Transcript: Social Engineering Video

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Imagine this: It's a regular Tuesday morning with nothing exciting going on, and then you receive an email from what looks to be an IT support person from your patient billing company.

The sender instructs you to click on a link to update your billing software passwords, but something not quite right in the email catches your eye.

The sender's email address looks suspiciously different from ones you have seen in the past, so you double check its legitimacy.

You were right to be suspicious, because that was an attempted email phishing attack, which is a form of social engineering.

Had you clicked the link provided, you would have been directed to a fake login page, which collects employee login credentials and transmits this information to the attackers.

Then, the attacker can use the employee's login credentials to access your organization's financial and patient data to possibly cause damage to your network while also gaining further access to your enterprise, sometimes even taking control or stealing patient data.

These threats can affect organizations in various parts of a hospital and in different health care settings.

Just imagine if your co-workers, who may not know how to identify a social engineering threat, encountered a phishing attempt!

Collectively, healthcare organizations have lost millions of dollars over the years, and the cost to healthcare and patients is increasing. Additionally, these attacks can lead to hospital shutdowns, diverting care, and even loss of public trust.

The bottom line is: Cyber-attacks can happen anywhere, any time…and we have to increase our cybersecurity awareness as these threats evolve.

Social engineering began as tricks to fool people into compromising their passwords via email by claiming to represent a supervisor, or by phone, posing as a system administrator.

Typically, these attacks have been called "Phishing attacks", but recently they have become much more sophisticated and personal.

The Attacker may leverage trending events such as a global healthcare emergency, or a high-profile cyber attack.

Another trick is sending emails, calls or flyers to respond for free software or tickets to a healthcare industry conference. The Attacker may even send several emails to establish a level of trust.

You need to be suspicious of emails or messages from unknown senders, those that request sensitive information such as Protected Health Information (PHI) or personal information, or include a call to action that stresses urgency or importance.

You need to train staff to recognize suspicious e-mails and messages, and to know where to report them.

And you should never open email attachments or click links from unknown senders.

The Health Industry Cybersecurity Practices, also called HICP, Publication aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector.

This includes Social Engineering Attacks, which is the first threat in the HICP Five Threat Series.

The HHS 405(d) program has more resources, like other publications, awareness products, and outreach-focused social media platforms and events, to keep your organization cyber safe, which keeps your patients safe.

The Department of Health and Human Services, or HHS for short, and the public-private partnership initiative known as 405(d), are committed to aligning healthcare cybersecurity approaches, by creating,

managing, and leading all industry-led processes to develop consensus-based guidelines, practices and methodologies to strengthen the healthcare sector's cybersecurity posture against cyber threats like social engineering. As healthcare industry professionals, the best way for us to stay vigilant is for everyone, including you, to play a part and remember that Cyber Safety is Patient Safety.

Produced by the U.S. Department of Health and Human Services at Taxpayer expense.