DigiKnow

CYBER SECURITY DEPENDS ON YOU

ARTIFICIAL INTELLIGENCE AND SOMEONE WANTS YOUR PHONE NUMBER

May 2023| Issue 2023:4

ARTIFICIAL INTELLIGENCE (AI), THE HOTEST TREND IN TECHNOLOGY?

One of the most widely covered subjects in the media today is AI. The pace at which it is growing is both a source of excitement and fear in business, healthcare, and academia. So, what is this all about?

Generative artificial intelligence (AI) describes algorithms (such as ChatGPT) that can be used to create new content, including audio, code, images, text, simulations, and videos.

According to Gartner analyst Avivah Litan, some of the biggest risks of generative AI concern trust and security. Some countries, like Italy, have completely banned ChatGP. The European Union has proposed the European AI Act, with rules that will heavily restrict the use of AI in critical infrastructure, education, law enforcement, and the judicial system.

Areas of concern with generative AI include: deepfakes, data privacy and hallucinations. A **deepfake** uses AI to create photos, videos or voice recordings that are fake but take the image or likeness of another person. These counterfeit images have been used to attack politicians and celebrities, to create and spread misinformation and even to set up fake accounts.

Data Privacy is a major concern because user data is often stored for model training. Employees can inadvertently expose sensitive or proprietary data when interacting with generative chatbot solutions. Additionally, information can be stored indefinitely and can be harvested in a data breach.

THE GOOGLE VOICE SCAM
How this Verification Code Scam Works and How to Avoid It

According to the Federal Trade Commission (FTC) and the Better Business Bureau (BBB) there is a relatively new scam circulating involving online selling sites and hijacked phone numbers.

Here's how it works:

The FTC states that scammers target people who post things for sale on sites like Craigslist or Facebook Marketplace. They also prey on people who post that they are looking for help finding their lost pet.

The scammers contact you and say they want to buy the item you're selling — or that they found your pet. But before they commit to buying your item, or returning your pet, they seem hesitant. They might say they've heard about fake online listings and want to verify that you're a real person. Or they might say they want to verify that you're the pet's true owner.

The scammer asks for your phone number so that they can text you a verification code. They instruct you to reply with the 6-digit code on the platform where your item is listed.

Sounds reasonable, right? However, here's what's really happening. The scammer is setting up a Google Voice number linked to your phone number. If you send the verification code, the scammer will be able to complete the account setup. The scammer can then use that phone number to conceal their identity. Or, if a scammer gets your Google Voice verification code and other information about you, they can pretend to be you and open new accounts in your name.

If you gave someone a Google Voice verification code, follow these steps from Google to reclaim your number.

- On your computer, go to voice.google.com.
- At the top right, click Settings.
- Under Linked numbers, click New linked number.
- Enter the phone number to link.
- To verify your number, Voice provides a six-digit code:

Hallucinations refer to the errors AI models are prone to make because even though they are advanced, they are NOT human and rely on training and data to provide answers. Training data can lead to factually incorrect or biased answers. This can be a serious problem when people are relying on bots for factual information. Wrong responses can be difficult to spot, particularly as AI technology becomes more pervasive and relied upon.

What's next? Despite the risks, it is unlikely that organizations will stop pursuing AI solutions. AI has shown promise in the pharmaceutical and health fields such as helping geneticists understand how and why genes turn off and on. Policies and guidelines will be increasingly necessary to promote trust and security.

Solomon Adote
Chief Information Officer

- If it's a mobile number, click Send code and Voice sends the code in a text message to the phone.
- If it's a landline number, click the verify by phone link, and then click Call. Voice calls the phone number and gives the code.
- Enter the code and then click Verify.
- If the number is being used by another account, you get a message asking if you want to claim it.
- Click Claim
- The number is linked with your account again.

Don’t share your Google Voice verification code — or any verification code — with anyone if you didn’t contact them first. It's a scam, every time.

Sources: FTC, BBB, Google

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**