The Impact of Social Engineering on Healthcare

August 18, 2022

Agenda

- What is Social Engineering?

- Phases of a Social Engineering Attack

- Types of Social Engineering

- Personality Traits of a Social Engineer and
  Social Engineering Behaviors/Scenarios

- Impact of Social Engineering and Data Breaches

- Steps to Protect Your Organization

- Resources

Slides Key:

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

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

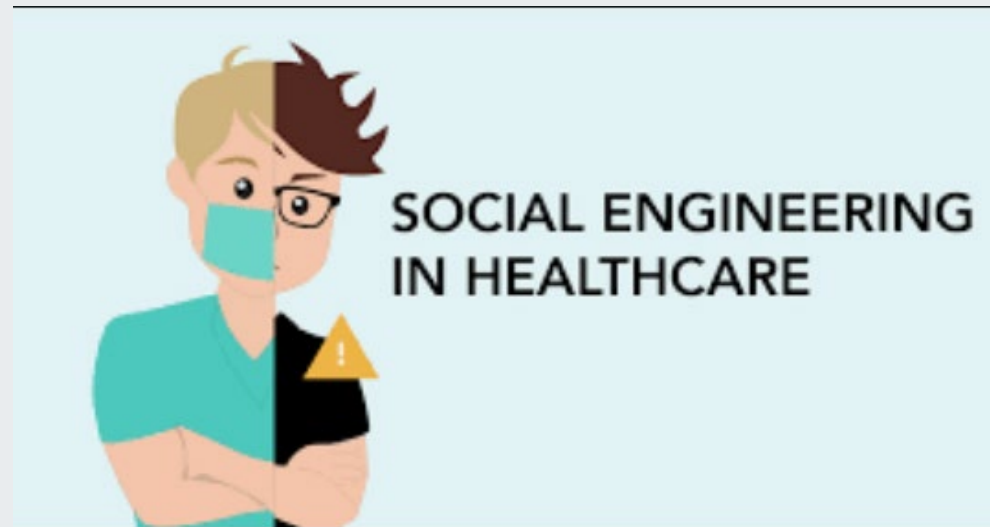Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

What is Social Engineering?

Social engineering is the manipulation of human psychology for one's own gain. A social engineer can manipulate staff members into giving access to their computers, routers, or Wi-Fi; the social engineer can then steal Protected Health Information (PHI), Personal Identifiable Information (PII), and/or install malware posing a significant threat to the Health sector.
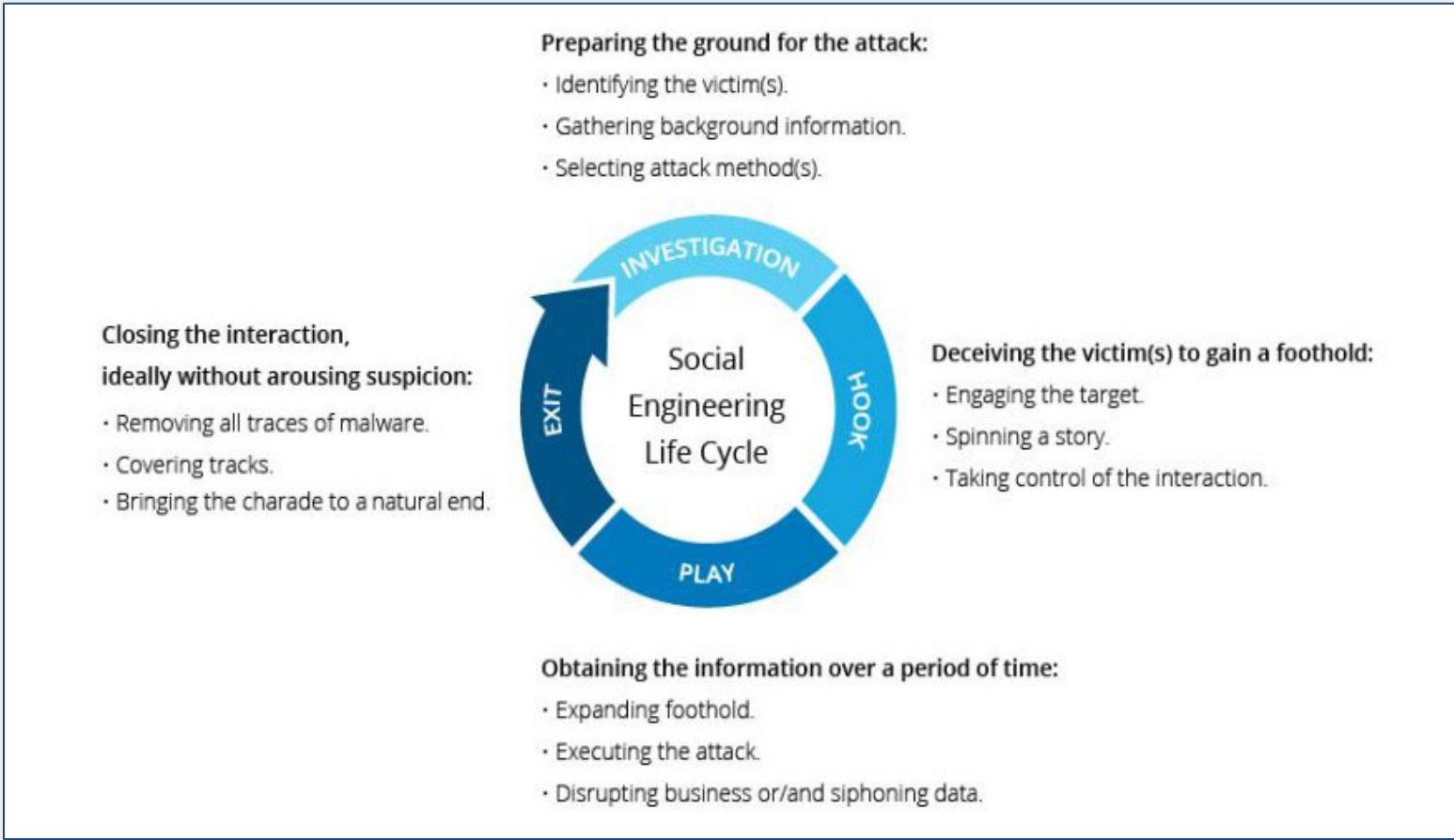

Source: Security Metrics

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Phases of a Social Engineering Attack

Preparing the ground for the attack:
- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

INVESTIGATION

HOOK

PLAY

EXIT

Social Engineering Life Cycle
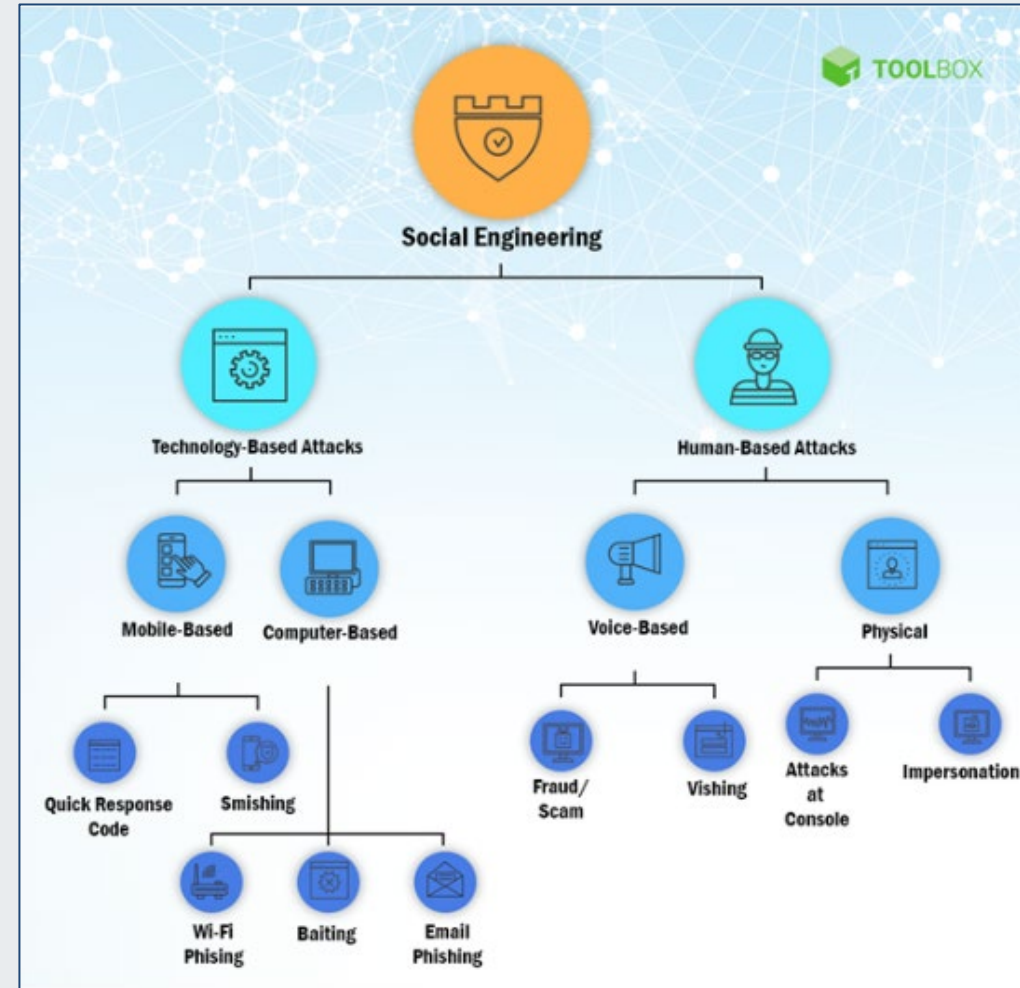
Source: Imperva

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

4

Types of Social Engineering Attacks

- Phishing

- Spearphishing

- Vishing

- Callback Phishing

- Business Email Compromise (BEC)

- Baiting

- Tailgating

- Deepfake Software

- Smishing
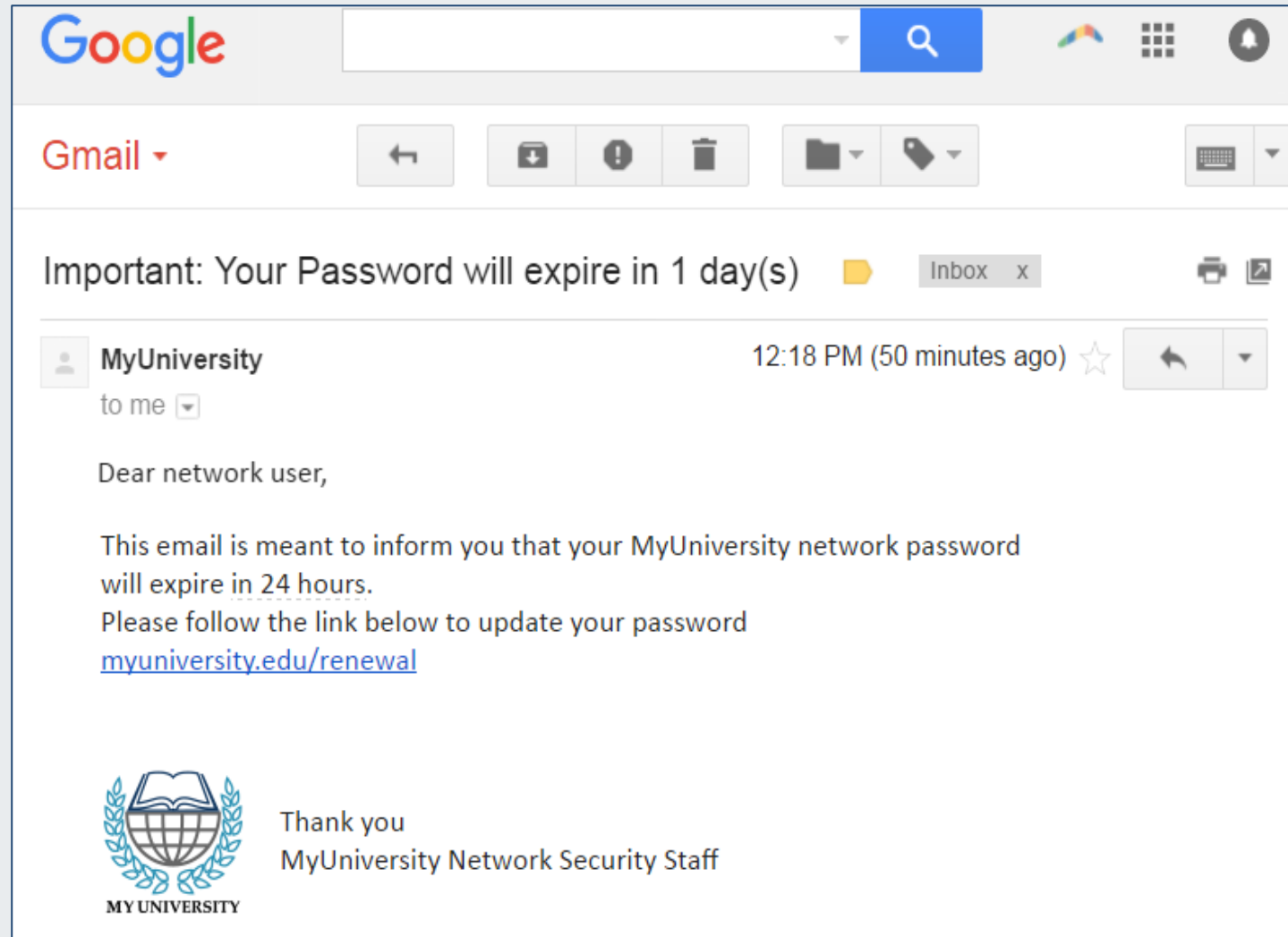
- Whaling

Source: SpiceWorks/Toolbox

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Phishing

Phishing is a type of social engineering in which an attacker sends a fraudulent message designed to trick a person into revealing sensitive information, or to deploy malicious software onto the victim's infrastructure, such as ransomware.

Source: Imperva

Phishing Attacks Top Threat to Healthcare

According to Carahsoft's 2021 HIMSS Healthcare Cybersecurity Survey, over a 12-month period, phishing attacks were the most common threat accounting for 45% of security incidents, followed by ransomware.

Threat	Percentage
Supply Chain Compromise or Attack	2%
Theft or Loss	2%
Distributed Denial of Service Attack	2%
Website or Web Application Attack	2%
Credential Harvesting Attack	4%
Fire, Flash Flood, or Natural Hazard	4%
Social Engineering Attack	5%
Negligent Insider Activity	5%
Breach or Data Leakage	7%
Ransomware Attack	17%
Phishing Attack	45%
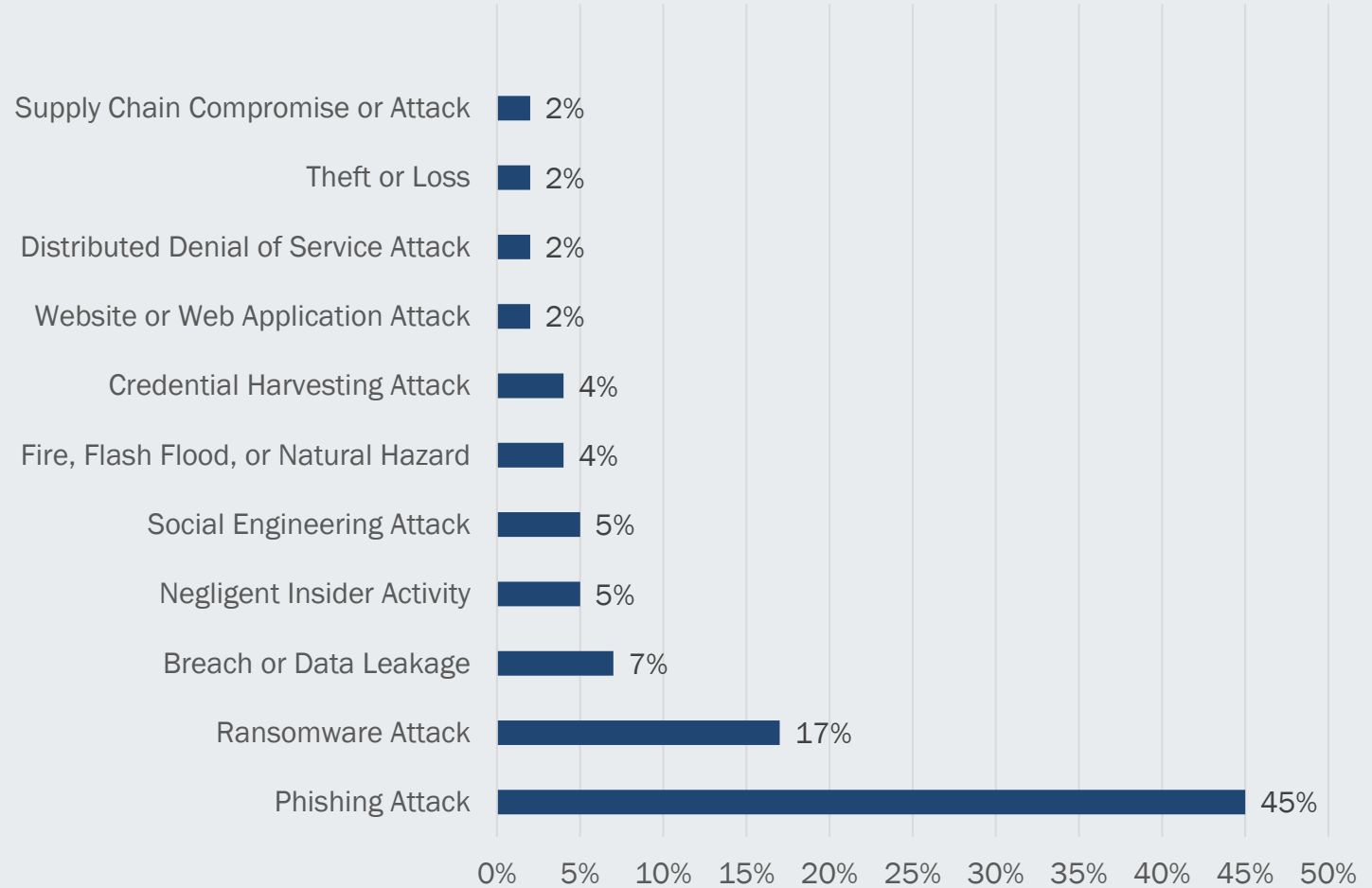
Source: MedCity News

Vishing

Vishing or "voice phishing," involves some form of a phone call to perform social engineering that involves defrauding people over the phone, enticing them to divulge sensitive information.

Agari's Q2 2022 cyber-intelligence report shows that phishing volumes have increased by 6% compared to Q1 2022. However, the use of 'hybrid vishing' has increased by 625%.
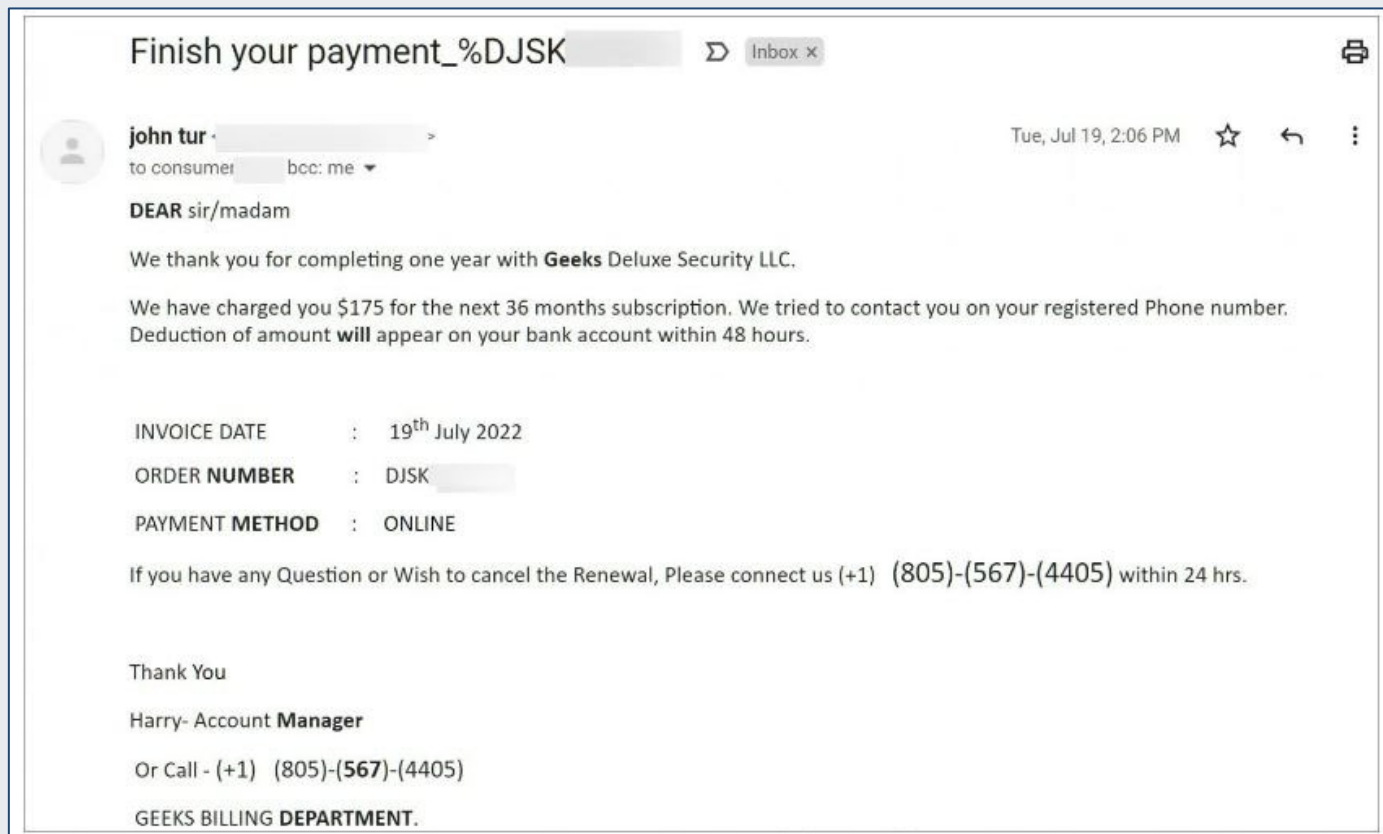
Share of Reported Vishing Cases Among Response-Based Attacks
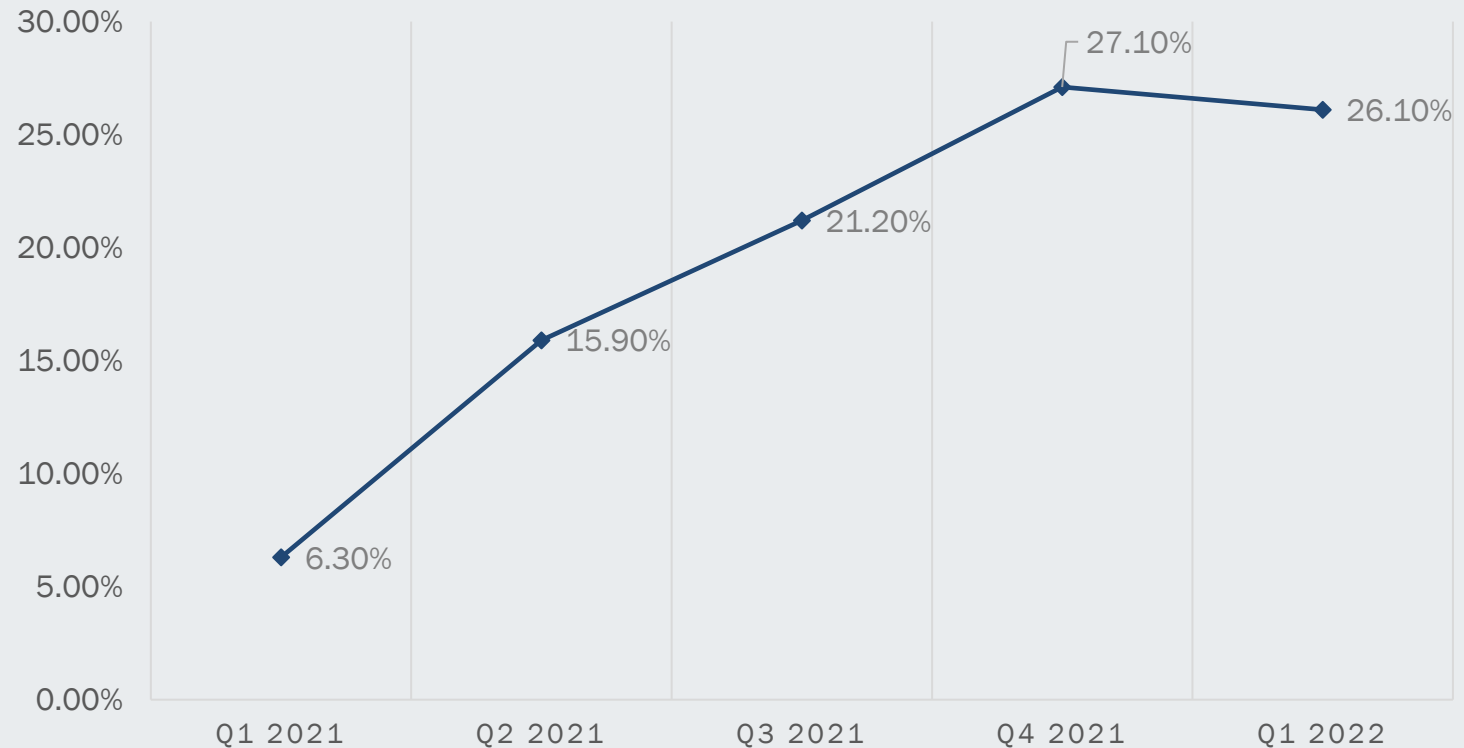
Source: Agari

Callback Phishing

Callback phishing is a hybrid form of vishing. This type of social engineering attack usually involves sending the target a fake email and calling, before sending a fake subscription/invoice notice.


Callback phishing email sample.
Source: BleepingComputer

Business Email Compromise (BEC)

A business email compromise (BEC) is when a threat actor sends an email to their target posing as trusted source with the intent to scam a business or defraud a company.

This type of attack can be difficult to detect and relies on impersonation, along with other social engineering tactics, to trick people into interacting on the threat actor's behalf.
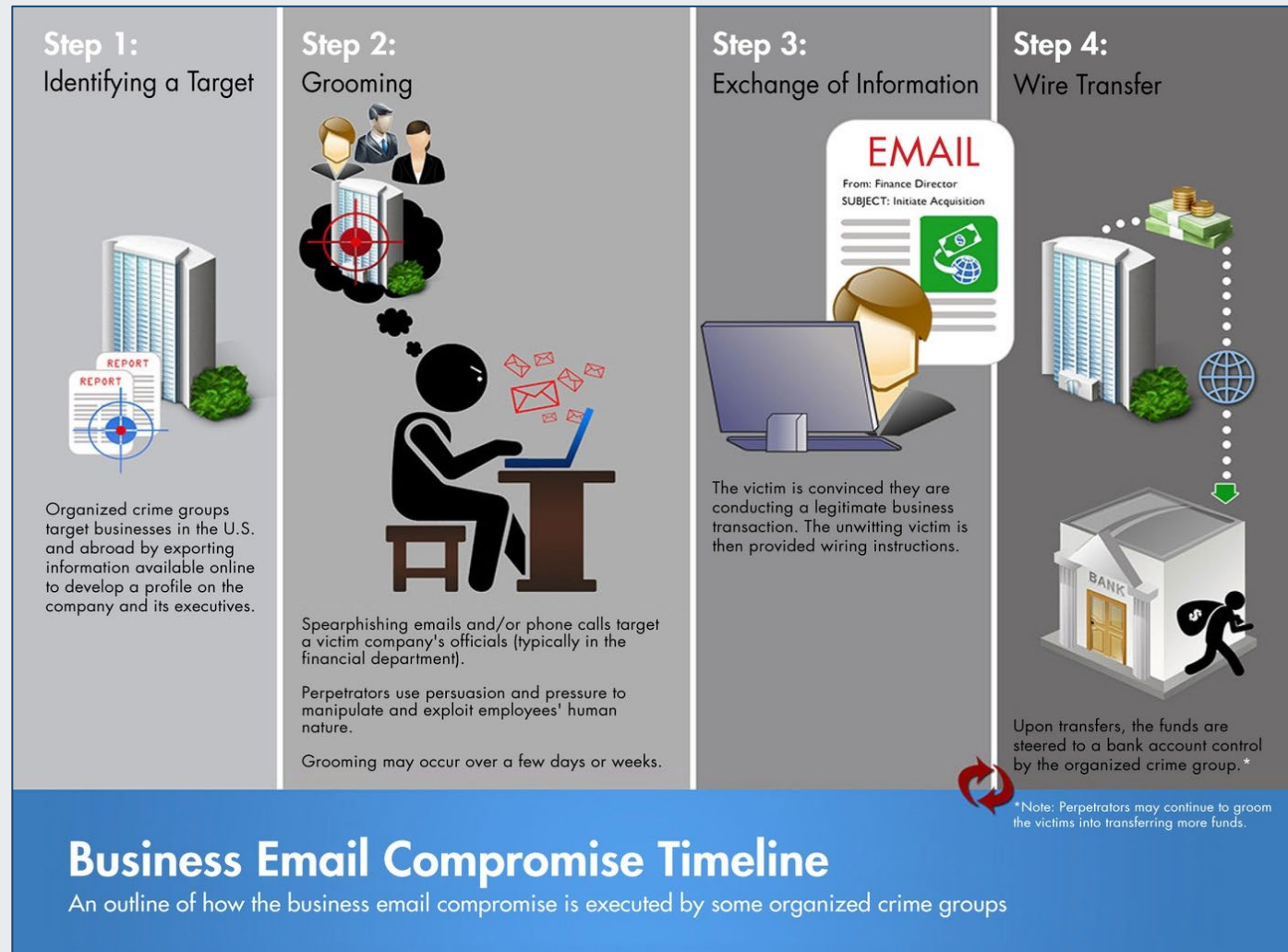
Source: FBI

Deepfake Software

The use of deepfake software involves a combination of voice cloning and video and allows anyone to take on the identity of trusted persona.

Source: Hitachi Systems Security

Want to see a magic trick? Tom Cruise impersonator Miles Fisher (left) and the deepfake Tom Cruise created by Chris Ume (right). | Image: Chris Ume

Source: The Verge

Whaling

Whaling is a phishing attack that involves a fake email masquerading as a legitimate email in order to target senior executives.

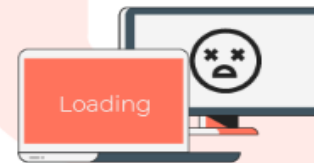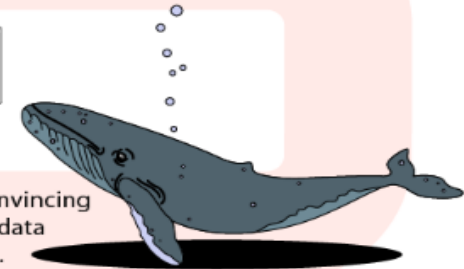*Source: Everyday Cyber*

Personality Traits of a Social Engineer and Social Engineering Behaviors/Scenarios

- The Dumpster Dive
- The Changing Passwords
- The Name-Drop
- The Walk-In
- The Unlocked Computer
- The Relaxing Conversation
- The Fake IT Guy
- The iPad Walk Out
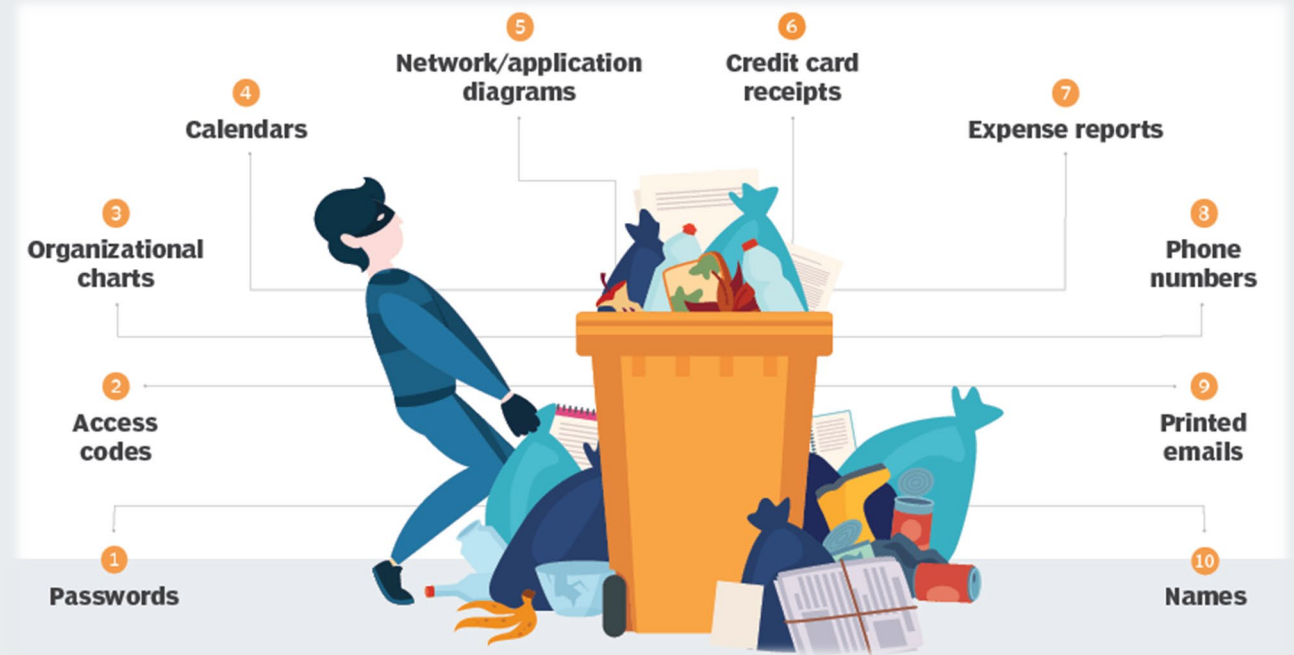
Source: TechTarget

Why Is Social Engineering a Problem for Healthcare?

Social engineering can be difficult to identify, particularly in larger organizations where staff members do not always know their fellow coworkers. Some reasons social engineers target healthcare employees:

- People are naturally trusting
- People have a desire to help
- People want to look intelligent
- People do not want to get in trouble
- Some people take short cuts

1. Attacker performs reconnaissance attack

2. User receives an e-mail with a pdf file attachment supposedly from a hospital's supplier

3. User opens the attached file which executes malware

4. Malware steals user's credentials and sensitive data

5. Malware sends the stolen data to a remote user
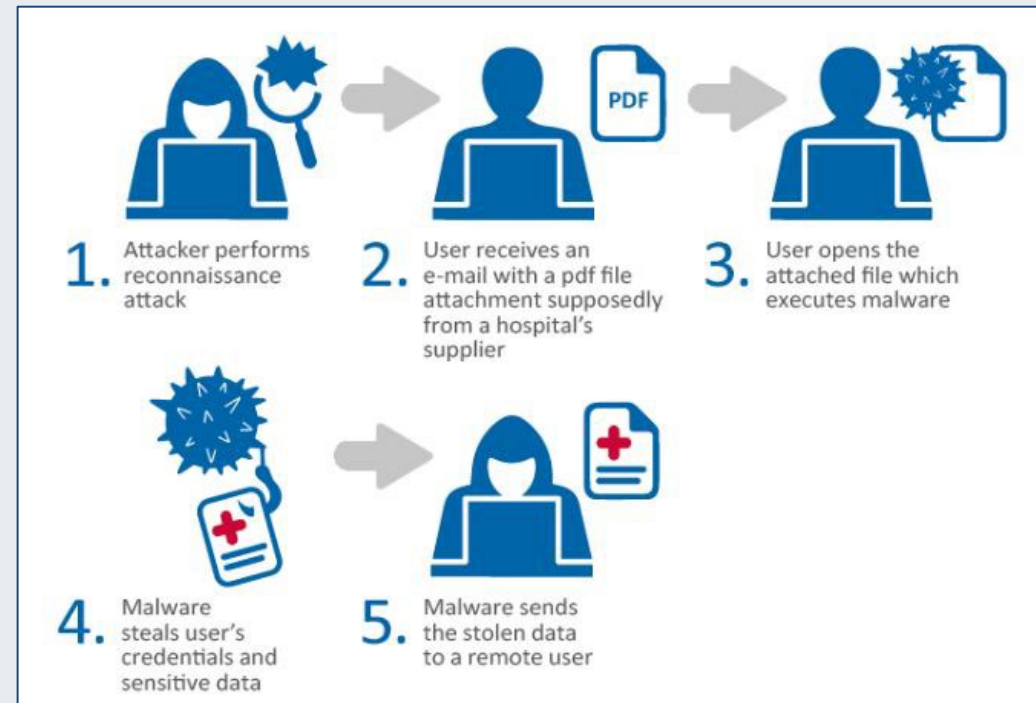
Source: Research Gate

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Impact of Social Engineering and Data Breaches

Attacks Linked to Social Engineering

Percentage of Attacks Tied to Phishing, Vulnerability Exploitation, and Stolen Credentials, by Quarter, 2021

Legend: Phishing, Vulnerability Exploit, Stolen Credentials

Quarter	Phishing	Vulnerability Exploit	Stolen Credentials
2021 Q1	47%	37%	5%
2021 Q2	36%	23%	22%
2021 Q3	30%	52%	7%
2021 Q4	42%	31%	0%

Source: IBM Security X-Force

Average Cost of a Data Breach

Top Five Countries or Regions with Highest Data Breach Cost:

The United States = $9.44 million

The Middle East = $7.46 million

Canada = $5.64 million

The United Kingdom = $5.05 million

Germany = $4.85 million

Average Total Cost of a Data Breach in Millions USD

Source: IBM

Average Cost of a Data Breach By Industry

Average Cost of a Data Breach by Industry in Millions USD

Public Sector: $1.93 (2021), $2.07 (2022)
Energy: $4.65 (2021), $4.72 (2022)
Technology: $4.65 (2021), $4.97 (2022)
Pharmaceuticals: $5.04 (2021), $5.01 (2022)
Financial: $5.72 (2021), $5.97 (2022)
Healthcare: $9.23 (2021), $10.10 (2022)

■ 2021 ■ 2022

Source: IBM

Steps to Protect Your Organization

- Implement backups with best practices
- Have a structured program for regular software updates
- Rollout sensible restrictions
- Impose proper credential tracking
- Train staff to be alert and cautious
- Train staff to verify all requests
- Hold every department accountable for security
- Increase physical security
- Hire a consultant
- Take advantage of resources

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Resources

Health Industry Cybersecurity Practices (HICP)

Source: HHS

CISA: Free Cyber Services & Tools

Maximize the Organization's Resilience to a Destructive Cyber Incident

Service	Skill Level	Owner	Description	Link
Microsoft Security Compliance Toolkit 1.0	Basic	Microsoft	This toolset allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.	Download Microsoft Security Compliance Toolkit 1.0 from Official Microsoft Download Center
Authentication Tool	Advanced	Trusona	A passwordless authentication for WordPress admins that enhances security & usability.	Trusona for WordPress – WordPress plugin | WordPress.org
HYPR Zero	Advanced	HYPR True Passwordless(™) MFA platform	HYPR Zero is designed for smaller organizations and delivers passwordless multi-factor authentication.	True Passwordless MFA for Small Business Pricing | HYPR
Windows Auto-Backup	Basic	Microsoft	This tool sets up automatic backups of Windows 10 and 11 operating systems.	https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef
Google Backup & Sync	Basic	Google	This tool backs up files on Windows or Mac computers. **Note:** it does not allow users to restore their system; it only saves copies of files.	https://support.google.com/drive/answer/7638428
Microsoft Threat Modeling Tool	Advanced	Microsoft	This tool is designed to make threat modeling easier for developers through a standard notation for visualizing system components, data flows, and security boundaries.	https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
Microsoft SecCon Framework	Advanced	Microsoft	This framework is designed to help prioritize endpoint hardening recommendations.	https://github.com/microsoft/SecCon-Framework

Source: CISA

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Reference Materials

References

- "Healthcare: Recognize Social Engineering Techniques," Security Metrics. https://www.securitymetrics.com/blog/healthcare-recognize-social-engineering-techniques

- "Business Email Compromise (BEC)," Proofpoint. https://www.proofpoint.com/us/threat-reference/business-email-compromise#:~:text=Business%20email%20compromise%20(BEC)%20is,every%20industry%20around%20the%20world.

- "Scams and Safety: Business Email Compromise," FBI. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

- Larson, Selena, Blackford, Daniel, and Proofpoint Research Team. "How Threat Actors Hijack Attention: The 2022 Social Engineering Report," Proofpoint. June 22, 2022. https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-hijack-attention-2022-social-engineering-report

- "1H 2022 Healthcare Data Breach Report," HIPAA Journal. August 11,2022. https://www.hipaajournal.com/1h-2022-healthcare-data-breach-report/ .

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- "X-Force Threat Intelligence Index 2022" IBM Security. 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ

- "Health Industry Cybersecurity Practices (HICP) - Small Healthcare Organization,"HHS. https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Small-Practices-Official-Document-R.pdf

- "Health Industry Cybersecurity Practices (HICP) – Medium & Large Healthcare Organizations,"HHS. https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Medium-to-Large-Organizations-Official-Document-R.pdf

- "Free Cybersecurity Services and Tools," CISA. https://www.cisa.gov/free-cybersecurity-services-and-tools

  Dove, Martina. "See No Evil, Hear No Evil: The Use of Deepfakes in Social Engineering Attacks." The State of Security. January 24, 2022. https://www.tripwire.com/state-of-security/security-data-protection/use-of-deepfakes-in-social-engineering-attacks/

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

References

- "The Soaring Cost of a Data Breach Leads to Soaring Prices,"IDAgent. August 11, 2022. https://www.idagent.com/blog/the-soaring-cost-of-a-data-breach-leads-to-soaring-prices/
- "What Growing Federal Scrutiny of Healthcare Cybersecurity Means for Organizations," Health Tech Magazine. June 30, 2022. https://healthtechmagazine.net/article/2022/06/what-growing-federal-scrutiny-healthcare-cybersecurity-means-organizations
- Siwicki, Bill. "How to protect against social engineering attacks," HealthcareIT News. July 26,2021. https://www.healthcareitnews.com/news/how-protect-against-social-engineering-attacks
- "9 Ways to Social Engineer a Hospital," Security Metrics. https://www.securitymetrics.com/blog/9-ways-social-engineer-hospital#:~:text=Social%20engineering%20is%20basically%20human,)%20and%2For%20install%20malware.
- McKeon, Jill. "Common Types of Social Engineering, Phishing Attacks in Healthcare," Health IT Security. May 27, 2022. https://healthitsecurity.com/features/common-types-of-social-engineering-phishing-attacks-in-healthcare

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- TripWire Guest Authors. "Q1 2022 Phishing Threat Trends and Intelligence Report," Tripwire. June 20,2022. https://www.tripwire.com/state-of-security/security-data-protection/phishing-threat-trends-intelligence-report/

- "Social Engineering Training: What Your Employees Should Know," Security Metrics. https://www.securitymetrics.com/blog/social-engineering-training-what-your-employees-should-know

- Toulas, Bill. "Callback phishing attacks see massive 625% growth since Q1 2021," Bleeping Computer. August 15, 2022. https://www.bleepingcomputer.com/news/security/callback-phishing-attacks-see-massive-625-percent-growth-since-q1-2021/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Questions

FAQ

Upcoming Briefing

- 9/1 – Emerging Technology and the Security Implications for the Health Sector

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.

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**

Contacts

HHS.GOV/HC3

HC3@HHS.GOV