Spot the Impostor

Tackling the Rise in Social Engineering Scams

BioCatch

WHITE PAPER

Executive Summary

At the heart of every cyberattack is an element of social engineering. From more common attacks, such as phishing, to more sophisticated attacks, such as authorized push payments and phone scams, criminals have impersonation of our most-trusted institutions down to a science. Well-crafted schemes carry all the signs of legitimacy, using personal details collected from the dark web, data breaches, and social media, that can catch even the most cautious individuals off-guard. Social engineers learn bank security practices and processes, capitalize on events in the news, and target the most vulnerable to achieve shocking success.

Social engineering scams are on the rise worldwide. According to the U.S. Federal Trade Commission, impostor scams continue to be the number one type of fraud reported by consumers resulting in over $2.3 billion in losses in 2021. Nearly £250 million was lost to authorized push payment scams in the first half of 2022, and top UK bank Barclays reported a 20% increase in impersonation scams[1]. In Australia, there were over 239,000 scams reported by consumers resulting in over $570 million AUD in losses last year, according to Scamwatch.

The challenge with detecting many social engineering scams is that the criminal does not interact directly with the banking platform and instead convinces the victim to execute the payment themselves. Traditional device, IP and location-based authentication controls will thus appear genuine. Even in cases where risk is detected and step-up authentication is required, such as out-of-band SMS OTP, the challenge will be passed because a legitimate user is performing the transaction. Legacy-based fraud prevention measures are no longer a match on their own for criminals who have learned to easily spoof them, and new approaches that provide deeper visibility into risk across a digital session are required.

This white paper will examine the recent outbreak of social engineering scams around the globe, how government and industry are responding, and how behavioral biometrics is helping financial institutions protect their customers from falling victim to these attacks.

[1] Reuters, From romance scams to phantom PPE, banks battle coronavirus crimewave, December 2020

Common Social Engineering Scams

Social engineering is at the root of almost every cyber attack. In the financial industry, there are three main types of social engineering:

Information harvesting

Real-time payment scams

Remote access tool (RAT) scams

The main goal of most social engineering schemes is to harvest personal or financial information from a victim that can be used at a later time to commit fraud. Information harvesting starts with a communication to a victim, typically via a phishing email or SMS messages, creating a situation that leads the victim to believe they should input their personal data. Phishing is the oldest form of social engineering since the advent of the Internet, and it still remains the most common. However, in recent years, phishing via SMS message, or smishing, has become far more prevalent based on studies that show consumers are more likely to respond to a text message. According to research by MobileMarketer.com, SMS recipients open 98% of their text messages while email recipients only open about 20% of their messages.

The second type of social engineering, and much of the main focus of this paper, is related to real-time payments. These scams involve impersonation of a variety of types from falsely representing an official from a bank, government agency or other trusted organization to romance, investment and lottery schemes. Impersonation scams seek to elicit an emotional response from a victim in the hopes of getting them to initiate a real-time payment to an account controlled by the criminal. Information harvesting is often directly tied to impersonation scams. Whether gathered through an attack or purchased on the dark web, the more information a criminal knows about a person, the more likely it is the victim can be successfully swindled. Authorized push payment fraud is a well-known type of impersonation scam that is rampant in the UK.

> Banks in Latin America saw the most profound impact of social engineering scam fraud in 2022 – a 156% increase.

Identifying real-time payment scams is often difficult since the criminal does not interact directly with the banking platform and instead convinces the victim to execute the payment themselves. As a result, legacy fraud detection tools struggle to detect these attacks since the device is a user's trusted device, the network connection matches the known user profile, and any second-factor authentication challenge would also pass since the victim possesses the device to which any OTP code will be sent.

Finally, scams that involve the use of remote access tools (RAT) typically rely on social engineering to get a victim to download software that enables a criminal to take over their device and initiate a payment.

The Outbreak of Social Engineering Scams

The coexistence of 'traditional' online banking fraud and more advanced social engineering scams is a key trend that must be monitored carefully in order to define the best approach to preventing fraud and protecting customers. As banking security measures have become more stringent, criminals have turned to targeting the weakest link: the human.

The increase in scams is supported by both industry data and among cases reported as fraud by BioCatch's global customer base. In 2022, BioCatch customers collectively reported a 30% increase in social engineering scams, and nearly 80% originate in the mobile channel. This trend was most profound in Latin America which experienced a 156% increase.

The dollar value of potential loss associated with social engineering scams is often much higher as well due to the nature of the attack. In a manual account takeover, criminals often opt for lower value and higher volume of payments in order to avoid raising red flags with the financial institution. However, with an impersonation scam where the genuine user is conducting the transaction, criminals will take more risk and attempt to coerce a victim into making payments in higher amounts. Last year, 43% of all impersonation scam cases had an amount greater than $1,000 USD. A breakdown of payment values associated with scams is listed below.

Protecting Scam Victims: How Government and Industry are Responding

While senior citizens have been thought to be the most vulnerable to these scams, younger customers who value convenience over privacy are increasingly falling prey. The growth of social engineering scams in recent years has forced both government and industry to pay more attention to the issue of liability and customer reimbursement. In 2022, the issue of involving the receiving bank in the reimbursement of select financial scams was raised in many countries.

How a Click or Swipe Can Protect Your Life Savings

Every click of a mouse or swipe on a mobile device tells a story. According to a recent article in Protocol:

In April, systems at the National Australia Bank watched as a customer tried to raise her account transaction limit from $20,000 to $100,000. She logged in with the right username and password and seemed legit, but recently-installed software detected that her behavior was significantly different from previous sessions.

"The way she was using her mouse looked different," Chris Sheehan, a National Australia Bank investigations manager, told Protocol. "The number of clicks on the mouse looked different. Her cutting and pasting details looked different."

The deviations were picked up by the bank's new BioCatch software, which led the bank's anti-fraud team to figure out that the customer was in trouble. She was on her cell phone with a fraudster and was stressed by the account changes he was coaching her to make. The team quickly called her landline to warn her and she put things to a stop.

Source: *Protocol, Banks Watch Your Every Move Online. Here's How It Prevents Fraud*, June 2021

In the UK, the Payment Systems Regulator (PSR) released a consultation document in September 2022 which outlines the proposed legislation around scam reimbursement. The expectation is this will become law in 2023. The major points include mandatory reimbursement for all authorized push payment (APP) scams unless it can be proven the customer was grossly negligent and a 50/50 liability split between the sending and receiving banks.

While the UK is leading the way in legislative action, other countries are considering a similar response to address the problem. The Monetary Authority of Singapore (MAS) is working on a framework similar to the proposed legislation in the UK that would involve shared responsibility among relevant parties when a scam occurs. In Australia, the Australian Competition and Consumer Commission (ACCC) continues to advocate for a model that would require banks to reimburse scam victims.

In the U.S., Senate hearings were held in late 2022 with the major banks who own Early Warning Services, the operator of the Zelle instant payment platform, to address the high level of scams being reported by consumers. In October, Senator Elizabeth Warren sent a letter to the Consumer Financial Protection Bureau (CFPB) summarizing the findings of the investigation and recommending amendments to the Electronic Fund Transfers Act (EFTA) to provide greater protection to consumers using these platforms. In response, the banks that own Zelle announced they are preparing a rule change that would require all banks on the network to reimburse customers that fall victim to certain types of scams, with suggested liability shifts on the bank receiving the funds.

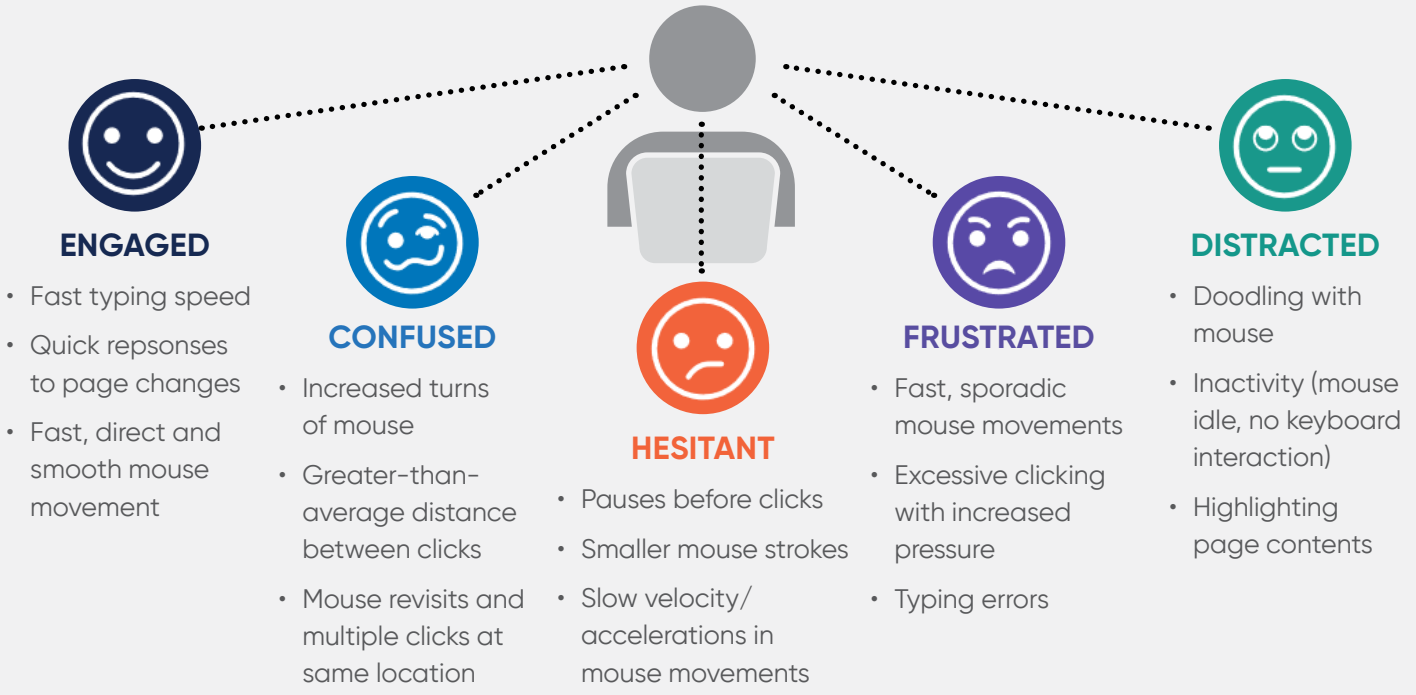
How Customers Behave Can Actually Protect Them

How customers behave in the digital world can be the one thing that protects them from being scammed. For banks, this can translate into millions in fraud loss savings by identifying unauthorized payments and transactions before they occur.

BioCatch has invested significant research in data science to uncover patterns of "good" and "bad" behavior and worked with customers to build advanced risk models to detect a myriad of fraud threats. As a result of this investment, behavioral biometrics is playing a crucial role in helping financial institutions identify and stop social engineering scams.

Even if it is a genuine user making a payment, when a person is acting under the influence of a criminal, there are subtle changes in behavior that can build a picture of a user's emotions or intention during a session and suggest a social engineering scam may be at play. The figure below summarizes different behavior patterns that victims of social engineering scams can exhibit during a session and how these can be interpreted.

Let's examine some of these patterns in more depth.



Typing Patterns

The way a user types can provide insights such as whether they are receiving instructions from a criminal to perform an action or whether they are using long- or short-term memory when inputting information. Segmented typing patterns by a user can indicate dictation. For example, a criminal dictating an account number for a victim to enter and transfer funds to. This one pattern is present in 1 out of every 20 impersonation scams as compared to 1 out of every 500 genuine sessions.

Mouse Doodling

A key sign that a user is distracted is excessive mouse doodling. This behavior is logical given the long waits, pauses and dead time caused by a criminal explaining or dictating instructions to a victim or to keep a digital session from expiring in the process. The average number of doodles across all confirmed impersonation scams is six. While only one percent of the general population exhibit six or more doodles in a session, that figure rises to 38% in reported fraud cases.

Session Length

The active intervention of a criminal in social engineering scams prolongs a session significantly. Only one percent of genuine sessions last more than 30 minutes. However, 10% of sessions that involve an impersonation scam last that long. That number is even higher in social engineering scams that involve the use of a remote access tool (RAT) to take over a victim's computer. In scams where the use of a RAT is detected, 12% of the sessions are more than 30 minutes, likely accounting for the time it takes a victim to download it.

Payment Context

There are numerous indicators throughout the customer journey as it pertains to making a payment and how those actions might indicate social engineering – from the navigation flow to the time it takes to initiate the payment. For example, the time it takes to add a new payee shows significant variance in genuine and fraud sessions. The vast majority of genuine users start the Add Payee process within five minutes of a session starting which indicates that there is a conscious decision to make a payment, and this is done almost immediately. On the contrary, 42% of sessions involving impersonation scams take over 30 minutes to complete the Add Payee process.

Active Call

The active call pattern is unique to the mobile channel and looks at whether a user is on an active phone call while navigating a live session in the mobile banking application. Over 40% of impersonation scams show that the victim was on an active phone call during the live session compared to less than one percent of the genuine population.

Each of these patterns on its own does not imply a scam is in progress, but when combined with hundreds of other data points and compared against the norms of the genuine user population, these insights can be used to build risk models that produce highly accurate profiling to detect advanced social engineering.

Tackling the Rise in Social Engineering Scams

Adopting a strategy to address the rise in social engineering scams – and identify authorized payments that really aren't authorized at all – should focus on four main aspects:

Technology. With social engineering scams overtaking traditional account takeover fraud, implementing technology, such as behavioral biometrics, that can see beyond what legacy-based fraud prevention tools can provide will be critical.

Education. Government regulation and industry initiatives now provide an incentive for financial institutions to rethink their consumer education programs. Beside avoiding financial losses and the impact on reputational risk, financial institutions can use investment in consumer awareness as a brand differentiator.

Payment Value. Criminals will take more risk and attempt to coerce a victim into making higher value payments in an impersonation scam. More than half of all attempted payments in a scam have a value greater than $1,000, with nearly one in ten payments having a value greater than $10,000.

Platform. As with other fraud types, mobile applications are becoming increasingly popular with customers and criminals alike with nearly 80% of social engineering scams carried out on a mobile device. Scam detection should thus be focused on the mobile channel.

About BioCatch

BioCatch is the leader in Behavioral Biometrics, a technology that leverages machine learning to analyze an online user's physical and cognitive digital behavior to protect individuals online. BioCatch's mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist.

Today, BioCatch counts over 25 of the top 100 global banks as customers who use BioCatch solutions to fight fraud, drive digital transformation and accelerate business growth. BioCatch's Client Innovation Board, an industry-led initiative including American Express, Barclays, Citi Ventures, and National Australia Bank, helps enable BioCatch to identify creative and cutting-edge ways to leverage the unique attributes of behavior for fraud prevention. With over a decade of analyzing data, more than 70 registered patents, and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems.

For more information, please visit www.biocatch.com

BioCatch

www.biocatch.com
E: info@biocatch.com
@biocatch
/company/biocatch