How to Protect Against Social Engineering in Healthcare

At the heart of every successful cyberattack lies a human element. Social engineering, or the devious art of manipulating you into divulging confidential information, is now a ruthless menace impacting healthcare. Unlike traditional hacking that targets systems, social engineering targets you—it seeks to exploit your trust, curiosity, and inherent desire to help.

Common Tactics of Social Engineering

Phishing

The leading cause of healthcare data breaches today is phishing. While these emails appear to come from trusted sources, their aim is to steal sensitive data or have the target open a malicious link or attachment to initiate ransomware attacks, in turn compromising patient care by disrupting access to your digital records.

Business Email Compromise (BEC)

BEC is a more targeted type of phishing attack. By impersonating a trusted contact, this attack aims to trick recipients into performing out-of-the-ordinary tasks like wire transfers, purchasing gift cards, or providing login credentials, ultimately leading to further compromises.

Vishing

"Voice phishing" involves attackers calling targets, often impersonating patients or colleagues, to extract sensitive information to access and control networks or devices. Tactics now include using AI-generated voice-replication tools to mimic trusted people, which makes vishing even harder to detect.

Consequences of Falling Victim to Social Engineering

Data Breaches

Exposure of sensitive protected health information (PHI) or personally identifiable information (PII) can lead to identity theft and other privacy violations.

Operational Disruption

Interruption of medical services, potentially endangering patient care and compromising safety.

Financial Losses

Including costs related to legal fees, compliance penalties, ransom payments, and lost revenue.

Reputational Damage

Loss of trust from patients and partners, impacting your organization's credibility and long-term viability.

Why You Might Be Vulnerable to Social Engineering

High-Stress Environment

Medical staff are often multitasking, moving quickly, and working under pressure, making them more likely to overlook phishing attempts.

Valuable Data

Your organization likely stores a vast amount of sensitive data, making it a lucrative target for cybercriminals.

Legacy Systems

Many healthcare facilities use outdated systems that are more vulnerable to attacks.

High Volume of Communication

Constant email and communication between departments and with patients increases the chances of pulling off successful social engineering attacks.

Lack of Training

Insufficient cybersecurity awareness training among healthcare staff makes it easier for threat actors to exploit human error.

Solutions to Combat Social Engineering

□ **Implement Multi-Factor Authentication (MFA)**

Implement MFA to add an extra layer of security, ensuring that even if passwords are compromised, unauthorized access is still prevented.

□ **Employ Managed Detection and Response (MDR)**

MDR services can monitor identities, analyze security events, and promptly respond to threats.

□ **Create an Incident Response Plan**

Develop and maintain a robust plan to quickly address any breaches and minimize damage.

□ **Introduce Security Awareness Training (SAT)**

SAT programs can train staff to recognize and respond to phishing and other social engineering tactics. Incorporate phishing simulations to test and improve their skills.

□ **Verify Senders of Emails**

Review emails carefully and double-check the authenticity of the person, service, or business sending you the message.

□ **Perform Regular Audits and Updates**

Conduct frequent audits and keep all systems and software updated to mitigate vulnerabilities.

□ **Don't Click Links**

Do not click any links or open an unsolicited attachment from unverified senders.

□ **Develop Strict Access Controls**

Reduce the risk of data breaches by limiting access to sensitive information based on each individual's needs and role.

By remaining vigilant against tricky tradecraft and implementing trusted solutions, healthcare organizations like yours can significantly reduce your vulnerability to social engineering attacks and protect critical data and operations.

Want to dive deeper into social engineering in healthcare?

Check out our blog for more insights and strategies.

HUNTRESS®