First Bank & Trust Company

The Bank That Puts You First

Member FDIC

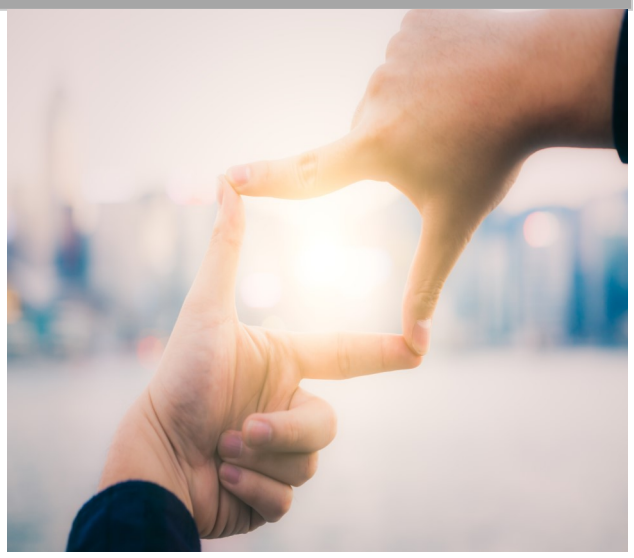
Member FDIC

EQUAL HOUSING LENDER

January 2022

Top 10 Fraud Trends in 2022

An exponential increase in the number of digital accounts and subsequent online activity will fuel attacks with greater severity in 2022, across digital touchpoints



What a year 2021 has been! Nothing short of a roller coaster. The resurgence of the Covid-19 virus in many parts of the world has brought back curbs and restricted many offline activities once again. Digital continues to be the preferred mode of working, entertaining, socializing, shopping, and a host of other daily-life activities. Digital payment methods, including BNPL (buy now pay later) and cryptocurrency platforms, rose in popularity, with fraud and online abuse following suit in abundance. No industry was spared and fraud losses amounted to billions of dollars.

Attacks will continue to rise in 2022 with even more sophistication. This, however, does not mean typical attacks will become outdated. Instead, attackers will sharpen their tactics and leverage advancements in automation to scale the attacks with tried-and-tested techniques for greater financial returns.

Here are our predictions for the top fraud trends and cybersecurity movements that will continue to plague digital businesses in 2022:

1. Automation:

Automation will continue to play a central role in attacks such as credential stuffing, password spraying, and brute-forcing. Fraudsters need fewer investments to scale attacks when they use bots and automation. Further, bot technology has advanced to the point today that bots can mimic humans fairly accurately, which causes bot detection to be even more difficult for businesses. Availability of commoditized botnets-as-a-service and the required support will make automation an even more potent tool for legitimate businesses to defend against in the coming year.

2. Account Takeover:

Account takeover (ATO) attacks have grown leaps and bounds over the last few years – thanks to an explosion in the number of digital accounts – as more and more people turned to digital channels for daily life activities. This increase in digital accounts combined with incessant incidents of data

Continued on page 2

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-266-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
Lebanon, Virginia East
276-889-3401
Lebanon, Virginia West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton, Virginia
276-679-7401
Staunton, Virginia
540-885-8000
Verona, Virginia
540-248-7700
Waynesboro, Virginia
540-943-5020
Wise, Virginia
276-328-3439
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan
Production Offices
Bedford, Virginia
540-583-5458
Daleville, Virginia
540-966-7006
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust
Mortgage Lending Division
Bristol, Virginia
276 -644-9900

breaches will continue to provide attackers with the required raw materials to launch account takeover attacks. High returns and ease of execution will continue to drive the rise of account takeover attacks well into 2022.

3. Crypto Attacks:

The popularity of digital payments including cryptocurrency platforms has increased cyber threats to fintech companies a notch higher. Fraudsters increasingly will improvise on phishing and social engineering to target cryptocurrency platforms, during 2022. The use of malware for crypto-jacking and infecting the system to enable mining of cryptocurrency will evolve into a bigger threat.

4. Phishing:

With numerous spelling errors, faulty language, and unbelievable claims, it was fairly easy to identify a phishing email three to five years ago. However, over the years, phishing emails and URLs have become more refined and believable, which helps scammers execute hyper-targeted attacks. In the coming year, scammers will continue to spend time improving their phishing tactics by making them more personalized and specific.

5. Targeted Attacks:

In 2021, we saw a diversification of attacks and a rise in attacks that were especially designed to target specific industries. Attackers have studied the prevalent fraud defenses across several industries. They will use this knowledge to maneuver their resources and extract maximum returns from these attacks.

6. Ransomware:

Ransomware will be a preferred tool for targeted attacks, especially against the payment service providers (PSP). This trend will affect all partners in the payment ecosystem globally. This is not to suggest other industries are safe from these attacks. It is likely that attackers will increase the amounts of ransom demands in 2022.

7. Cyberactivism:

An online version of real-world protests, cyberactivism is on the rise. Protesters engage in disrupting the websites of target businesses. Fraudsters can game web-authentication measures to take advantage of such protests and exploit loopholes in business networks. They can use these protests as a means to drop malware or ransomware to steal sensitive information or to extort money.

8. IoT-driven Attacks:

The number of IoT-connected devices is expected to cross the 25.4 billion mark by 2030. Inherently, IoT devices are not that secure and are, therefore, vulnerable to an increased threat of cyberattacks. Senior-level security executives say that IoT security is a significant threat that they are still trying to get their arms around. To make matters worse, generally consumers do not change the default passwords which makes these smart devices more susceptible to account takeover attacks.

9. Supply Chain Attacks:

The ongoing disruption in supply chains is an opportunity that attackers will try to take greater advantage of in 2022. SolarWinds, Codecov, and Kaseya are still fresh in our memory. We expect an increase in similar attacks that can be used to harvest sensitive data or infect systems with malware. This will fuel the need for greater government regulations.

10. Account Security:

In the wake of rising fraud and online abuse, digital businesses will focus their attention on the account security of the customers. Comprehensive account security will be on top of the priority list of fraud teams and they will look beyond the traditional castle-and-moat method to verify user identities. A tiered approach to web authentication of users will become popular.

Fraudsters are in the business of making money and the coming year will be no different. The attacks, however, will be more sophisticated in technique and strategic in approach, such that they can reap maximum returns with the least possible investments. Attackers will also look for the path of least resistance and will exploit loopholes in business networks – whether external or internal. Furthermore, since they have invested time and resources to understand the current fraud defense mechanisms, attackers will use this knowledge to counter them.

In 2022, businesses must remain aware of the shifting risks they face and take appropriate measures to protect themselves and their consumers. To counter a technologically superior opponent, digital businesses should also leverage the power of the latest technology. Think in terms of deterrence, not just mitigation.

Source: Security Boulevard, Vanita Pandey, December 20, 2021

Robocalls are still out of control -- and aren't likely to stop in 2022

The US Federal Communications Commission upped its game in 2021 when it came to fighting illegal robocallers. But experts say the battle to end robocalls is far from over.

The FCC's deadline to implement technology to beat back annoying robocalls went into effect over the summer. As of June 30, every major voice provider in the US, including phone companies AT&T, Verizon and T-Mobile and cable provider Comcast, was required to implement a technology, called Stir/Shaken, designed to curb the tide of spam calls by requiring voice providers to verify where calls are coming from. And in December, the agency moved up the deadline for many smaller providers to comply with this technology.

But even though the crackdown has helped dampen the calls, scammers are back at work looking for ways to trick Americans into picking up the phone and handing over money.

"Stir/Shaken has shut down one avenue," said Clayton Lia-Braaten, senior advisory board member at Truecaller, which makes a spam-blocking and caller ID app. "But it's making already very capable criminals even more sophisticated and sinister in their scams."

To help you get a handle on what Stir/Shaken has meant so far and what's next in the effort to stamp out robocalls, keep reading.

Where are we now?

The hope of Stir/Shaken was that it would finally curb the flood of spam calls involving health-related scams, expiring car warranties that don't exist and fake banks offering bogus interest-rate discounts for credit cards. For years, the scourge of illegal robocalls has plagued the public. It's the No. 1 consumer complaint and a top priority at the FCC.

Since a peak in March 2021 when Americans got 4.9 billion robocalls, Stir/Shaken has helped curb the number of robocalls, according to YouMail, a company specializing in blocking robocalls. In November that figure was down to 4.1 billion calls for the month, YouMail said. Still, the volume of robocalls is rising again, and Americans are getting more than they did in November 2020, when 3.8 billion robocalls set phones ringing and buzzing.

YouMail predicts that Americans are on pace to receive about 51 billion robocalls by year's end, up from 46 billion in 2020.

Like a game of whack-a-mole, whenever regulators or law enforcement smack down one way that robocalls are made, scammers change tactics and use a different method. Experts say that's what is happening now as robocallers move away from using spoofed phone numbers made to look like a call is coming from a neighbor. Now they're buying lists of real phone numbers to trick spam-blocking software into letting the calls through. The problem is that buying lists of phone numbers from third-party data providers is legal, which makes it difficult for law enforcement to figure out who is buying these lists and using them for nefarious purposes.

What's Stir/Shaken?

Stir/Shaken is a technology that ensures calls traveling through phone networks have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before the calls reach you. In short, the technology authenticates a phone call's origin and makes certain the information on the caller ID matches.

The FCC is continuing to address the issue, with new regulations voted on in October. The new FCC requirements would ensure that the gateway providers are verifying calls before they pass them on to other operators in the states.

Source: CNET.com, Marguerite Reardon, Dec. 23, 2021 8:00 a.m. PT