CTSI
TECHNICAL UPDATE
Volume 28 Number 27 | July 2, 2024

CYBERSECURITY INSIGHTS: CALLBACK PHISHING AND EMPLOYEE TRAINING

In today's digital age, cybersecurity is a critical concern for counties of all sizes. As cyber threats become increasingly sophisticated, counties must stay vigilant and proactive in protecting their sensitive data. CTSI will stay informed of evolving threats and provide quarterly cybersecurity updates on the latest concerns, best practices, and security protocols. This knowledge can significantly reduce the risk of a successful cyber attack and promote a security-first culture.

CALLBACK PHISHING

Have you ever received an email telling you to call a phone number? Calling a phone number may seem safer than clicking on a link, but that's what makes this tactic so effective. In callback phishing scams, cybercriminals send you an email about something urgent, such as a fraudulent charge or a vital software update. This tactic is unique because the email includes a phone number you are prompted to call. Cybercriminals use callback phishing scams for their malicious purposes. Cybercriminals will trick you into revealing sensitive information if you call the number in the email. They may use an automated voice message that prompts you to enter sensitive information, such as your credit card or social security number. Cybercriminals can also try to trick you into downloading malware. To do this, they'll answer the phone and walk you through downloading malicious files onto your device.

Follow the tips below to stay safe from callback phishing scams:

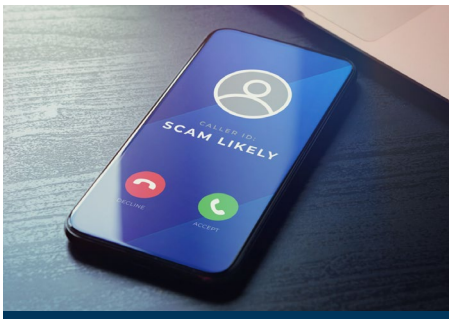
- Think before calling unknown phone numbers. Verify that a phone number is legitimate by navigating to that specific person or the business's official website.
- Before sharing sensitive information over the phone, ask the caller to tell you what information they have on file. If they can't prove they are legitimate, hang up.
- Watch out for a sense of urgency in emails. Phishing attacks rely on impulsive actions. So, always think before you call.

EMPLOYEE TRAINING

Employees are widely considered counties' first line of defense against cyber incidents, especially since all it takes is one staff mistake to compromise and wreak havoc on an entire workplace system. In light of this, counties must offer cybersecurity training. This training should center around helping county employees correctly identify and respond to common cyber threats. Additional training topics may include specific cybersecurity policies and methods for reporting suspicious activities. Because digital risks are everchanging, this training shouldn't be a standalone occurrence. Instead, counties should provide cybersecurity training regularly and update this training when needed to reflect the latest threats, attack trends, and workplace changes. Human error is one of the leading causes of cybersecurity breaches. Regular training and updates can help reduce the likelihood of mistakes leading to a breach. Keeping cybersecurity top of mind and providing clear guidance makes them less likely to fall victim to scams or inadvertently compromise security.

Follow the tips below to keep county employees safe:

- Promote good cyber hygiene practices, such as using strong passwords, recognizing phishing emails, and securely handling sensitive information.
- Periodically run simulated phishing exercises to test county employee awareness and response to phishing attempts.
- Establish a feedback mechanism for employees to report suspicious activities and suggest improvements to security practices.



WHAT THIS MEANS FOR COUNTIES

Regular cybersecurity updates are vital to an effective security strategy. They help keep counties informed, vigilant, and prepared to respond to threats. CTSI recommends counties implement these essential cybersecurity controls to help manage their cyber exposures. This will safeguard and reduce digital vulnerabilities at the county level and assist in obtaining coverage with higher limits and lower premiums for CAPP. For more information, contact CTSI at (303) 861-0507.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 Grant St., Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832