CTSI
TECHNICAL **UPDATE**
Volume 28 Number 4 | January 23, 2024

CYBERSECURITY REMINDERS: EMERGING CYBER THREATS IN 2024

As technology continues to advance at a rapid pace, so do the capabilities for individuals to exploit vulnerabilities for various motives. The year ahead promises a range of cyber threats, including the resurgence of traditional menaces like ransomware to the emergence of novel dangers such as AI-driven attacks and quantum-enabled exploits. Understanding and anticipating the evolving nature of cyber attacks is critical. This Technical Update provides a glimpse into threats that we believe deserve our attention now as we aim to keep our digital domains secure with the new year.

AI ADVANCED PHISHING

What is artificial intelligence (AI) phishing? We have all received phishing attempts, likely even within the last year. A bad actor trying to get money, gift cards, or access to your email. Sometimes they pretend to be your bank, a tech company (Microsoft, Amazon, etc.), or a co-worker. The ultimate objective is to gain access to your email, access to the network, or for you to purchase gift cards and send the information to them.

How does AI affect these types of attacks? One way of identifying these attempts in the past was poor grammar or spelling in the initial email. Another was unprofessional or overly formal language being used in the email, text, or chat. With AI this is shifting quickly. Even those who do not speak English well can use AI to compose a business-friendly email with urgency asking you to login immediately to rectify an order or error with your account. By collecting biological data on the internet, AI can be trained to sound like a co-worker or friend who is asking you for a favor.

How can you protect yourself? With these newer, more advanced methods in AI, we can't always trust what we hear or read. If you have the ability to enable SPF, DKIM, or DMARC authentication (or all three) on your email server, do so. If your email host allows you to flag external emails, this can help identify those emails pretending to be a co-worker. Look at the sender's email address for those seeming to be from a financial institution or online account. If they are asking you to login, do not click any links in the email. Instead, open a browser, go to their official site and login to your account. From there see if there are any notices of needing to reset your login information or update information for your account.

NATION-STATE ATTACKS

Why are nation-state attacks a concern? In October of last year, Microsoft issued a warning that nation-states, or state-sponsored attacks, increased dramatically in 2023. Most of these came from North Korea, China, pro-Israel, or pro-Palestinian groups. Many of these attacks are targeted at governmental entities, infrastructure, military suppliers, and similar businesses or entities. Any company that has personal information for a group of people (patients, employees, online accounts, etc.) could be a potential target. These state-sponsored attacks can have the objective of disrupting infrastructure of an area of another country or stealing military or medical secrets. Another objective may just be to gain as much personal information to send fake news or gossip to influence elections or support for issues that will be to their benefit.

How can you protect yourself? In these cases, take common sense precautions when it comes to unusual emails and text messages. Also, make sure all networking equipment and Internet of Things (IoT) are kept up-to-date with firmware and security updates. Before connecting an IoT device, such as a wireless camera, Alexa device, wireless light or similar devices, to the work network, please consult your supervisor or IT department. These often have weak security and can be a vector point for a network intrusion.

WHAT THIS MEANS FOR COUNTIES

Protect yourself from AI-driven phishing attacks with a mixture of awareness, vigilance, and proactive measures. Number one tip is to always verify sender authenticity! Understanding the evolving landscape will help you adapt your security measures accordingly and maintain a secure digital environment.

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