FRAUD PREVENTION FRIDAY

IBSC

Independent Banks of South Carolina

Friday, April 4, 2025

Top News

- Getting The Word Out About FTC Imposter Scams
- Proactively Fight Banking Fraud to Fuel Growth
- Malicious Cyber Actors Use Buffer Overflow Vulnerabilities to Compromise Software
- Is Behavioral Biometrics the Future of Fraud Protection?

Getting The Word Out About FTC Imposter Scams

Source: Federal Trade Commission

Using old tactics and new twists, scammers are impersonating government agencies, including the FTC, to try to steal people's personal information and money. The FTC is committed to combatting these imposter scams, and there's encouraging news these efforts are making a difference to American consumers.

Every day, we're working to increase awareness about FTC imposter scams by giving people practical information when and where they need it — like the FTC's anatomy of an imposter scam blog series. We take it seriously when scammers claim that the Chairman of the FTC is on the line to help you get out of a bind or that you're being charged with serious crimes. No one at the FTC will call, email, or text you to say any of those things. That's why you'll find clear warnings across the FTC's website, on our homepage, on the bio pages for FTC commissioners and officials:

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. If you have been targeted by an illegal business practice or scam, report it.

These warnings are getting noticed and making a difference, but you don't have to take our word for it. Listen to people who — in the middle of a conversation with a scammer pretending to be from the FTC — stopped and searched for the FTC online.

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

Proactively Fight Banking Fraud to Fuel Growth

Source: BAI

More than 75% of banks report increases in consumer fraud, with 25% facing losses of $1 million or more. Meanwhile, consumers have experienced over $10 billion in cumulative fraud losses. Your bank is already under pressure with rising deposit costs, intense competition from interest rates, and high customer expectations for a seamless digital experience. And now, the impact of increased fraud adds another layer of complexity to the mix.

But there is a way forward.

With the right solutions, you can do more than protect your bank and customers from fraud—you can build trust and cultivate deep online relationships. Advanced fraud protection doesn't just safeguard against risk; it enhances your bank's relationship with customers. This can lead to more deposits, a stronger reputation as a secure and reliable bank, and a foundation for long-term success.

In this article, we'll explore the riskiest step in the customer journey, its potential impact, and actionable strategies to navigate it successfully. You'll also discover how strong fraud defenses can complement your growth strategy, transforming security and seamless digital experiences into a key competitive advantage.

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

Malicious Cyber Actors Use Buffer Overflow Vulnerabilities to Compromise Software

Source: Cybersecurity & Infrastructure Security Agency (CISA)

Buffer overflow vulnerabilities are a prevalent type of memory safety software design defect that regularly lead to system compromise. The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) recognize that memory safety vulnerabilities encompass a wide range of issues—many of which require significant time and effort to properly resolve. While all types of memory safety vulnerabilities can be prevented by using memory safe languages during development, other mitigations may only address certain types of memory safety vulnerabilities. Regardless, buffer overflow vulnerabilities are a well understood subset of memory safety vulnerability and can be addressed by using memory safe languages and other proven techniques listed in this Alert. Despite the existence of well-documented, effective mitigations for buffer overflow vulnerabilities, many manufacturers continue to use unsafe software development practices that allow these vulnerabilities to persist. For these reasons—as well as the damage exploitation of these defects can cause—CISA, FBI, and others[1] designate buffer overflow vulnerabilities as unforgivable defects.

CISA and FBI maintain that the use of unsafe software development practices that allow the persistence of buffer overflow vulnerabilities—especially the use of memory-unsafe programming languages—poses unacceptable risk to our national and economic security. CISA and FBI urge manufacturers to use proven prevention methods and mitigations to eliminate this class of defect while urging software customers to demand secure products from manufacturers that include these preventions.

(Click the heading link to read more.)

Is Behavioral Biometrics the Future of Fraud Protection?

Source: PCBB - BID Daily Newsletter

Traditional physical biometric methods — such as fingerprint or facial recognition — make users undergo a one-time authentication process. In contrast, behavioral biometrics confirms a user's identity by continuously tracking and analyzing their behavior and how they interact with their devices in real time, thereby allowing for continuous authentication.

- Behavioral biometrics focuses on various behaviors, including a user's:
- Typing patterns (speed, rhythm, pressure, shortcuts)
- Mouse movements (how and the speed at which it's moved and clicked)
- Touchscreen interactions (pressure, location, and gestures used)
- Smartphone orientation (landscape or portrait)

As these patterns are unique to every individual, they create a "behavioral profile" that can be seamlessly and continuously analyzed and monitored in the background using artificial intelligence (AI) and machine learning (ML).

This real-time analysis helps detect unusual activity patterns — such as significant changes in typing speed or irregular touchpad movements — and can raise an alert for possibly suspicious behavior. The system can then trigger the need for additional verification steps, delay a transaction until more information is provided, or even freeze an account to prevent fraud as early in the process as possible. Preliminary research shows behavioral biometrics have a 90% effectiveness in identifying and preventing money mule activity.

(Click the heading link to read more.)