FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, February 7, 2025

Customers Want Extra Security That Can Stop Fraud Deepfakes

Source: BAI Bank Strategies - Executive Report

Deepfakes by fraudsters are on the rise—but financial institutions can catch them before accountholders are violated.

Deepfake images and video with increasingly realistic attributes can be used to circumvent identity verification and authentication methods when opening bank accounts or taking out credit. And it's a financial crime made easier with the advent of generative artificial intelligence (gen AI) tools, according to a November alert issued by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN).

FinCEN's alert explains typologies associated with the latest deepfake schemes and provides red flag indicators to assist with identifying and reporting related suspicious activity.

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

Top News

Educate Employees on Risky Behavior

Source: CBM Preferred Partner SHAZAM

In any given workplace, it's common to see sticky notes stuck to computer screens or other highly visible locations in an employee's workspace. The notes typically contain reminders or bits of important information the employee needs to remember.

In many work environments, these types of reminders are harmless. However, in a financial institution, they can result in a serious breach of security. When the sticky note contains a customer's name or other identifying information, the employee may be unknowingly enabling a data breach.

Some other examples of common employee-oriented risk include an unsecured, financial institution-issued employee computer loaded with customer information; improper disposal of sensitive documents; and accidentally emailing or mailing documents with personal information to the wrong recipient.

Below are a few important steps financial institutions can put into practice in an effort to protect sensitive information and potentially cut down on data breaches:

- Consider your financial institution's most vulnerable points: Performing a security assessment will help identify weaknesses, as well as bring to light any activities (intentional or unintentional) that could potentially lead to a data breach.
- Amp up security and protection for high-risk areas: Implement additional access controls and security measures where needed.
- Educate employees about security best practices: Provide employees with the knowledge, resources and strategies necessary to successfully adhere to security policies and procedures. Keep security top of mind with regularly published reminders of appropriate guidelines to follow.
- Train employees on proper reporting procedures: Be sure employees know and understand what constitutes a data breach, as well as whom to notify and how if they witness a breach or spot a vulnerability that could lead to one.

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

A New Resource For Fighting Fraud

Source: ICBA Independent Banker

The rise in fraud has become one of the biggest concerns for community banks and their customers in recent years. Fraud has a serious bottom-line impact on banks, and it hits customers in a very personal way, all of which goes against the ethos of community banking.

Fortunately, community banks know their customers exceptionally well and are therefore uniquely positioned to help prevent and detect fraud on the front lines.

At ICBA, we understand the gravity of frauds and scams and their impact on customers. In this new column, we'll be looking at ways to make this fight easier. We'll be tackling issues including:

- Debit card fraud
- ATM fraud
- Impersonation scams
- AI-assisted fraud and scams
- Cryptocurrency scams
- Phishing, smishing and vishing (cyberattacks using social engineering, SMS messages and voice calls respectively)

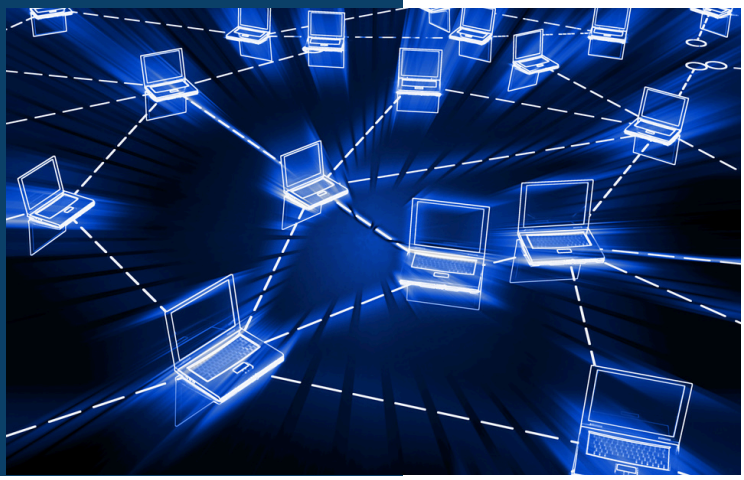
We'll be giving you critically important, new information and resources, so that you can build protection for your customers and promote resilience within your communities.

Check fraud

This year, ICBA has addressed check fraud in some depth, and if you've missed our reports, you can visit our website at icba.org for some valuable resources. Start by downloading our guides:

- Check Fraud: A Practical Guide to Altered, Forged, and Counterfeit Checks for Community Bankers
- Check Fraud: Detection Mechanisms
- Check Fraud: Engagement with Federal Bank Regulators

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



It's Time to Bolster Cybersecurity Measures - Now and Forever

Source: ICBA Independent Banker

Cyberattacks are becoming more sophisticated, and banks face increasing regulatory pressure to strengthen their cybersecurity strategies. Meanwhile, the cost of a data breach is skyrocketing.

Last year, the average cost of a data breach in the U.S. was $4.88 million, up from $4.45 million the previous year. This represents a 10% spike in breaches—the highest increase since the global pandemic, according to IBM.

Community banks are feeling the effects of the changing regulatory landscape and growing customer data privacy concerns. As a result, ICBA members are prioritizing cybersecurity as a strategic imperative. They are improving security measures, providing additional employee training, and staying ahead of the latest threats and trends.

More than just due diligence

As pillars of their communities, ICBA members must approach cybersecurity on an around-the-clock basis. After all, the bad actors never sleep; they're constantly coming up with new ways to infiltrate systems, exploit them, steal their data and use it for nefarious purposes. Being forever vigilant is essential and can't be overlooked. Vigilance must become a part of your bank's culture.

It's important to note that not every data breach or cyberattack is overly sophisticated. In fact, many of them can infiltrate through fairly innocent means. For example, the employee who doesn't understand the danger of opening a phishing email from an unknown source can unwittingly wreak havoc on the bank's systems, databases and customer data. Banks can reinforce the importance of recognizing and avoiding phishing attempts by investing in regular cybersecurity awareness training.

(Click the heading link to read more.)

What's In A Name? When It Comes To Malware, A Lot.

Source: PCBB The BID

Melissa is malware that attacks Microsoft Word and Outlook. You might wonder why its creator chose that name. Cyber lore has it that he named his malicious piece of handiwork after a stripper he knew in Florida.

Malware and other cyber threats tend to have less racy origins than Melissa. Yet, there are so many swirling around these days that you could be forgiven for having trouble keeping track of the latest named threat that your IT team is warning you about. The world is beset by cyber threats, each with its own unique new name. While those names can seem arbitrary, many are actually communicating a great deal of information.

So, how do all these worms and bots get their names, and what is the significance of each name? Some basic conventions on threat names have developed over time. The people who coin the names try to follow these conventions so that a name suggests the type of threat it poses. There are exceptions, though, like Melissa, which is more of a ribald boast by its creator than anything else.

Why Names Are Important

If you understand the naming protocols, you can get an idea of the nature of a threat. Names for threats like malware and ransomware tend to follow a few rules or standards that help categorize them (e.g., function, method, or origin). Understanding the nature of risks being posed by a named threat can thus help prioritize your response.

(Click the heading link to read more.)