication
  - https://mgage.com/knowledge-share/case-studies/using-sms-two-factor-authentication/
- SS7 attack
  - https://whatis.techtarget.com/definition/SS7-attack
- Forgotten Your Password? Not Having One Will Make You Safer, Says World Economic Forum
  - https://www.weforum.org/press/2020/01/forgotten-your-password-not-having-one-will-make-you-safer-says-world-economic-forum
- One Simple Action you can take to prevent 99.9% of attacks on your accounts
  - https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
- SMS Two Factor Authentication (2FA)?
  - https://www.smsglobal.com/us/two-factor-authentication/
- NIST Denounces SMS 2FA - What are the Alternatives?
  - https://www.securityweek.com/nist-denounces-sms-2fa-what-are-alternatives

References

- What Are the Differences Between Hard Tokens and Soft Tokens?
  - https://www.cdw.com/content/cdw/en/articles/security/2019/04/09/hard-tokens-vs-soft-tokens.html
- Multi-Factor Authentication Gains Traction In Healthcare
  - https://www.healthitoutcomes.com/doc/multi-factor-authentication-gains-traction-in-healthcare-0001
- Multifactor Authentication Tools — SSL
  - https://www.entrust.com/multi-factor-authentication-tools/
- Planning a cloud-based Azure Multi-Factor Authentication deployment
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
- When to use an Azure Multi-Factor Authentication Provider
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider
- Why Multi-Factor Authentication Matters
  - https://cmitsolutions.com/blog/why-multi-factor-authentication-matters/
- Managing Multi-Factor Authentication
  - https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm
- Breach at Cloud Solution Provider PCM Inc.
  - https://krebsonsecurity.com/2019/06/breach-at-cloud-solution-provider-pcm-inc/
- Password-less Protection
  - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup

References

- Passwordless Authentication: The next breakthrough in secure digital transformation
  - http://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf
- The Evolution of Authentication
  - https://www.hypr.com/the-evolution-of-authentication-white-paper/

Questions

Upcoming Briefs

- Cybersecurity Implications for Telework in HPH
- Sector by Use of Third-Party Services

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**