Phishing Awareness Fact Sheet

IN TODAY'S WORLD, CYBER SECURITY THREATS ABOUND. YOU ARE THE GUARDIAN OF YOUR ENTERPRISE.

As many as 90% of cyber security incidents are the result of human error. A preventable cyber attack could be devastating, leading to financial and reputational losses. To assist with your cyber security awareness initiatives, we are excited provide you with premium cyber security information and expert-level answers to common cyber security questions. Share this content with your peers and your teams to increase cyber security awareness.

PHISHING ATTACK SURGES…

In August of 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a joint advisory warning of a wave of "vishing," or voice phishing, attacks targeting US private sector companies. Since then, phishing attacks of numerous varieties have plagued public and private industry groups. In recent weeks, a spike in pandemic-themed phishing emails have jeopardized employee information. Within these emails, hackers have posed as employers who are requesting proof of vaccination, describing new in-office coronavirus prevention strategies or similar.

TOP WAYS TO AVOID PHISHING THREATS?

- Track the latest phishing trends and know what to watch out for. Stay current when it comes to the latest phishing campaigns by following vendor-sponsored cyber security blogs, like CyberTalk.org.

- Beware of voice phishing (vishing) groups for hire have emerged and are targeting employees who are working from home. These attacks often combine a phone call with emails urging users to fill in their corporate credentials.

- Understand mobile phishing threats. Mobile phishing remains as one of the largest concerns for security teams. One call or click and an employee's information sharing could accidentally take down the entire corporate network.

- Deploy email security solutions. Modern email filtering solutions can protect against malware and other malicious payloads in email messages. Solutions can detect emails that contain malicious links, attachments, spam content, and language that could suggest a phishing attack.

CHECK OUT CYBER TALK'S OTHER EXECUTIVE-LEVEL PHISHING RESOURCES…

- Executive-level phishing attacks have been known to result in as much as $75.8 million in losses. Is your organization prepared? Read our latest phishing whitepaper here.

- Wondering if phishing can be detected by firewalls? Heard about those spontaneously disappearing phishing emails? Can you report phishing as an illegal activity? Get answers to those phishing questions and more, right here.

- Are you a financial industry executive? Discover phishing campaigns that hackers have devised to undermine your industry. Financial industry executives' resources.

For further expert insights into phishing threats, read about the five most expensive phishing scams of all time here.