CRISP

Connecting Providers with Technology to Improve Patient Care

# CRISP Cyber: Advancing Health Care Security Webinar Q&A

1. **In the HIMSS Cybersecurity report, organizations were warned about APIs being forecasted as the next big cyber-attack. Does CRISP use API? If so, how are you defending against a potential attack?**

   CRISP utilizes multiple APIs across our landscape, and we are always preparing, monitoring, and reacting to emerging threats that hit the market. If you would like to learn more, please contact security@crisphealth.org for a more technical discussion.

2. **Can you give suggestions on staff phishing training? Do you suggest in person or online, or any materials you use?**

I suggest a mix of both in-person and online training. While online training is great, many of the content details can be lost due to a lack of true focus on the training. Doing a yearly in person review, and bi-yearly online refresher can help keep the knowledge fresh in your staff's minds.

3. **What is your favorite phish, and are there different types of phishing?**

My favorite kinds of phish are the ones that are custom crafted to the environments their targeting. It shows effort and dedication from the people attacking us. I appreciate the work, and it makes successfully defending against their hard work all the more enjoyable. There are also different kinds of phishing attacks, ranging from **deceptive** (imitating a legitimate service) to **spear phishing** (attempting to get you to reveal confidential information).

4. **How secure are hospital system EMRs for accessing the CRISP Portal?**

Hospitals are required to follow strict HIPAA requirements and part of this includes standard security and privacy practice. If you would like to know more about a certain hospital, please reach out to the security and privacy team there for more information.

5. **What kind of encryption is used in the data center?**

We adhere to internal standards, which are set above the industry acceptance level.

6. **What is the difference between a hard and soft token?**

Hard tokens are something you have on you as a physical object, such as an RSA token. A Soft Token is a software-based security control that replicates the advantages of multifactor authentication while creating a simplified distribution infrastructure with significantly lower costs.

7. **How do you report a potentially malicious e-mail?**

Different environments have different reporting mechanisms. For CRISP, all phishing emails can be sent as an attachment to security@crisphealth.org for review. I recommend reaching out to your internal security team to learn how you can report potentially malicious emails in your environment.