FAKE INFORMATION IS GETTING HARDER TO DETECT

BY JAY BORDEN

We all believe we can differentiate between real information and fake information.

However, the number of phishing messages, phishing texts and overall fake information on the web indicates we are not as good as we would like to believe.

Historically, cyberattackers would work to steal credentials or infect a device with malware. Now they use much simpler techniques, phishing or its variants, smishing and vishing. Why attempt to break in if you can get an authorized user to let you in. Of course, most people don't give attackers access knowingly. That is where the fake messages come in.

When people fall for them and click a link or provide their log in credentials, then the attackers have been given a key that opens the door.

Think you can spot a phishing message? Statistics show otherwise. People are considered the source of most breaches. The exact percent of breaches caused by people varies a bit by researcher but falls between 80% - 90% of breaches.

The exact number is less important than recognizing the success of this type of attack.

To make the messages even harder to distinguish, AI is being used by cyberattackers to create ever more believable messages. The attackers run this like a business. They expand use of messages that work and drop ones that don't. AI is being used to not only create the wording of the message, but also to help tune the subject of the message.

Why does it work? Because we aren't as good at spotting fake information as we want to believe.

FAKE INFORMATION IS GETTING HARDER TO DETECT

CONTINUED

Part of the problem can be attributed to work overload. We are all so busy and lack the time to check if something is real. We just click it.

Then there is fatigue. This can be generated by repeated messages being sent to approve a Multi-Function Authorization request. We know that if we receive a request to enter a code it is only because we wanted to get into a site or application. But what if you receive 100 pop up messages asking you to authorize the MFA request? Someone may approve it just to get them to stop.

Regardless of the reason, confirming only one of the MFA requests or other fake messages gives the attackers access to the system using your credentials.

What if the request is a voicemail message from an executive in your company. Isn't that to be trusted? No, it isn't.

All that is need is less than one minute of a person's voice entered into an AI system that can then have the voice say anything you want. This isn't a rare situation or capability. There are over a thousand different services on the web that will do this.

Smishing is the use of text messaging to send the fake messages. How are they sent? Through phone farms. What is a phone farm? It is a location probably in Asia that has a collection of smart phones used just for this purpose. As one example there is a building in Shenzhen, China that locals call the "stolen iPhone building."

Phone farms are also being used to post views on social media then repost or comment to make them seem more popular and believable. It is a powerful way to spread propaganda and sway people's opinions.

It does work. Research shows if we see something often enough, we begin to believe it. That is the purpose of the social media postings. It can influence and shift people's opinions on a topic.

FAKE INFORMATION IS GETTING HARDER TO DETECT

CONTINUED

Part of the purpose of these types of campaigns is to sow enough doubt that people don't know what to believe or trust.

What can we do?
First train people to not trust any unsolicited email with a link in it. No matter who appears to have sent it. Confirm the message using a known contact method, never a link, email, or phone number in the message.

Even if the message is someone's voice, probably an executive of the company, do not trust it. Confirm it using a known contact method.

If MFA confirmation requests start bombarding you, do not click to approve them. Report it to your IT department. Let them handle it.

In the case of social media and sensitive issues, do not trust what you read. No matter how many "people" say it or support it online.

Knowing what is going on can help you stay safer.

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.