LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Utilizing Two Factor Authorization

TLP: WHITE, ID# 202109171300

About Health Sector Cybersecurity Coordination Center (HC3)

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector.

HC3 Products

Sector & 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.

White Papers

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

Threat Briefings & Webinar

Briefing presentations providing 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.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV or visit us at www.HHS.Gov/HC3.

What is Two-Factor Authentication?

Two Factor Authentication (2FA) is process in which a user must provide two different types of information to gain access to an account or system.

Types of Factors for 2FA

Knowledge tokens include PINs and security questions

Hardware tokens are physical objects, like bank cards or USB drives

Biometrics use **fingerprints and voices** for identification

Types of Two-Factor Authentication

- **Hardware tokens** - the oldest form of two-factor authentication. Physical devices act like electronic keys, generating a time-valid numeric code to access user accounts. This technique may also include a wireless keycard opening, smart cards, USB sticks.

- **SMS text-message and voice-based 2FA** - receiving either a text or voice message, which provides a code that must then be entered to access a site or account.

- **Software tokens** - one of the most popular 2FA forms. Uses a software-generated, time-based, one-time passcode (also called TOTP, or “soft-token”). A user needs to have a free 2FA app on their phone or desktop. During sign-in, the user first enters a username and password, and when prompted, enters the code shown on the app.

- **Push notifications -** websites and apps send the user a push notification when there is an authentication attempt. It is a passwordless authentication with no codes to enter, and no additional interaction required.

- **Biometric 2FA** - this technique includes verifying a person’s identity via fingerprints, retina patterns, facial recognition, ambient noise, pulse, typing patterns, and vocal prints.

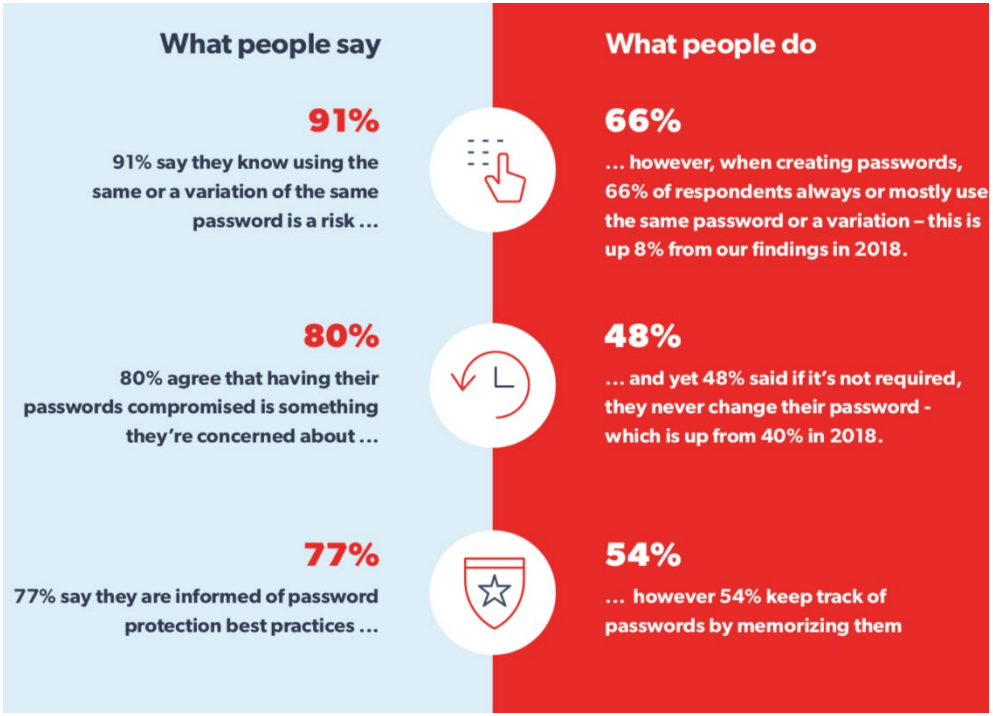
2FA vs Multifactor Authentication

(MFA) uses two or more factors of to verify the identity of the user while 2FA only uses 2 mechanisms.

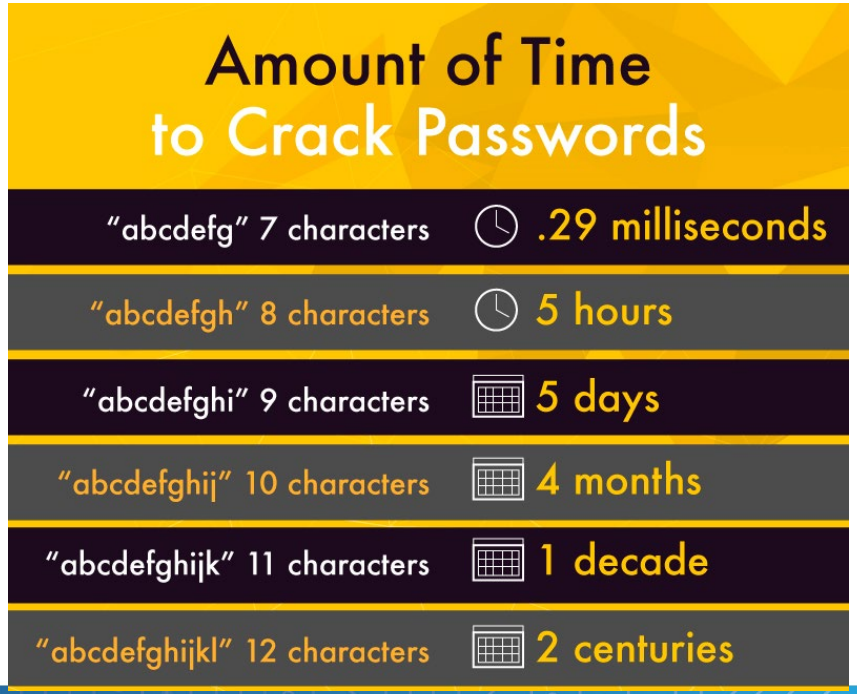
Why is 2FA Important?

- Most passwords used are weak and due to the advanced nature of hacking, can be cracked.
- The Office for Civil Rights identified weakened healthcare authentication measures were one of the biggest causes of data breaches in recent years.
- If a threat actor attempts to login into a user's device, having 2FA will alert the user so they can take additional steps to protect their account.

2FA Can Protect Against a Brute Force Attack



- A brute force attack is when a threat actor can exploit a system with a weak password.
- This type of attack uses trial-and-error to guess passwords, login information, encryption keys, or even locate a hidden web page.



Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.

Your 'friend' sends you a strange message.

Your emotions are heightened.

The request is urgent.

The offer feels too good to be true.

You're receiving help you didn't ask for.

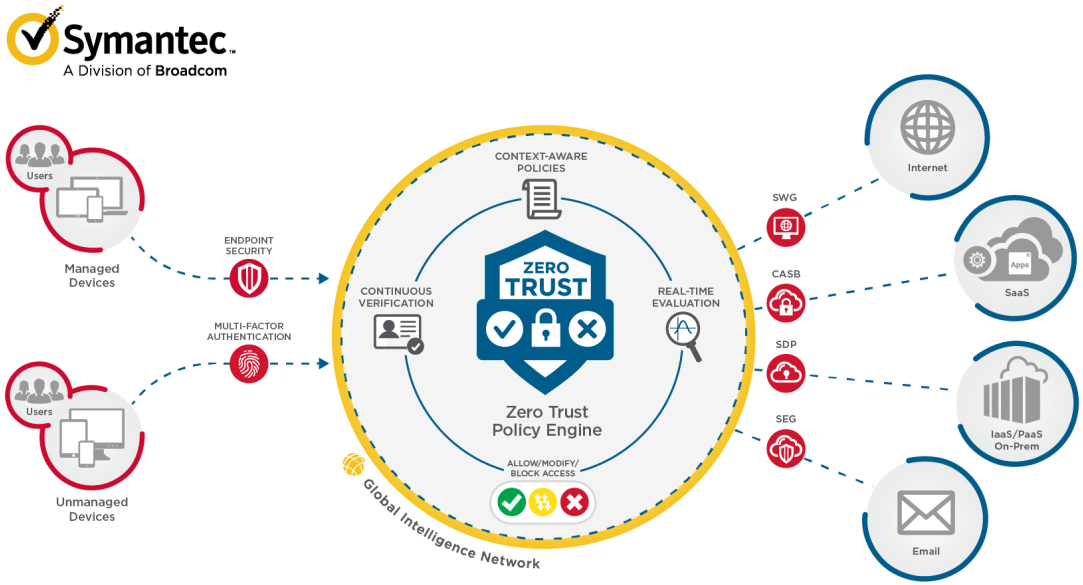
The sender can't prove their identity.

- A social engineering attack is when a threat actor manipulates or convinces their target to give up sensitive data or passwords
- Five traditional methods of this type of attack are: baiting, scareware, pretexting, phishing, and spear phishing
- An example of this type of attack: a threat actor will contact their target pretending to be an IT professional. Once they have earned the target's trust, the threat actor will ask the target for their login credentials

2FA Can Be Exploited

- SMS-based man-in-the-middle attacks is a type of session hijacking involving SMS one-time passcodes (OTP). Threat actors can compromise their target's smartphone by temporarily assigning their number to one under their control. Hackers can also gain access to a target's phone by convincing a customer service agent to reassign a phone.
- Supply chain attacks is cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. SolarWinds is a recent example of this kind of attack.
- Compromised MFA authentication workflow bypass is a denial-of-service vulnerability that allows any registered user to be authenticated by modifying users' one-time passwords, which will result in locking the targeted user out.
- Pass-the-cookie attack uses browser cookies and sites that store authentication details in the cookie. If a hacker can successfully extra this information, they can take over their target's account.

Zero Trust Will Require the Use of 2FA

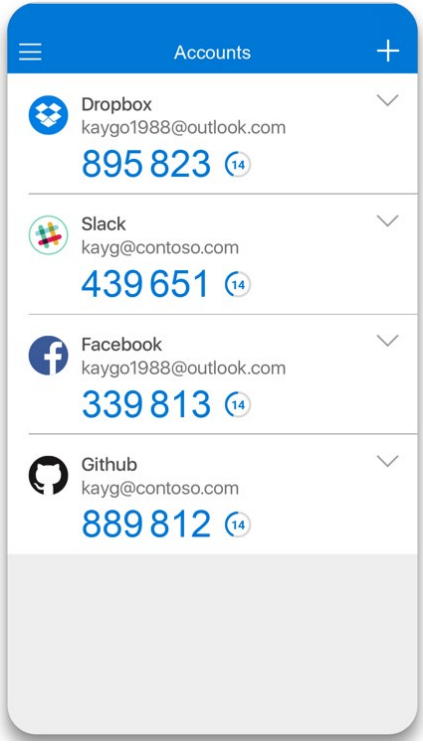


Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

- In May 2021, The Biden administration released a Cyber Executive Order that included the implementation of CISA's *Zero Trust Maturity Model* which is one of many roadmaps for agencies to reference as they transition towards a zero-trust architecture.

- 2FA is a type of MFA and it is the foundational element of the zero-trust security model. In order to protect sensitive data, verification of users trying to access that data must take place.

Where and How Can 2FA Be Used?



- 2FA is supported by many services, including Microsoft, Google, Facebook, Twitter, CapitalOne, Bank Of America, Chase, USAA, Fidelity, Amazon, and Apple.
- A directory of these services can be found here: https://2fa.directory/.
- Popular consumer grade 2FA tokens include applications such as Microsoft Authenticator, Google Authenticator, and Authy.
- Hardware tokens for consumers include YubiKey, Thetis FIDO2, and Google Titan.
- A guide on how to set up 2FA on popular services can be found here: How to set up two-factor authentication on your online accounts - The Verge.

Reference Materials

References

Reference Links:

- https://www.duq.edu/about/campus/computing-and-technology/safe-computing/duo-2fa
- https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon
- https://www.hipaajournal.com/considered-phi-hipaa/
- https://vimeo.com/187687586
- https://aldridge.com/how-to-join-a-microsoft-teams-meeting/
- https://us.norton.com/internetsecurity-how-to-importance-two-factor-authentication.html
- https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa
- https://us.norton.com/internetsecurity-how-to-importance-two-factor-authentication.html
- https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa
- https://www.fastcompany.com/90343839/gen-z-think-theyre-better-at-online-security-than-they-actually-are
- https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon
- https://www.hipaajournal.com/considered-phi-hipaa/
- https://www.cisa.gov/BadPractices
- https://healthitsecurity.com/resources/webcasts/applying-nist-800-207-principles-to-a-zero-trust-architecture-in-healthcare
- https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
- https://www.imperva.com/learn/application-security/social-engineering-attack/
- https://www.bankinfosecurity.com/webinars/anatomy-spear-phishing-attack-how-hackers-build-targeted-attacks-and-w-1968

References (Part II)

Reference Links:

- https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa
- https://healthitsecurity.com/resources/webcasts/applying-nist-800-207-principles-to-a-zero-trust-architecture-in-healthcare
- https://phoenixnap.com/blog/brute-force-attack
- https://www.forcepoint.com/cyber-edu/brute-force-attack
- https://www.csoonline.com/article/3620223/how-to-hack-2fa.html
- https://www.msp360.com/resources/blog/two-factor-authentication-solutions/
- https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa
- https://us.norton.com/internetsecurity-how-to-importance-two-factor-authentication.html
- https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/
- https://www.zdnet.com/article/cybersecurity-how-to-get-your-software-patching-strategy-right-and-keep-the-hackers-at-bay/
- https://www.zdnet.com/article/protect-yourself-how-to-choose-the-right-two-factor-authenticator-app/
- https://www.businesswire.com/news/home/20201210005650/en/Kaspersky-Report-Criminals-Targeted-Remote-Work-In-2020
- https://help.salesforce.com/s/articleView?id=000352937&type=1
- https://www.cpapracticeadvisor.com/firm-management/article/21210714/security-for-a-workfromhome-world
- https://healthitsecurity.com/features/can-multi-factor-authentication-help-healthcares-security-posture
- https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html#:~:text=An%20exploit%20is%20a%20program,by%20cybercriminals%20to%20deliver%20malware.

References (Part III)

Reference Links:

- https://www.cisa.gov/sites/default/files/publications/CISA%20MultiFactor%20Auth%20HDO_040721_508.pdf
- https://www.cisa.gov/executive-order-improving-nations-cybersecurity
- https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
- https://rublon.com/blog/mfa-2fa-difference/
- https://www.duq.edu/about/campus/computing-and-technology/safe-computing/duo-2fa
- https://doubleoctopus.com/security-wiki/authentication/multi-factor-authentication/
- https://cyberpulse.info/what-is-the-difference-between-2fa-and-mfa/
- https://www.cloudbric.com/blog/2017/07/two-factor-vs-multi-factor-authentication
- https://healthitsecurity.com/features/can-multi-factor-authentication-help-healthcares-security-posture
- https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
- https://www.cisa.gov/sites/default/files/publications/CISA%20MultiFactor%20Auth%20HDO_040721_508.pdf
- https://www.cisa.gov/executive-order-improving-nations-cybersecurity
- https://www.hipaajournal.com/july-2021-healthcare-data-breach-report/
- https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/
- https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/
- https://www.businesswire.com/news/home/20201210005650/en/Kaspersky-Report-Criminals-Targeted-Remote-Work-In-2020
- https://securelist.com/the-story-of-the-year-remote-work/99720/

Questions

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV