FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, April 18, 2025

How to Fight AI-Boosted Spear Phishing Fraud

Source: Independent Banker

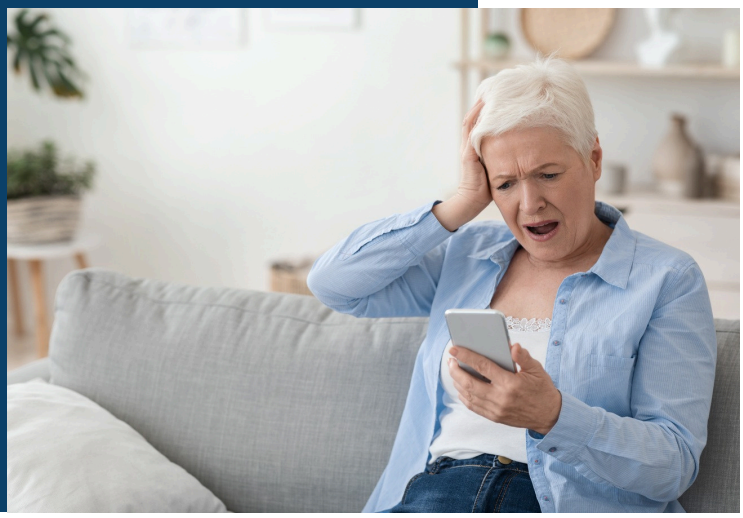
Artificial intelligence has streamlined spear phishing, a kind of cyberattack involving emails, video calls or other forms of communication facilitated by fraudsters posing as a trusted colleague, boss or organization. Here's how your community bank can hit back.

In 2023, an employee of multinational design and engineering company Arup thought he was just doing what he was told. During a video call, the chief financial officer directed him to transfer $25 million to a specific account. Except it wasn't really the company's CFO. Instead, it was a deepfake created by hackers to trick the Arup employee. Not only did the hackers spoof the CFO's image and voice; they also created digital replicas of fellow employees to commit this fraud.

(*Click the heading link to read more.*)

Top News

- How to Fight AI-Boosted Spear Phishing Fraud
- Is That Unexpected Text a Scam?
- Jackpot! How Banks Can Prevent ATM Attacks
- How Can Generative AI Be Used in Cybersecurity
- New FTC Data Show Top Text Message Scams of 2024; Overall Losses to Text Scams Hit $470 Million



Is That Unexpected Text a Scam?

Source: Federal Trade Commission

Did you know that people almost always open text messages? In a new Data Spotlight about the big jump in reported fraud losses involving text scams, the FTC notes a study finding open rates can be as high as 98%. Those are really good odds for a scammer. And when scammers get you to respond to their messages, they're cashing in. Here's how you can increase your chances of keeping your money safe.

Some text scams start as fake fraud alerts. You get a message from someone claiming to be from the fraud department with Amazon or your bank, offering to help with a suspicious charge. But that's the hook they use to get you to respond by messaging back or calling a number. Instead of help, they'll spin elaborate lies and drain your bank account.

Or maybe you get a text about a problem with a delivery or a message about unpaid tolls. In both cases, they tell you to click a link to fix the issue. When you land on what seems to be the USPS or highway toll program website (they're not), they tell you to pay "re-delivery fees" or "unpaid tolls." That's when you might end up giving your credit card or even your Social Security number to a scammer.

(*Click the heading link to read more.*)

Jackpot! How Banks Can Prevent ATM Attacks

Source: Bank Director

So-called ATM jackpotting attacks are on the upswing, and smaller banks are particularly susceptible to losing money to these crimes.
In February, police in Florence, South Carolina, extradited a New York man for allegedly stealing almost $100,000 in an ATM jackpotting attack on Oct. 9, 2024. In early March, U.S. attorneys in Buffalo, New York, charged two men with bank theft and conspiracy to commit bank theft for stealing nearly $300,000 across several ATM jackpotting attacks in October and November 2024, according to a news release. The targets in the attacks were small banks and credit unions.
ATM jackpotting schemes "are typically being done by organized crime groups," says David Tente, executive director, USA and Americas with the ATM Industry Association. "It's not the kind of attack you would see from the novice who wakes up and decides to steal an ATM."
Jackpotting manipulates a machine's cash dispenser so it discharges all the money inside the ATM. A thief typically uses a standardized master key, easily purchased online, to open the ATM. They then install an infected hard drive or malware that allows a hacker to take control of the machine and withdraw all its cash, unconnected to any bank account.

(*Click the heading link to read more.*)

How Can Generative AI Be Used in Cybersecurity?

Source: Endeavor IT

Generative AI in Cybersecurity
As cyber threats grow in sophistication, the intersection of artificial intelligence (AI) and cybersecurity has become a crucial area of focus. Among AI advancements, generative AI stands out as a game-changing tool with immense potential to enhance cybersecurity measures. But how can generative AI be used in cybersecurity to safeguard networks of all sizes? Let's explore the key ways generative AI is transforming the cybersecurity landscape while also addressing its challenges and limitations.

What is Generative AI in Cybersecurity?
Generative AI refers to AI models designed to create new data based on patterns identified in existing datasets. Popular examples include OpenAI's ChatGPT and advanced image-generation tools. While generative AI is often associated with creative tasks, its capabilities extend into cybersecurity, where it bolsters both defensive and proactive measures. By analyzing and generating patterns, generative AI enhances threat detection, automates responses, and supports simulation-based training.
Key benefits of future generative AI in cybersecurity include:

- **Advanced Threat Detection:** Identifying sophisticated attack patterns and uncovering vulnerabilities.
- **Automated Security Responses:** Delivering faster and more efficient responses to security incidents.
- **Data Simulation and Training:** Creating synthetic datasets for testing and refining security systems.

(Click the heading link to read more.)

New FTC Data Show Top Text Message Scams of 2024; Overall Losses to Text Scams Hit $470 Million

Source: Federal Trade Commission

New data from the Federal Trade Commission show that in 2024, consumers reported losing $470 million to scams that started with text messages. This amount is five times higher than what was reported in 2020, even though the number of reports declined.
The most commonly reported type of text scam was fake package delivery, where scammers send alerts about a supposed issue with an incoming delivery. Bogus job opportunities were also common, including "task scams," which involve promises of online work requiring people to complete a series of online tasks and end up with requests for people to invest their own money.
Other text message scams reported frequently were fake "fraud alert" messages sent to consumers warning about a suspicious purchase or an issue with their bank; warnings about fake unpaid tolls with a link to pay them; and "wrong number" scams that start as a seemingly misdirected message. Wrong number scams often evolve into a conversation with romantic undertones that can lead to investment and other scams.
The spotlight includes advice for consumers on how to handle text message scams, including:
Forwarding messages to 7726 (SPAM). This helps your wireless provider spot and block similar messages.
Reporting on either the Apple iMessages app or Google Messages app for Android users.
Reporting to the FTC at ReportFraud.ftc.gov.

(Click the heading link to read more.)