CTSI
TECHNICAL **UPDATE**
Volume 27 Number 32 | August 8, 2023

CYBERSECURITY REMINDERS: AI AND PHISHING

Cybersecurity is a critical business concern from the front line of information technology all the way to the C-suite. Attacks can disrupt operations, fracture supply chains, and diminish customer confidence. In past years, cybercriminals focused on malware attacks. Most recently, they have shifted their focus to using artificial intelligence and phishing attacks.

ARTIFICIAL INTELLIGENCE

AI has been in the news a lot lately. It has amazing potential to do good, but also a massive ability to do harm. AI is a tool like any other. Unfortunately, threat actors trying to gain information from victims have already begun to exploit the abilities of AI. These imposters have been able to train AI to copy a person's voice just from social media video posts and then, in turn, use that to call relatives or friends claiming to be in distress and needing money transferred. They are also using AI to better communicate, if English is not their first language. Another growing area of concern is in creating online profiles for dating apps and "catphishing" others into giving them money or information.

You can protect yourself by limiting public posts on social media and verifying who it is with whom you are communicating. The more publicly accessible content you post, the more information exists that can be used to train AI to sound or even look like you. Soon it may be near impossible to distinguish true or fake recordings of celebrities or politicians without advanced computerized analyzation. Making your social media posts private and only approving personal connections can assist in limiting what data on you is out there.

Whatever the case, if you don't know the person, be cautious in letting them follow you or accepting a friend request. Secondly, if you receive a distressing email or phone call from a co-worker, family member or friend, especially if the phone number or email address is unfamiliar, take extra effort to verify the person really is the one that they claim to be. For example, you might text them on their number familiar to you and ask if they are in need or you may tell them you are going to hang up and call them back at their usual number. Also, in voice conversations look for unnatural accents or intonation or longer pauses than normal as they take more time to type what they want the AI to say compared to a normal conversation.

PHISHING ATTEMPTS FOR 2023

We regularly see IT and online service notification attempts that could potentially affect users' daily work. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email. These are some of the most popular phishing email subjects:

- **HR:** Vacation Policy Update
- **Zoom:** The meeting has started! Where are you?
- **Adobe Sign:** Performance Review
- **Sharepoint:** [[manager_name]] shared "Test_Data" with you
- **DocuSign:** DocuSign Account Suspension Notice
- **Webmail:** Security alert for [[email]]

The #1 attack vector according to KnowBe4 Phishing Security Tests are phishing links in the email body. When these links are clicked, they often lead to disastrous cyberattacks such as ransomware and business email compromise. Below is a ranking of the top 5 attack vector types:

- **Link:** Phishing Hyperlink in the Email
- **Spoofs Domain:** Appears to Come from the User's Domain
- **PDF Attachment:** Email Contains a PDF Attachment
- **Branded:** Phishing Test Link Has User's Organizational Logo and Name
- **HTML Attachment:** Email Contains an HTML Attachment

WHAT THIS MEANS FOR COUNTIES

Be careful out there! As AI technology continues to develop, scammers will find new and creative ways to use it to exploit people. Workplace fraud is on the rise as more business-related emails are coming from HR/IT/Managers in recent months. It's essential to be aware of these trends and take steps to protect yourself.

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