AI INSPIRED BANK SCAMS

BY JAY BORDEN

Bank scams are an old stand by for cybercriminals. Banks are where the money is and people are the cause of most of the breaches.

Now the cybercriminals have gotten a new helper, Artificial Intelligence, AI. New research indicates AI was used in almost half of the bank scams. Why? Because it makes them more successful.

How do many bank scams start? With a convincing email or text or phone message. This is an area where AI shines as it writes very convincing letters, emails, and messages.

The targets are people and companies. Cybercriminals will take anyone's money. Always be wary of any message that wants your private information. The FBI warns never click a link in an email or text.

Another aid are the improvements in transaction processing speed, especially faster transfers out of the country. Less time to catch suspicious activity. Once the money is out of the country it is almost impossible to trace or to recover.

How big are bank scams? In 2023, the last full year of data, the Federal Trade Commission said consumers reported over $10 billion lost in fraud, 14% higher than the prior year. There is no way to know how much wasn't reported.

Even if the $10 billion represents it all, that is a staggering number. Breaking it down:

- $4.6 billion was investment fraud
- $2.7 billion was imposter fraud.

It is pervasive, over 25% of bank customers reported fraud on their accounts.

AI INSPIRED BANK SCAMS

CONTINUED

How exactly is AI helping cyber attackers? With deepfakes, more credible phishing messages, and by tuning the message to the target quickly and easily.

Deepfakes are pictures, videos or voice messages that appear to come from someone authorized to request your credentials or initiate wire transfers, etc.

In a real example a deepfake video call was used to convince an employee to wire $25 million. Of course, it was really sent to the perpetrators of the fake video call.

With one hundred words or less and a short video of a person, AI can make that person say anything, and it is good enough to fool many people.

Now scammers have made their AI systems available to other scammers for only $50 a month. Puts it in almost anyone's reach.

Phishing is one of the most successful tools of attackers. What makes them successful? The credibility of the message.

Scammers have gotten reasonably good at it. But AI bumps it up. If the AI system can be fed memos or emails or videos of the supposed sender it can duplicate the style and language. Real samples are readily available from public sources. Videos of speeches, memos or letters. even their social media posts.

Even without having the words of the person, AI will find the types of language and word order people at that level tend to use. It may not be as good as if they have the samples but all they need do is fool one person.

Fraud detection systems rely on errors, anomalies, things being different from what is expected. But the AI systems reduce that to the point where the fraud detection systems allow the message through.

Experts are saying that the losses from fraud in the United States alone may grow to $40 billion by 2027. That is incredible growth. Even if the predictions are off by 50%, that still means fraud losses will grow from $10 billion to $20 billion!

AI INSPIRED BANK SCAMS

Continued

What can you do?

Know the most common types of fraud messages.

Messages or phone calls that appear to come from your bank saying there has been suspicious activity on your account. Of course, you will be asked for private information to prove you are the account owner.

You may receive a check and then be asked to return part of the check amount, so the check won't bounce. The attackers tell you it will be replaced. But if you send the money the original check will bounce, and you will never see anything else. The funds you sent are now gone.

Another way are emails or phone calls from people you would trust, your IT support team, company executives, bank officers, government officials or others. Here again you would be asked to prove your identity.

Fake investment scams are also popular. Everyone invests to make money. You would be presented with an offer that has a high rate of return. Remember the old adage, if it sounds too good to be true, it probably is. Very apropos here.

For those without money to invest and who may have poor credit, the lure is a loan on terms more favorable than they may get elsewhere.

Remember people are the cause of over 80% of breaches and AI will probably push that figure higher.

Learn how to recognize fakes and how to authenticate calls, emails or messages.

Stay alert and good luck.

Visit our site, onebrightlycyber.com to learn all the ways we help keep you safer.

Welcome to peace of mind.