Multifactor Authentication

February 9, 2023

TLP: CLEAR, ID# *202302091300*

Agenda

- Introduction
- Multifactor Authentication (MFA)
- SMS 2 Factor Authentication
- Hard Token Multifactor Authentication
- Soft Token Multifactor Authentication
- Password-less Multifactor Authentication
- 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 report released by the World Economic Forum finds that freeing ourselves of passwords will actually make us safer and businesses more efficient.
- Cybercrime 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)

Photo credit: 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.

Photo credit: 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.

Photo credit: 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.

Photo credit: 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.

Photo credit: mGage

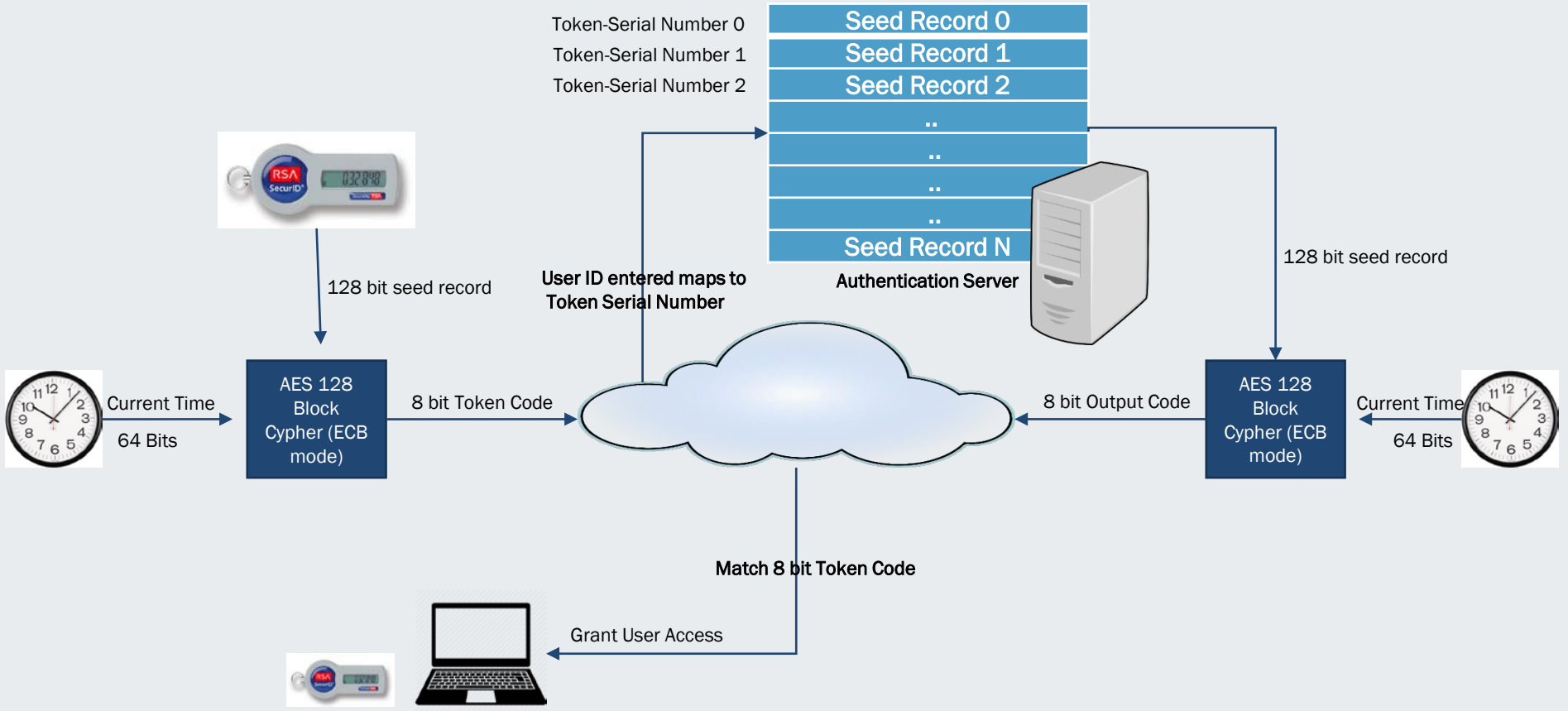
Hard Token Multifactor Authentication

- 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.

Photo credit: CDW

Photo credit: PIVKey

Hard Token Multifactor Authentication, cont.



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.**

Photo credit: HYPR.com

Soft Token Multifactor Authentication, cont.

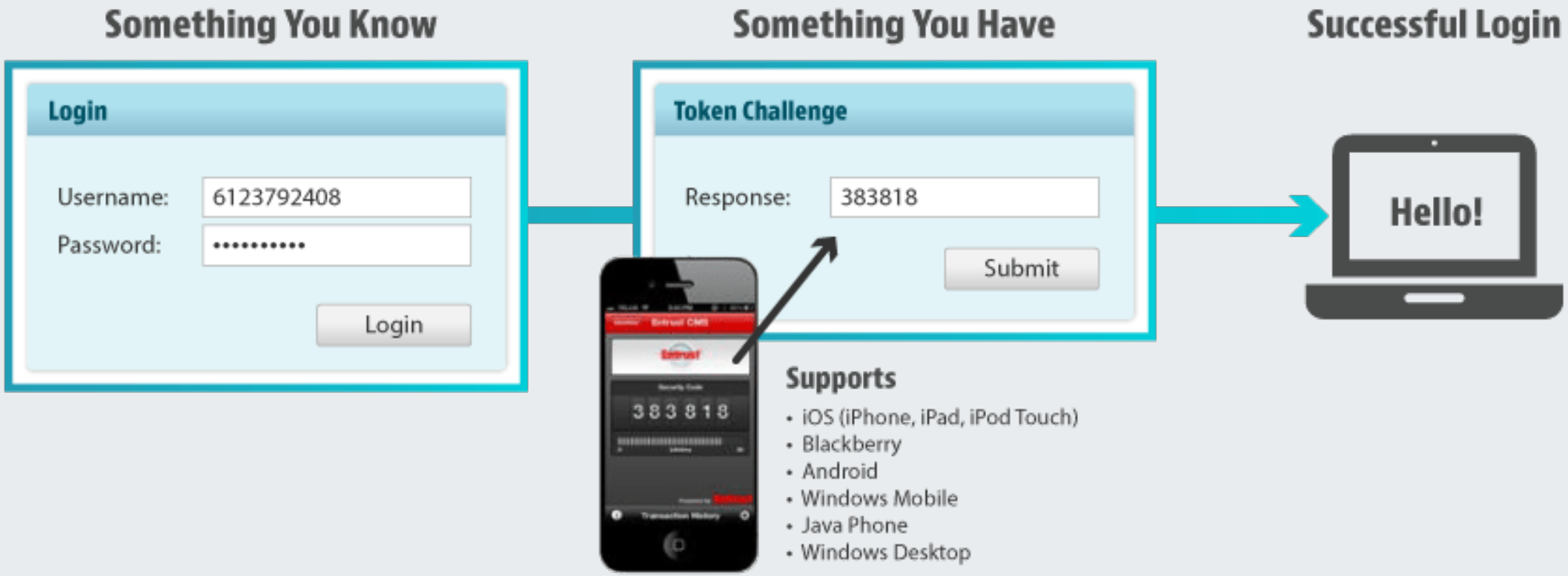


Photo credit: Entrust

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.

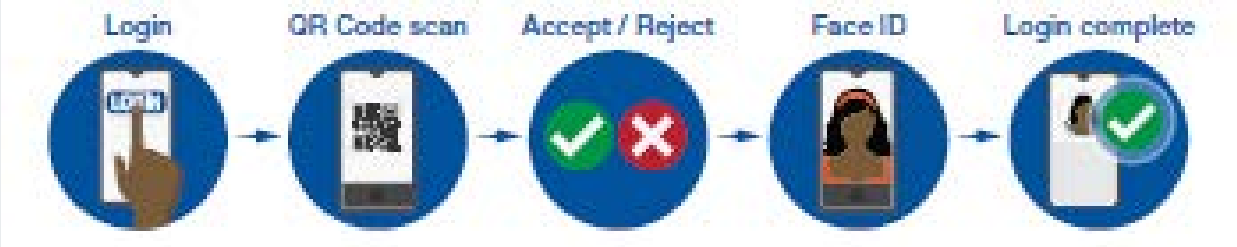
Photo credit: HYPR.com

Password-less Multifactor Authentication, cont.

Facial Biometric Technology Authentication

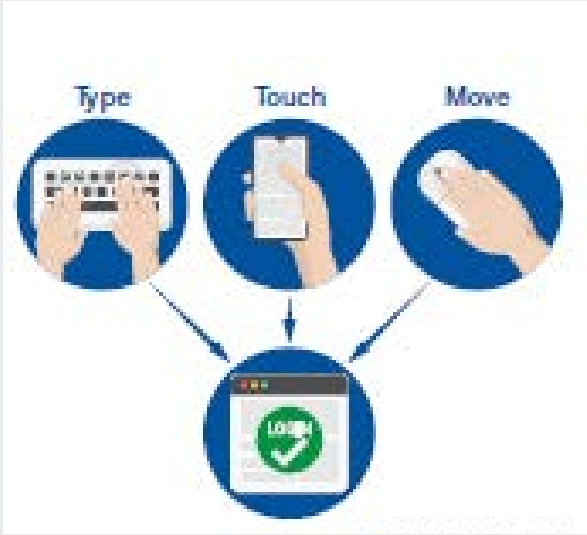
World Economic Forum

QR Code Authentication



World Economic Forum

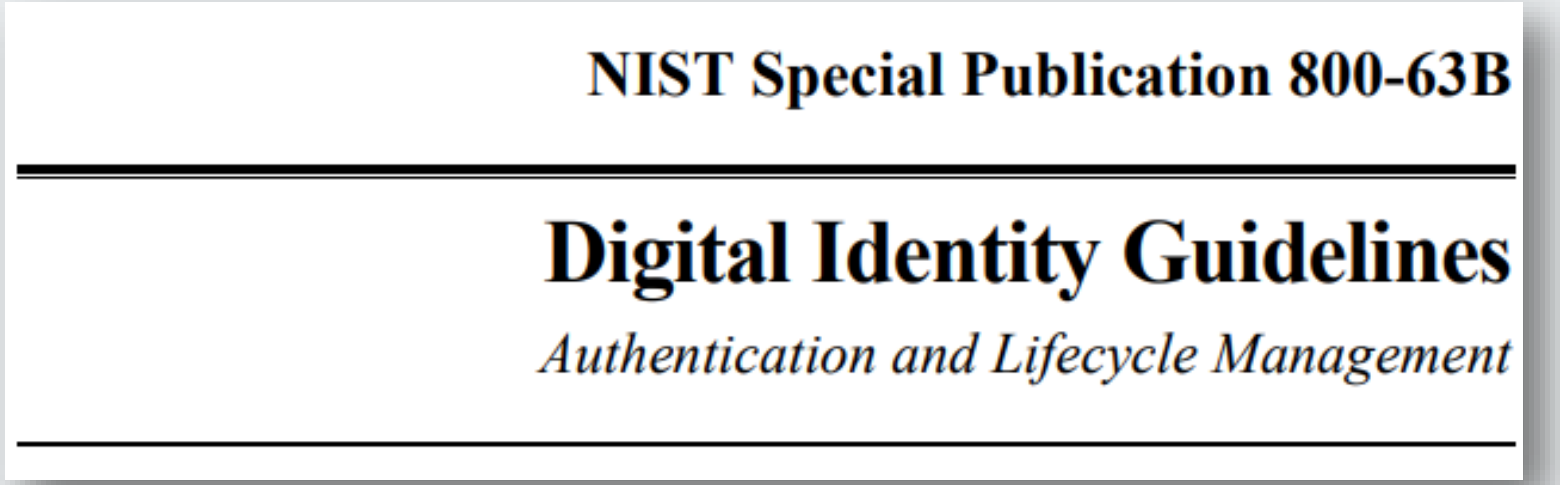
Behavioral Analysis



World Economic Forum

NIST SP 800-63B – Chapter 8

- Authenticator threats – post-authentication masquerading attacks
- Mitigation strategies and examples – theft, duplication, eavesdropping, offline cracking, side channel attacks, phishing/pharming, social engineering, online guessing, endpoint compromise, unauthorized binding.
- Authenticator recovery – a weak point
- Session hijacking attacks


NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

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.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Reference Materials

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/

References

- Password-less Protection
  - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup
- 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

FAQ

Upcoming Briefing

- **Today at 1pm EST – 2022 Year in Review**

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.

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

HHS.GOV/HC3

HC3@HHS.GOV