



# Privileged User Compromise

August 15, 2024





# Agenda

---

- What is a Privileged User?
- Privileged Access in Healthcare
- Why Privileged Accounts Pose a Risk
- Threats to Privileged Users and Accounts
- Other Common Threats to Privileged Users and Accounts
- Common Mistakes of Privileged Users
- Tips to Secure Privileged Accounts
- Conclusion
- Relevant HC3 Reports
- Resources
- References

## Slides Key:



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



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



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# What is a Privileged User?

---



# What is a Privileged User?

---

- Privileged users are humans, or system-related identities such as applications, programs or processes, which are authorized to access critical applications and sensitive data. (“Keys to the kingdom”)
- Organizations often have two-to-three times more privileged user accounts than individual employees.



Office of  
**Information Security**  
Securing One HHS



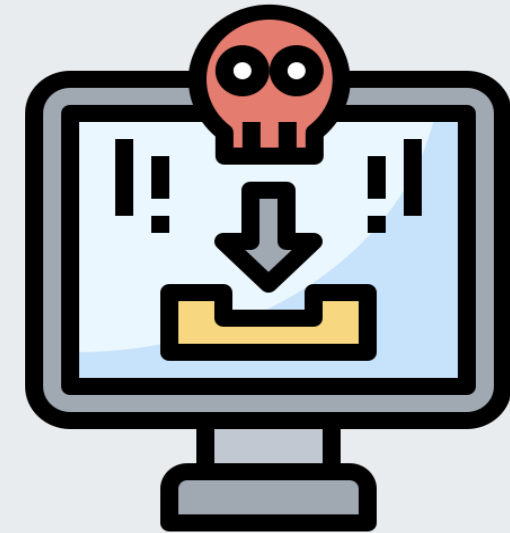
**Health Sector Cybersecurity  
Coordination Center**



# What is a Privileged User? (Continued)

---

- **Privileged Users/Accounts:**
  - Employees, customers, or subcontractors who have permission to access critical applications and sensitive data.
  - Attacks could lead to data breaches, financial losses, and reputational damage.
- **Critical Infrastructure:**
  - There are 16 critical infrastructure sectors (i.e., commercial facilities, dams, information technology, etc.).
  - Four sectors are “lifeline” sectors: Water/wastewater, communications, energy, and transportation.







# Privileged Users vs. Privileged Accounts

---

- **Privileged users** have unique identities. (Active Directory, Azure, etc.)
- Users can have multiple accounts for different situations.
- Examples:
  - Domain administrators, server administrators, or IT experts
  - Business users or developers
  - People who have access to SaaS applications
  - People who retain local administrative rights
  - Accounts with special permissions to run automated tasks



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Privileged Users vs. Privileged Accounts, continued

---

- **Privileged accounts** can be shared by multiple people.
- Can be used to access servers, perform upgrades, modify settings, and perform general maintenance.
- Human Privileged Account Examples:
  - Domain Admin accounts
  - Server Admin accounts
  - Root or Superuser accounts
  - System Admin accounts
  - Local Admin accounts
- Non-Human Privileged Account Examples:
  - Accounts that run applications, services, and scheduled tasks
  - Networking equipment accounts
  - Systems within DevOps toolchain



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Identity and Access Management vs. Privileged Access Management

---

- Identity and Access Management (IAM)
  - System to identify and authorize users across an organization.
- Privileged Access Management (PAM)
  - Strategy to focus on privileged accounts and systems.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# IAM is the New PAM

---

- Trend: Regular IAM solutions borrowing access controls from PAM platforms.
- PAM system enforces stricter set of policies than IAM system:
  - User behavior is carefully monitored and logged.
  - Passwords need to be stronger and may be rotated more often.
  - Multi-factor authentication is almost always required.
- Blurred lines between privileged users and ordinary users due to cloud computing.
  - Many practices and controls of PAM migrating over to IAM.
  - New IAM solutions rigorously monitor and log all user activity.
  - Enforce principle of least privilege.
- New Trends:
  - Just-in-time (JIT) access.
  - Zero standing privilege.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Privileged Access in Healthcare

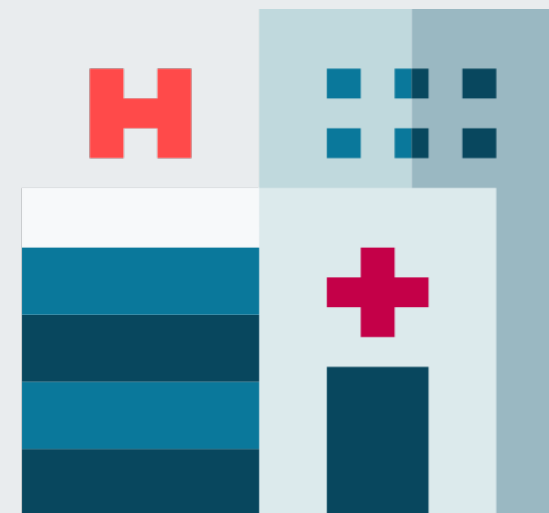
---



# Threat Landscape for Healthcare Industry

---

- HPH entities continue to be high-value targets for cybercriminals.
- The COVID-19 pandemic amplified the number of targeted attacks on healthcare provider network servers, e-mail systems, and devices.
- Larger attack surfaces leave provider and patient data at higher risk.
- Most healthcare organizations have moved patient records and data to networks and cloud environments.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Healthcare Data Security: Then

---

- Pre-1990s, patient medical records were kept on paper in a library.
- Records were updated by hand and transported manually to and from medical archives.
- There was no way to accurately monitor who had access to archives or looked at records, and there were few measures in place that prevented unauthorized access.
- Digitization of medical records began in 1991.
- New security and privacy concerns led to identity and access management security controls.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Healthcare Data Security: Now

---

- Almost all patient medical records are digitalized and housed within a database on a network.
- Privileged access control is the most important initiative to safeguard these records.
- Most modern access control systems are role-based.
- Each user is only given enough permissions to carry out their role.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Privileged Access in the HPH Sector

---

- Consider all human and non-human points of access:
  - People with administrator rights
  - Applications and medical devices
  - Third-party services
- Shared workstations and medical staff working under pressure may lead to weak authentication and shared credentials.
- HIPAA HITECH



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Regulation and Penalties

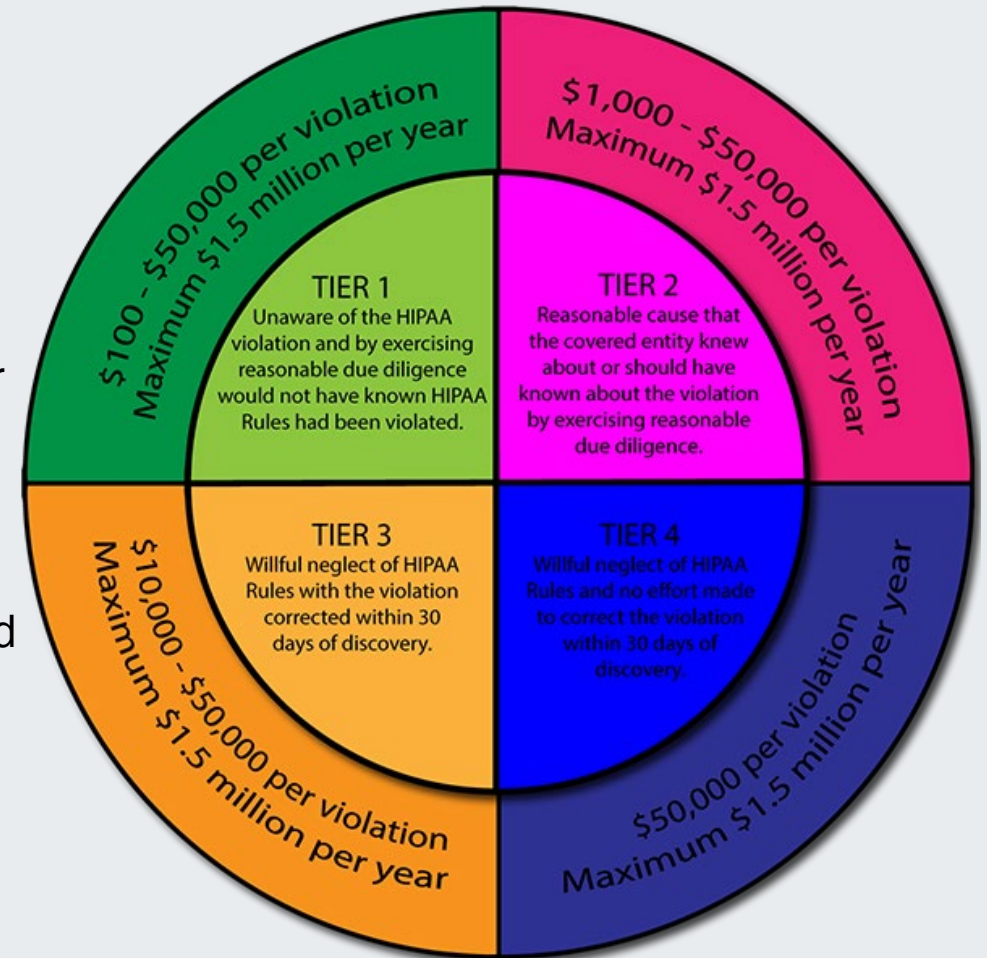
- IT organizations in the HPH sector face an increasingly tight regulatory environment.
- Strong privileged access security can make or break a healthcare organization.
- In 2023, a U.S. healthcare system agreed to pay \$5.5 million to the HHS to settle HIPAA HITECH violations
  - Failure to review access controls and examine audit logs.





# HIPAA Violation Penalties

- **Tier 1**
  - \$100-\$50,000 per violation
  - Unaware of the HIPAA violation, and by exercising reasonable due diligence, would not have known HIPAA rules had been violated.
- **Tier 2**
  - \$1,000-\$50,000 per violation
  - Reasonable cause that the covered entity knew about or should have known about the violation by exercising reasonable due diligence.
- **Tier 3**
  - \$10,000-\$50,000 per violation
  - Willful neglect of HIPAA rules, with the violation corrected within 30 days of discovery.
- **Tier 4**
  - \$50,000 per violation
  - Willful neglect of HIPAA rules, and no effort made to correct the violation within 30 days of discovery.



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center

HIPAA Violation Penalties. (Source: *The HIPAA Journal*)



# Why Privileged Accounts Pose a Risk

---



# Overview

---

- Multiple cybersecurity threats (compromised credentials, credential dumping, credential stuffing, phishing, insider threats, malware, etc.).
- Improper management of privileged users or accounts can lead to vulnerable sensitive data.
- Issues for admin and service accounts:
  - Often shared and used across many systems.
  - May use weak or default passwords.
  - Highly desirable hacking targets.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Overview, continued

---

- Nearly all cyber attacks involve privileged account compromise.
- Threat actors can remain undetected for weeks or months at a time.
- Threat actors exploit these privileged account weaknesses to:
  - Change system functionality
  - Disable access for some accounts
  - Elevate their existing permissions
  - Access systems and key administrative functions
  - Steal or poison data
  - Inject bad code or malware
  - Conceal or erase their activities



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

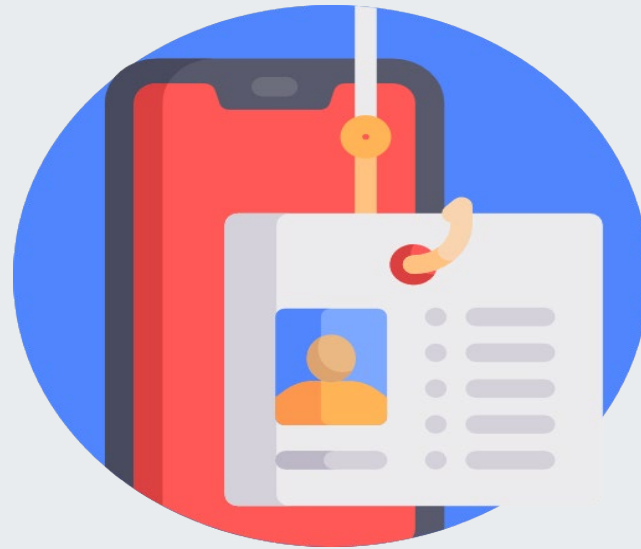




# How Privileged Account Passwords are Stolen

---

- Up to 80% of breaches result from stolen passwords.
- Stolen account credentials are hackers' most preferred method for privilege exploitation.
- Other common tactics include malware, social engineering, brute-force, etc.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# IBM's 2024 X-Force Threat Intelligence Index

- 71% increase in the volume of attacks using valid credentials.
- For the first time, abusing valid accounts became cybercriminals' most common entry point.
- Attackers find that obtaining valid credentials is easier.
- A large number of compromised credentials are already available and accessible on the dark web.

## X-Force Threat Intelligence Index 2024



[IBM Report](#) (Source: IBM)



# Threats to Privileged Users and Accounts

---



# Compromised Credentials

---

- **Definition:** A cyber attack in which threat actors use lists of compromised credentials to attempt to log into online accounts.
- **Goal:** To steal personal/financial information from a compromised account, or to take it over.
- **Issue:** Using the same password across multiple accounts.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# How Do Compromised Credential Attacks Work?

- Similar to brute-force attacks, but different.
- Credential stuffers already have a list of previously cracked and de-hashed passwords (i.e., data breaches, phishing, malware, keyloggers, etc.).
- No manual attempt to log in → Automation tool (brute-force checker) for obfuscation.
- Automation tools use leaked usernames and passwords to attempt logins on many different sites, apps, and services.
- Users that have same password across multiple accounts are easy targets.



Office of  
**Information Security**  
Securing One HHS



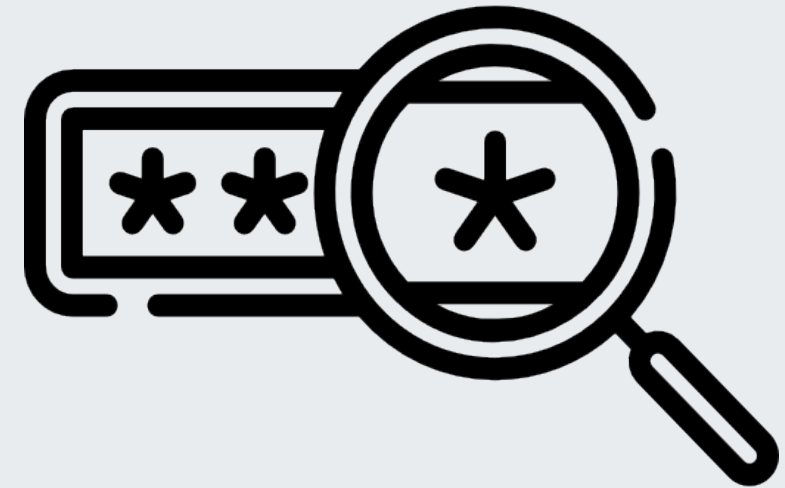
**Health Sector Cybersecurity  
Coordination Center**



# Risks of Compromised Credential Attacks

---

- Lock you out of your account
- Steal your personal/financial information
- Deface your account/page
- Modify your information
- Make purchases in your name
- Shut down your account
- Sell your credentials on the dark web
- Send messages in your name
- And more...





# Credential Dumping Overview

---

- **Definition:** Popular technique where an attacker scours a compromised computer for credentials in order to move laterally.
- **Goal:** To carry out further attacks on an already compromised computer.
- **Issue:** Software and operating systems sometimes reduce the number of times a user is required to enter their password.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Credential Dumping Tools

- Gaining low-level access to a computer can allow attackers to extract credentials.
- Mimikatz is the most popular credential dumping tool for penetration testers and malicious actors alike.
- Originally began as tool to highlight flaws in Microsoft Windows Local Security Authority Subsystem Service (LSASS).
- Other tools include gsecdump, creddump, and PWDumpX.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Credential Reuse Attack

---

- **Definition:** A cyberattack where an attacker uses stolen login credentials from one service to try to access accounts on other services.
- **Also Known As:** Credential Stuffing
- **Goal:** To gain unauthorized access to user accounts and data.
- **Issue:** Reuse of passwords across more than one application.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

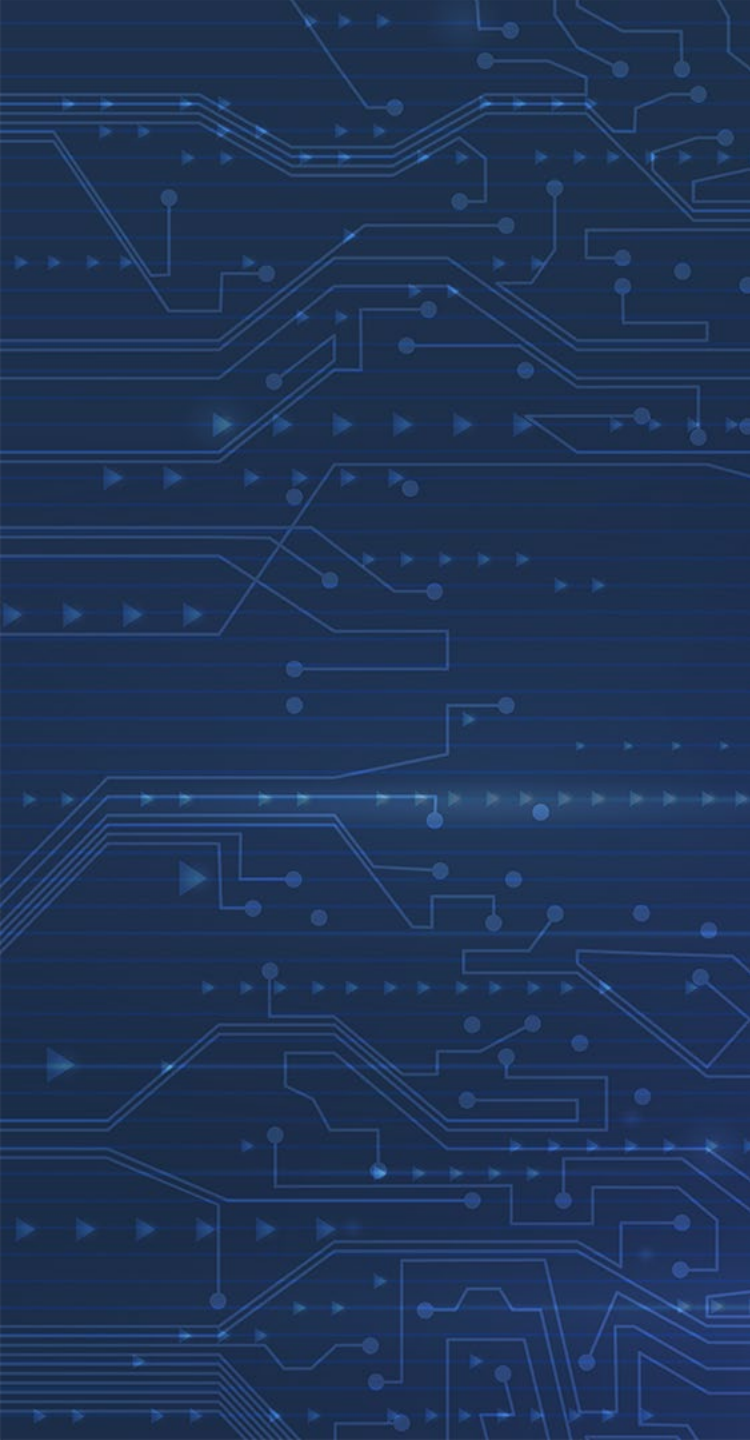


# Credential Reuse Attack Case Study

- In 2023, genetic testing firm data from millions of customers was stolen in a credential stuffing attack.
- Stolen data included names, profile photos, gender, date of birth, genetic ancestry results, and geographical location.
- “...may have been gathered by a threat actor from data leaked during incidents involving other online platforms where users recycled login credentials.”



Source: FIU News



# **Other Common Threats to Privileged Users and Accounts**

---



# Phishing

---

- The cybercriminal aims to convince their target to disclose sensitive information.
- In 2023, an average of 1.99 healthcare data breaches of 500 or more records were reported each day, and an average of 364,571 healthcare records were breached every day. ([HIPAA Journal](#))
- Threat actors target privileged users to gain access to an organization's privileged accounts, with multiple phishing tactics utilized.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Top Types of Phishing for 2024

---

- **E-mail Phishing:** The attacker sends an email that looks legitimate but is designed to trick the recipient into entering information in a reply or on a website, which the hacker uses to steal or sell their data.
- **Whaling:** A highly targeted phishing attack aimed at senior executives. Whaling often encourages victims to perform a secondary action, such as initiating a wire transfer of funds.
- **Vishing (Voice Phishing):** When someone uses a phone call to try to steal information. The attacker may pretend to be a trusted friend, a relative, or a representative of some kind.
- **Clone Phishing:** Involves a hacker making an identical copy of a message the recipient already received; they may include an additional message like “Resending this!” with a malicious link in the email.
- **Pharming:** The victim gets malicious code installed on their computer, and this code then sends the victim to a fake website designed to gather their login credentials.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Top Types of Phishing for 2024, continued

---

- **HTTPS Phishing:** This attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.
- **Pop-Up Phishing:** Often uses a pop-up about a problem with your computer's security, or some other issue, to trick you into clicking. You are then directed to download a file, which ends up being malware, or to call what is allegedly a support center.
- **Smishing:** Phishing through some form of text message or SMS.
- **Evil Twin Phishing:** In this attack, the hacker sets up a false Wi-Fi network that looks real. If someone logs into it and enters sensitive details, the hacker captures their info.
- **Quishing:** A cybersecurity threat in which attackers use QR codes to redirect victims to malicious websites or prompts them to download harmful content.
- **Spear Phishing:** Involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often gathers information about the person before starting the attack, such as their name, position, and contact details.





# Insider Threats

---

- A person within an organization, or a contractor, who had access to assets or inside information concerning the organization's security practices, data, and computer systems, and could negatively impact that organization.
- When privileged accounts are not managed properly, privileged users may misuse their privileges, which presents a serious risk to any organization.
- Types of Insider Threats:
  - Malicious insiders
  - Inside agents
  - Disgruntled employees
  - Negligent workers
  - Third parties



Office of  
**Information Security**  
Securing One HHS

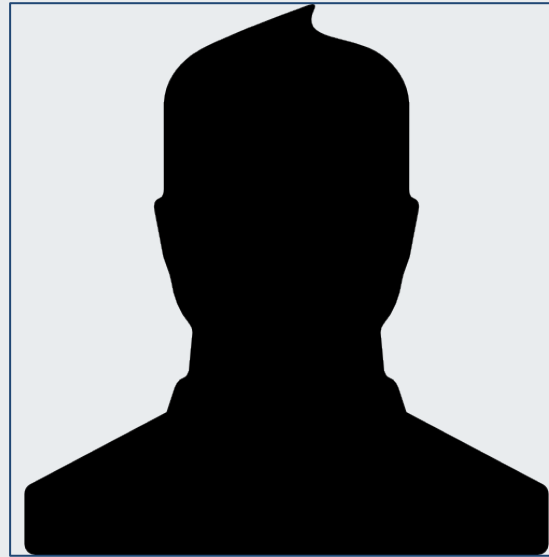


**Health Sector Cybersecurity  
Coordination Center**

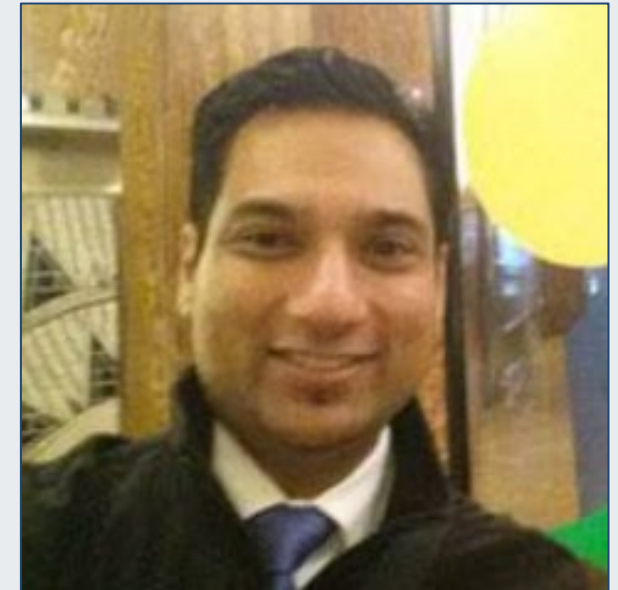


# Insider Threat Case Studies

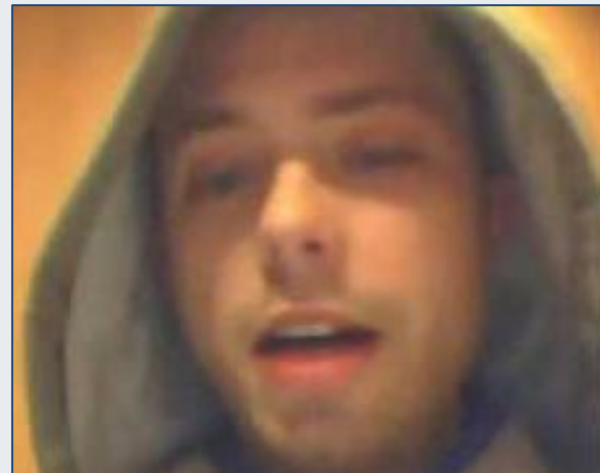
- In 2022, Aaron Lockner, disgruntled former IT specialist at a Chicago healthcare organization, hacked into a server, impacting the care of multiple patients.
- In 2018, Vikas Singla, the chief operating officer of a security firm for two hospitals and a medical center, helped unknown attackers access two hospitals' phone systems and printers.
- In 2011, Jesse William McGraw, a former security guard, used malware on dozens of machines to infiltrate a Texas hospital's network.



Unknown Photo for Aaron Lockner.  
(Source: Freepik)



Vikas Singla (Source: LinkedIn)

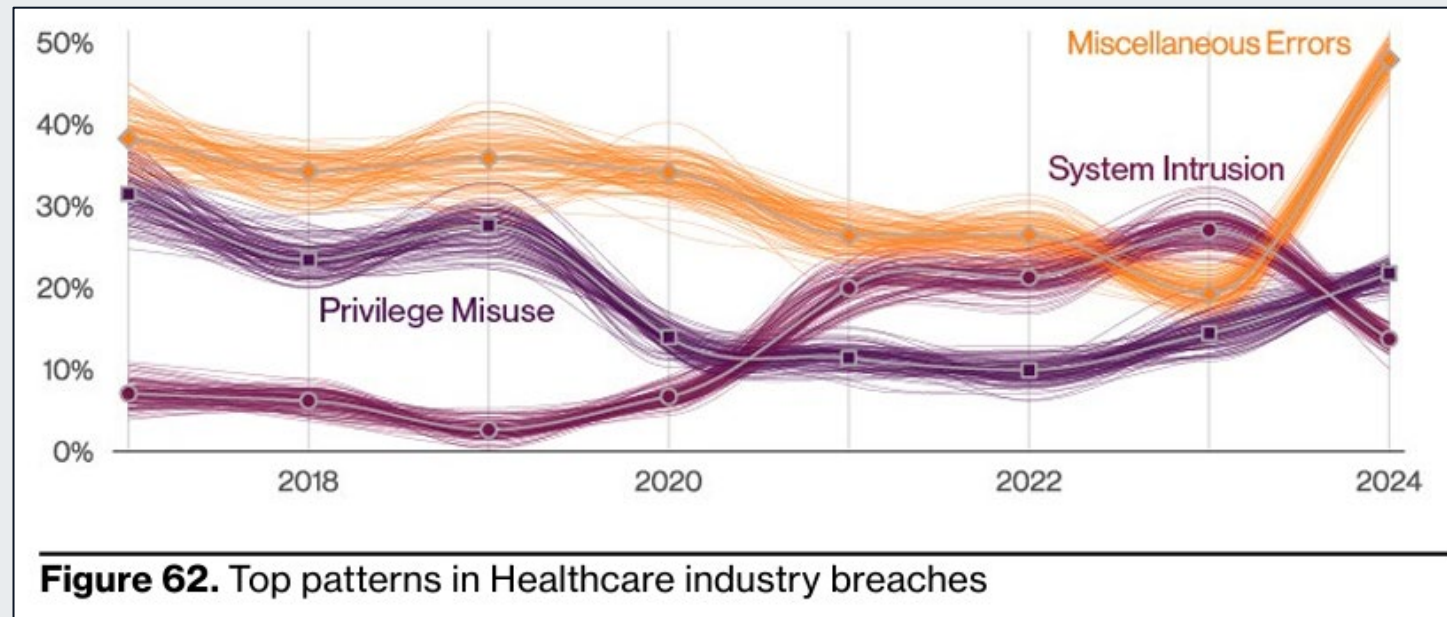


Jesse William McGraw (Source: YouTube)



# Insider Threats in Healthcare

- While most companies invest more money on insider threats with malicious intent, negligent insider threats are more common. ([2022 HC3 Insider Threats in Healthcare](#))
- Employees in the healthcare industry are 2.5 times more likely to make an error than to maliciously misuse their access. ([Verizon's 2024 Data Breach Investigations Report](#))



2024 Data Breach Investigations Report (Source: Verizon)



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



# Insider Threats in Healthcare, continued

---

- Third-party vendors may not have the same cybersecurity measures as healthcare organizations.
- HIPAA requirement: All HPH entities maintain business associate agreements (BAA) with third-party vendors that have access to protected health information.
- Third-party vendor breaches continue to overwhelm the healthcare industry. (2022 Health IT Security Report)



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Malware

---

- Short for 'malicious software'; any software or code designed to infiltrate/damage a computer system.
- Common types include viruses, worms, trojans, ransomware, adware, spyware, rootkits, keyloggers, fileless malware, cryptojacking, and hybrid malware.
- This type of threat is decreasing in favor of more effective, faster, and cost-effective means.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Brute Force

---

- A type of cyberattack that uses trial and error methods to guess login credentials.
- Least efficient method for trying to hack a password.
- Most successful in organizations without password management.
- Password managers help IT administrators enforce strong passwords and multi-factor authentication (MFA).
- Without a password management solution, passwords for privileged accounts could be hacked.





# Brute Force Case Study

- In 2024, the Russian threat group Midnight Blizzard (APT29) hacked a large American technology company using password spraying (brute force technique).
- The compromised account had unusual privileges, or hackers escalated them.
- The attack lasted upwards of seven weeks.
- Exfiltration of e-mails and documents from senior leadership and employees in the cybersecurity and legal team divisions.



Midnight Blizzard (Source: CrowdStrike)



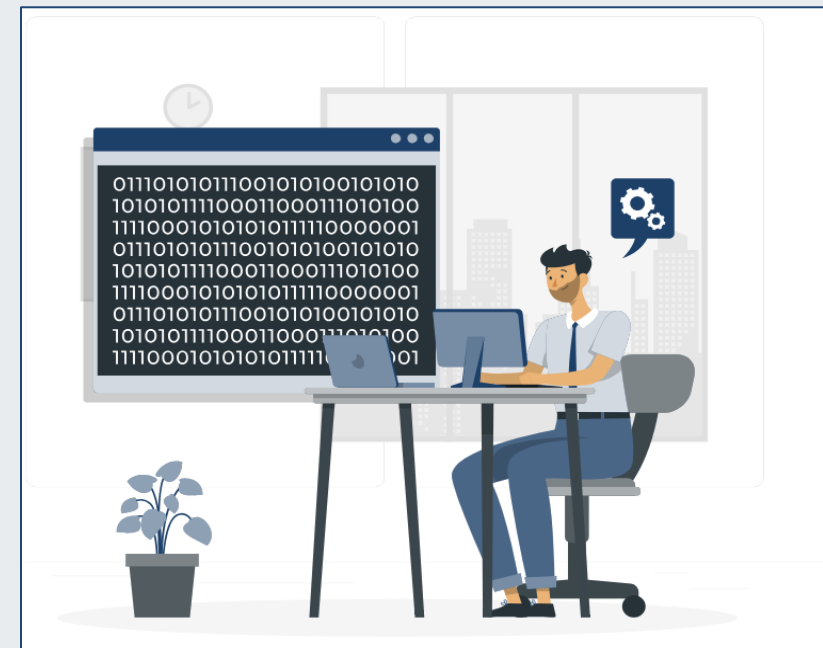
# Common Mistakes of Privileged Users

---



# Mismanaging Passwords

- Five most common password management mistakes:
  - Using default credentials
  - Using weak passwords
  - Using the same password for multiple accounts
  - Storing passwords in plain text
  - Using non-expiring passwords



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

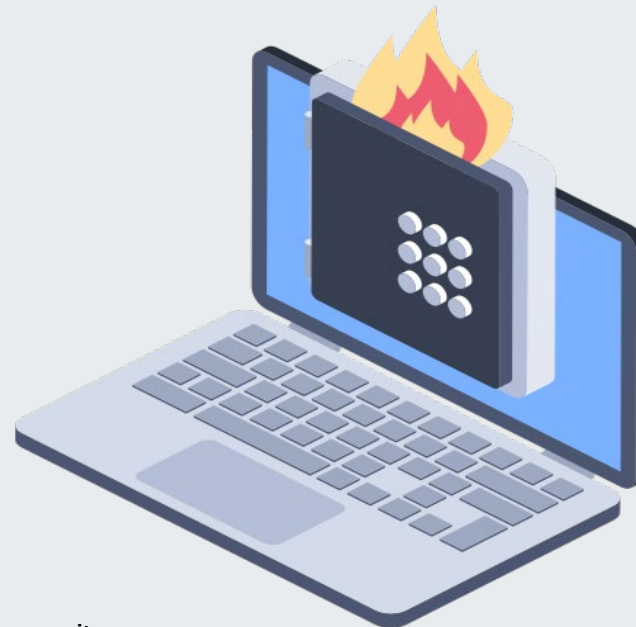




# Disabling or Not Using MFA

---

- Multi-factor authentication is the cybersecurity gold standard.
- Cybercriminals can steal or guess a password but cannot trick an MFA mechanism easily.
- Privileged users sometimes disable MFA technology, often at their own risk.
- Without MFA, sensitive data loses a crucial layer of protection.



Office of  
**Information Security**  
Securing One HHS



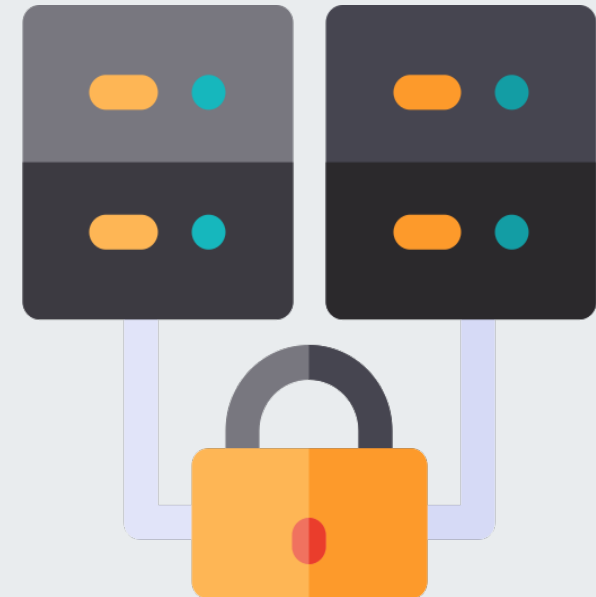
**Health Sector Cybersecurity  
Coordination Center**



# Sharing Privileges with Others

---

- Privileges should be granted only to those who need them.
- Administrator accounts are often shared due to the costs of creating additional accounts.
- Visibility is essential.
- Culpability during data compromise difficult.
- Secondary authentication is crucial.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

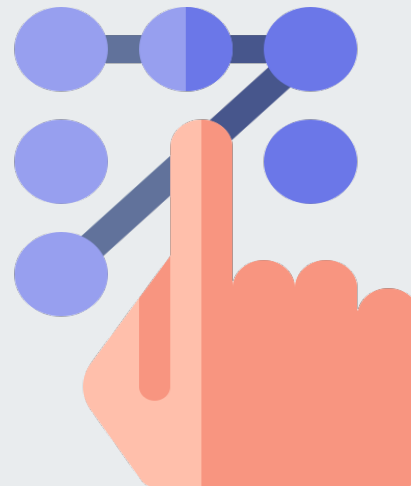




# Using Admin Accounts Excessively

---

- Using privileged accounts excessively increases an organization's vulnerability.
- The best practice is to never use privileged accounts to perform day-to-day tasks; there is potential for privileged users to ignore this.
- Deploy password management tool recommendations.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Ignoring Cybersecurity Policies

---

- Why people do not follow cybersecurity policies:
  - Ignorance
  - Negligence
  - Inconvenience
  - Sabotage



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Tips to Secure Privileged Accounts

---



# Why Secure Privileged Accounts Matter

---

- Stolen credentials are the heart of most attacks and breaches.
- Once compromised, threat actors can see and do anything.
- The higher the privileges, the more valuable they are.
- Privileged users are not limited to IT and security staff.
  - Executives
  - Employees/Contractors



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Tips to Secure Privileged Accounts

---

- Identify and track privileged accounts.
- Downgrade accounts where possible.
- Not all service accounts need privileged access.
- Do not use administrator account as a shared account.
- Remove stale privileged accounts.
- Change default passwords and enforce strict password rules.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Benefits of Privileged Access Management for the Healthcare Industry

---

- Reducing the Attack Surface
- Operating by the Principle of Least Privilege (PoLP)
- Reduced Insider Threats
- Pragmatic Application Control
- Remote Access
- Monitoring and Management of Privileged Sessions
- Achieve and Prove Compliance
- Help Satisfy Cyber Insurance Requirements



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered	Domain Policy Modification (2)	Multi-Factor Authentication	Debugger Evasion		Data from Information Repositories (3)	Ingress Tool Transfer	
Search Victim-Owned		Shared Modules	Shared Modules			Execution Guardrails (1)		Device Driver Discovery				
						Exploitation for Defense Evasion		Domain Trust				
						File and Directory						

Source: MITRE ATT&CK



Office of Information Security  
Securing One HHS



Health Sector Cybersecurity Coordination Center



# MITRE ATT&CK Techniques

---

- Privileged Account Management (Mitigation)
  - ID: [M1026](#)
- OS Credential Dumping (Technique)
  - ID: [T1003](#)
- Valid Accounts (Technique)
  - ID: [T1078](#)
- Account Manipulation (Technique)
  - ID: [T1098](#)
- Exploit Public-Facing Application (Technique)
  - ID: [T1190](#)
- Firmware Corruption (Technique)
  - ID: [T1495](#)
- Abuse Elevation Control Mechanism (Technique)
  - ID: [T1548](#)
- Remote Service Session Hijacking (Technique)
  - ID: [T1563](#)
- Forge Web Credentials (Technique)
  - ID: [T1606](#)
- Privilege Escalation (Technique)
  - ID: [TA0004](#)





# Conclusion

---



# Conclusion

---

- Differences between privileged users and accounts and mitigation systems
- Consequences to the HPH sector from privileged user compromise
- Types of threats
- Common mistakes
- Tips to secure privileged accounts



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Relevant HC3 Reports

---





# Relevant HC3 Reports

---

- Analyst Note – [Healthcare Sector DDoS Guide](#) (February 13, 2023)
- Threat Briefing – [Business Email Compromise \(BEC\) & Healthcare](#) (May 16, 2024)
- Threat Briefing – [Cybersecurity Incident Response Plans](#) (October 12, 2023)
- Threat Briefing – [Data Exfiltration Trends in Healthcare](#) (March 9, 2023)
- Threat Briefing – [The Impact of Social Engineering on Healthcare](#) (August 18, 2022)
- Threat Briefing – [Social Engineering Attacks Targeting the HPH Sector](#) (April 11, 2024)
- Threat Briefing – [Strengthening Cyber Posture in the Health Sector](#) (June 16, 2022)



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**





# Resources

---



# 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 Current Activity](#)
- [CISA Free Cybersecurity Tools](#)
- [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](#)



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Reference Materials



# References

---

- “6 Realities for Effectively Managing Privileged Accounts.” Fortra. Accessed June 19, 2024.  
<https://www.coresecurity.com/blog/6-realities-for-effectively-managing-privileged-accounts>
- “2024 Data Breach Investigations Report.” Verizon. 2024.  
<https://www.verizon.com/business/resources/T6bc/reports/2024-dbir-data-breach-investigations-report.pdf>
- “The Added Dangers Privileged Accounts Pose to Your Active Directory.” The Hacker News. May 26, 2022.  
<https://thehackernews.com/2022/05/the-added-dangers-privileged-accounts.html>
- Alder, Steve. “Healthcare Data Breach Statistics.” The HIPAA Journal. June 20, 2024.  
<https://www.hipaajournal.com/healthcare-data-breach-statistics/>
- Alder, Steve. “HHS Confirms When HIPAA Fines Can be Issued to Business Associates.” The HIPAA Journal. May 27, 2019.  
<https://www.hipaajournal.com/hhs-confirms-when-hipaa-fines-can-be-issued-to-business-associates/>
- Carson, Joseph. “Then and Now: Securing Privileged Access Within Healthcare Orgs.” Threat Post. June 3, 2021.  
<https://threatpost.com/securing-privileged-access-healthcare/166477/>
- Cheng, Jennifer. “Unmasking cyber criminals: The power of privileged identities.” IT Brief Australia. September 25, 2023.  
<https://itbrief.com.au/story/unmasking-cyber-criminals-the-power-of-privileged-identities>



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



- “The Critical Role of Identity Security in Healthcare Operations & Health Data Security.” BeyondTrust. March 14, 2024. <https://www.beyondtrust.com/blog/entry/identity-security-in-healthcare>
- Hoffman, Barbara. “A guide to managing and securing privileged users.” Delinea. Accessed June 19, 2024. <https://delinea.com/blog/privileged-users>
- “Identity Management and Privileged Access in Healthcare.” Bravura Security. Accessed July 10, 2024. <https://www.bravurasecurity.com/resources/documents/privileged-access-in-the-healthcare-market>
- Jaffe, Mark. “Privileged access: Securing cybercrime’s most coveted target.” Cyber Magazine. March 26, 2023. <https://cybermagazine.com/articles/privileged-access-securing-cybercrimes-most-coveted-target>
- “Key Lessons from Microsoft’s Password Spray Hack: Secure Every Account.” The Hacker News. March 25, 2024. <https://thehackernews.com/2024/03/key-lesson-from-microsofts-password.html>
- Khachatryan, Ani. “Top 5 Inadvertent Mistakes of Privileged Users and How to Prevent Them.” Ekran. February 8, 2023. <https://www.ekransystem.com/en/blog/inadvertent-privileged-user-mistakes>
- Linden, Imry. “Nearly All Damaging Cyber Attacks Involve Privileged Account Compromise.” Cybercrime Magazine. January 2, 2019. <https://cybersecurityventures.com/reduce-risks-with-a-privileged-access-security-hygiene-check/>







- Murphy, Bryan. “The Role of Privileged Access in Healthcare Security and Compliance.” CyberArk. October 29, 2018. <https://www.cyberark.com/resources/healthcare/the-role-of-privileged-access-in-healthcare-security-and-compliance>
- “Privileged Account Management (PAM).” Identity Management Institute. Accessed June 19, 2024. <https://identitymanagementinstitute.org/privileged-account-management-pam/>
- “Six Tips for Securing Privileged Accounts in the Enterprise.” CrowdStrike. January 12, 2021. <https://www.crowdstrike.com/blog/six-tips-for-securing-privileged-enterprise-accounts/>
- “Threat Report: Analyzing Identity Risks (AIR) Research Report.” ProofPoint. Accessed June 21, 2024. <https://www.proofpoint.com/us/resources/threat-reports/analyzing-identity-risks-air-research-report>
- Trevino, Aranza. “Types of Threats Privileged Accounts Face.” Keeper Security. June 5, 2023. <https://www.keepersecurity.com/blog/2023/06/05/types-of-threats-privileged-accounts-face/>
- Wang, Richard. “Privileged Account Management and Identity Access Management: Same family, different strengths.” Delinea. Accessed July 11, 2024. [https://delinea.com/blog/privileged-account-management-and-identity-access-management-same-family-different-strengths#:~:text=Identity%20and%20access%20management%20\(IAM,on%20privileged%20accounts%20and%20systems.](https://delinea.com/blog/privileged-account-management-and-identity-access-management-same-family-different-strengths#:~:text=Identity%20and%20access%20management%20(IAM,on%20privileged%20accounts%20and%20systems.)







Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Questions



# FAQ

---

## Upcoming Briefing

- September 19 – Healthcare Technology Security

## 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](mailto: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.



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



# 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.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# 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**





Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center

# Contacts



[WWW.HHS.GOV/HC3](http://WWW.HHS.GOV/HC3)



[HC3@HHS.GOV](mailto:HC3@HHS.GOV)