FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, June 13, 2025

The Cost of Compromised Emails

Source: SHAZAM Blog

Business email compromise, also known as email account compromise, is one of the most financially damaging cybercrimes. Americans lost $2.77 billion to cybercrimes directly related to BEC, according to the 2024 Internet Crime Report released by the FBI Internet Crime Complaint Center.

Since email is a primary way of conducting both personal and professional business, it's important to be diligent about these threats when using any email account. The good news is there are ways to protect yourself, your financial institution and your accountholders.

BEC emails are created to look like they're coming from a legitimate organization or person. Their goal is to have the unsuspecting recipient share sensitive personal and financial information that can be used to gain access to personal financial accounts or an organization's network. These emails play on people's emotions by creating a sense of urgency or appearing from a trustworthy source to trick people into giving up information criminals want.

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

Top News

Confidence Scams: What They Are and How to Protect Your Customers

Source: Federal Reserve Community Banking Connections

Financial risks related to confidence scams are growing, and scammers are taking advantage of newer technologies that increase risks. Confidence scams involve bad actors who engage in fraudulent activities that are designed to take advantage of a person's trust. Technology makes it easier for bad actors to impersonate trusted sources, and digital currencies and prepaid cards allow scammers to mask the movement of stolen funds, making it more difficult for victims' funds to be retrieved. This article discusses ways to increase community bankers' awareness of the various types of confidence scams and provides resources for bank staff and customers dealing with the consequences of such scams.

There are multiple databases that maintain information on confidence scams (see Common Types of Confidence Scams). Several federal government agencies maintain databases on consumer fraud, such as the Federal Trade Commission (FTC) Consumer Sentinel Network Data Book (Sentinel Data Book) and the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). The Consumer Financial Protection Bureau (CFPB) also collects information on incidents of fraud that shows a greater and increasing number of reported fraud cases, including confidence scams.

According to the Sentinel Data Book, the FTC received over 2.5 million reports of consumer fraud in 2023.

(Click the heading link to read more.)

Banks Struggle to Talk About Fraud

Source: Payments Dive

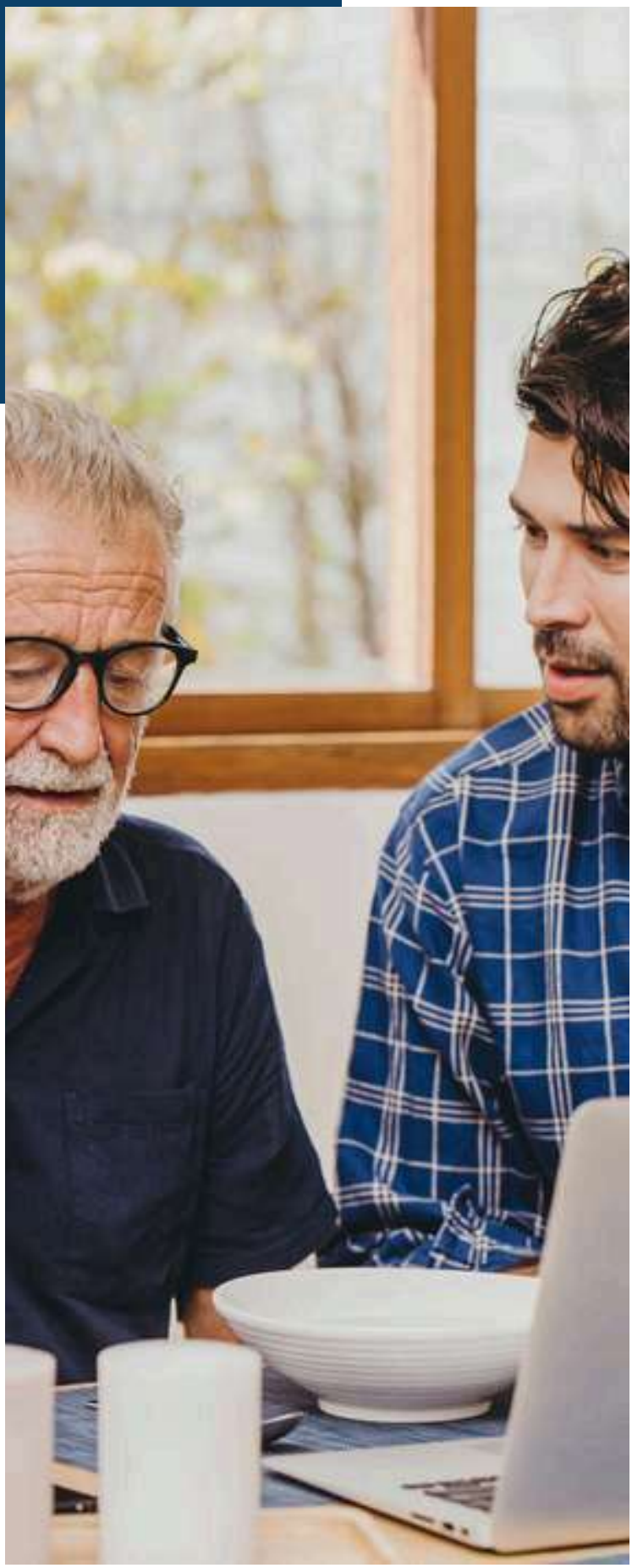
Community banks can strengthen their defenses against push-payment scams by establishing a fraud prevention network, hosting regular meetings, and utilizing secure communication channels to share scam-related insights. By collaborating with law enforcement and regulators, developing a shared fraud alert system, and educating customers collectively, banks can take a proactive stance against fraud. Additionally, participating in the CBM Risk Fraud Forum allows community banks to openly discuss scams that have impacted their institutions, exchange best practices, and stay informed about emerging threats, fostering a united front against financial fraud.

The following article discusses financial institutions' struggles to share information that might help them better protect customers, as discussed at the Nacha Smarter Faster Payments conference held in April.

Financial institutions are facing a flood of fraud, from push-payment scams to business email compromises to bad checks. Nonetheless, they're often stymied in trying to work together to root out bad actors.

That was painfully clear to attendees listening to several panel discussions at the Nacha Smarter Faster Payments conference last month. The industry event attracted about 2,100 payments, bank and credit union professionals between April 27 and April 30 in New Orleans.

(Click the heading link to read more.)



Phishing Threat Trends Report

Source: KnowBe4

The KnowBe4 Phishing Threat Trends Report can help community bankers to bolster their cybersecurity posture and stay one step ahead of phishing threats. With ransomware threats evolving and AI-driven phishing campaigns becoming more sophisticated, it's critical for banks to go beyond native security tools and traditional email gateways. By understanding how attackers bypass these defenses and infiltrate hiring processes, bankers can prioritize continuous employee training, simulate phishing scenarios, and adopt advanced email security solutions. Staying informed and proactive will help safeguard customer trust and financial data in an increasingly complex threat landscape.

The KnowBe4 Phishing Threat Trends Report brings you the latest insights into the phishing landscape, whether that's emerging attacks or techniques that are starting to gain traction, or new intel on established threats.

In this edition, they look at how the "old" threat of ransomware continues to grow and walk through the "new" sophisticated tactics that cybercriminals layered into an attack detected by KnowBe4 Defend. These tactics enabled it to bypass native security and a secure email gateway (SEG), and would make it virtually impossible to stop if it had launched.

Elsewhere, they continue to highlight how cybercriminals are using AI to architect polymorphic phishing campaigns; how they're injecting themselves into the hiring process to gain access to systems and data; and the attacks making it through native security and SEGs.

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