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)
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.
Phases of a Social Engineering Attack

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

Decieving 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/siphoning data.

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

Source: Imperva
Types of Social Engineering Attacks

- Phishing
- Spearphishing
- Vishing
- Callback Phishing
- Business Email Compromise (BEC)
- Baiting
- Tailgating
- Deepfake Software
- Smishing
- Whaling

Source: SpiceWorks/Toolbox
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.
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.

<table>
<thead>
<tr>
<th>Security Incident</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Attack</td>
<td>45%</td>
</tr>
<tr>
<td>Ransomware Attack</td>
<td>17%</td>
</tr>
<tr>
<td>Breach or Data Leakage</td>
<td>7%</td>
</tr>
<tr>
<td>Credential Harvesting Attack</td>
<td>4%</td>
</tr>
<tr>
<td>Social Engineering Attack</td>
<td>5%</td>
</tr>
<tr>
<td>Negligent Insider Activity</td>
<td>5%</td>
</tr>
<tr>
<td>Fire, Flash Flood, or Natural Hazard</td>
<td>4%</td>
</tr>
<tr>
<td>Website or Web Application Attack</td>
<td>2%</td>
</tr>
<tr>
<td>Distributed Denial of Service Attack</td>
<td>2%</td>
</tr>
<tr>
<td>Theft or Loss</td>
<td>2%</td>
</tr>
<tr>
<td>Supply Chain Compromise or Attack</td>
<td>2%</td>
</tr>
<tr>
<td>Theft or Loss</td>
<td>2%</td>
</tr>
</tbody>
</table>

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%.
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.
Business Email Compromise (BEC)

A business email compromise (BEC) is when a threat actor sends an email to their target posing as a 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.

Business Email Compromise Timeline
An outline of how the business email compromise is executed by some organized crime groups

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

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.
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

Source: Research Gate
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

- Phishing
- Vulnerability Exploit
- Stolen Credentials

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

Source: IBM
Average Cost of a Data Breach By Industry

Average Cost of a Data Breach by Industry in Millions USD

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
Resources
Health Industry Cybersecurity Practices (HICP)
CISA: Free Cyber Services & Tools

Maximize the Organization’s Resilience to a Destructive Cyber Incident

<table>
<thead>
<tr>
<th>Service</th>
<th>Skill Level</th>
<th>Owner</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Security Compliance</td>
<td>Basic</td>
<td>Microsoft</td>
<td>This toolset allows enterprise security administrators to download, analyze,</td>
<td>Download Microsoft Security Compliance Toolkit 1.0 from Official Microsoft Download Center</td>
</tr>
<tr>
<td>Toolkit 1.0</td>
<td></td>
<td></td>
<td>test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.</td>
<td></td>
</tr>
<tr>
<td>HYPR Zero</td>
<td>Advanced</td>
<td>HYPR</td>
<td>HYPR Zero is designed for smaller organizations and delivers passwordless multi-factor authentication.</td>
<td>True Passwordless MFA for Small Business Pricing</td>
</tr>
<tr>
<td>Windows Auto-Backup</td>
<td>Basic</td>
<td>Microsoft</td>
<td>This tool sets up automatic backups of Windows 10 and 11 operating systems.</td>
<td><a href="https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091c2-bb9d-3ea3-ad18-52ef2b8e8bf7">https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091c2-bb9d-3ea3-ad18-52ef2b8e8bf7</a></td>
</tr>
<tr>
<td>Google Backup &amp; Sync</td>
<td>Basic</td>
<td>Google</td>
<td>This tool backs up files on Windows or Mac computers. Note: it does not allow users to restore their systems; it only saves copies of files.</td>
<td><a href="https://support.google.com/drive/answer/7628428#">https://support.google.com/drive/answer/7628428#</a></td>
</tr>
<tr>
<td>Microsoft Threat Modeling Tool</td>
<td>Advanced</td>
<td>Microsoft</td>
<td>This tool is designed to make threat modeling easier for developers through a standard notation for visualizing system components, dataflows, and security boundaries.</td>
<td><a href="https://www.microsoft.com/en-us/securityengineering/video/threatmodeling">https://www.microsoft.com/en-us/securityengineering/video/threatmodeling</a>?</td>
</tr>
<tr>
<td>Microsoft SecCon Framework</td>
<td>Advanced</td>
<td>Microsoft</td>
<td>This framework is designed to help prioritize endpoint hardening recommendations.</td>
<td><a href="https://github.com/microsoft/SecCon-Framework">https://github.com/microsoft/SecCon-Framework</a></td>
</tr>
</tbody>
</table>

Source: CISA
References


References


References


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.
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

<table>
<thead>
<tr>
<th>Sector and Victim Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alerts and Analyst Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Briefings</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
Contacts

HHS.GOV/HC3

HC3@HHS.GOV