XTN®
Cognitive Security

a Cy4gate company

HOW A REAL-LIFE BANK SCAM NEARLY WORKED

And what you can learn from it

POV: You're a Senior IT Engineer

Alex, a Senior IT Engineer, was having what seemed like just another ordinary afternoon. He was working on projects, handling his usual tasks, when his phone buzzed. It was a message from his bank, just like the many he received regularly. There was nothing about it that seemed unusual, no strange links, no odd wording. It looked perfectly legitimate. Seconds later, his phone rang. A call from a Milan number, the same city as his bank. Instinctively, Alex picked up, expecting a routine check. What happened next, however, was something he never expected to experience firsthand, despite his professional background. Here's how it went...

THE SETUP

Alex receives a text message from his bank. Or so it seems.

"Dear Customer, you'll soon be contacted by operator ID 1610, Davide Rossi, for important account-related information."

The SMS lands directly in the official message thread from his bank, where he typically receives legit notifications. No strange links. No typos. Just a believable context and a plausible premise.

Seconds later, a call comes in from a Milan-area number.

"Good morning, we've detected a login attempt from a device and location different from your usual ones."

Alex asks: ***"What device? From where?"***

"An Android phone. From Bari."the bank's representative replies.

Alex responds: ***"That's not me. Please block it."***

"Of course. To proceed, we need to verify your identity. Can you provide a few details, starting with your tax identification number?"

That's when Alex hesitates, immediately sensing something's off. He knows the rules. His bank has made it clear in their email communications ("*We will never ask you for personal data over the phone*").

So he pushes back. ***"I'm not sharing anything. I know your policies."***

But the caller is prepared. ***"Yes, that's correct. You probably also received our recent email about reduced wire transfer limits, a new security measure."***(That email had actually gone out the previous week.)

Still suspicious, Alex says: ***"Let's do this. I'll hang up and call the bank's customer service to verify your call."***

"Ok, no problem,"they reply casually.

Call ends. A 4-minute convincing conversation that raised just enough doubt to make Alex question what was really happening.

THE TWIST

Alex opens his banking app. No suspicious transactions. Funds are safe. He searches for the official customer support number, and freezes. It's the same number that just called him.

Now even more suspicious, he dials the support line directly and starts going through the usual procedure. He enters his customer ID. Just as he's about to proceed, his phone rings again.

Incoming call again. The number on the screen is the same, the one he just confirmed belongs to his bank's support line.

Still rattled, he answers. This time, it's a different voice. Different tone. Different strategy.

"Good morning, Mr. Costa. We noticed you tried to contact our support. Was that you?"

Alex initially denies it, deciding to test the situation.

They say, ***"That's odd, because we have a request logged from your account."***

Alex responds, ***"Absolutely not."***

"Are you sure? This is strange, because our records show that a request was made from your end."

A sense of unease starts to creep in. Alex begins to second-guess himself. Could it be the scammers, or is this really the bank's support team reacting to the earlier phone request?

Normally, when contacting customer support, you're required to follow a standard verification process until an operator picks up. The bank wouldn't interrupt that procedure with a direct call. But the pressure is mounting, and Alex starts to doubt his own instincts.

Eventually, he admits: ***"Yes, it was me. I took some time to figure out what was going on because I thought I'd just been targeted by fraud, and I wanted to verify who I was really speaking to. The suspicious call had the same number as yours. It all felt off."***

The scammer remains calm and reassuring: ***"Of course, I understand. To proceed with the fraud report, let me help you complete your request. We'll just need a few details to get started. Let's begin with your tax ID."***

In that moment, Alex feels a cold rush of clarity. All his doubts vanish. He knows, without a doubt, he's dealing with fraudsters.

"No. As I said before (referring to the first call)***, I won't provide any personal detail over the phone. My bank's own policy forbids this. Let's do this: I'll hang up and call my bank's fraud department asking them to add you to the call. What's your name, please?"***

The reply? ***"Al Beback."***

Alex exhales. He's no longer confused. He's pissed.

"You're quite funny, and you're really good at this."

"Alex how many do you have?" asks the now-fully established scammer, his accent emerging and making his tone sound much less professional.

"50" Alex responds.

"Well, you wouldn't believe how many 20-year-olds fall for this." the scammer adds.

"Not your lucky day, huh?" Alex says with a chuckle. ***"My wife and I both work in cybersecurity."***

" ***Touche"*** the scammer replies, acknowledging Alex's expertise. " ***Yeah, well, I've got to go now. Got work to do,***" and he quickly ends the call.

BEHIND THE SCENES OF THE FRAUDSTER'S PLAYBOOK

What almost happened to Alex is known as an **Authorized Push Payment (APP) Scam**, a type of fraud where the victim is manipulated into authorizing a payment to a fraudster. In this case, the scam was carried out through **impersonation**, one of the most dangerous forms of social engineering. Now that you know how the story unfolded, let's look at the psychological tactics behind it.

Psychological Insights and Fraud Techniques

To understand how fraudsters manipulate their victims, it's essential to explore the psychological tactics and fraud techniques they employ.

BUILDING TRUST

- Spoofed SMS and calls appeared to come from the bank's official number.
- Authority-based trust lowered the victim's defenses.

MANIPULATING EMOTIONS

- Claimed a login attempt from an unknown device to trigger panic.
- Pressured the victim to act fast to "protect" their account.

LEVERAGING KNOWLEDGE

- Referenced recent actions to enhance credibility.
- Blended real details to increase trust.

Building Trust through Authority: Spoofing in Action

In Alex's case, the SMS appeared in his bank's chat history, and the call showed a Milan number matching the bank's official one, that's spoofing. This created confusion and lowered his guard. By using trusted numbers, fraudsters increase the chances of immediate trust. Had Alex saved the bank's number, the caller ID would have been even more convincing.

Creating Urgency: Manipulating Emotions and Fears

The second psychological tactic aimed to create a sense of urgency in the victim. By claiming that an unfamiliar device had tried to log in, the scammers triggered immediate alarm. This common strategy pressures victims into acting swiftly to safeguard their assets. Other tactics could have included alerts about suspicious transfers, warnings of account lockdowns due to security issues, or demands for immediate changes to passwords or security questions.

Using Knowledge to Create Legitimacy

The scammer used knowledge of Alex's recent actions to make the call appear legitimate. By mentioning Alex's attempt to contact the bank, access his account, and his recent support request, the scammer created a sense of familiarity. This made Alex question his instincts, blurring the line between a real call and a scam. The detailed information made the interaction seem credible, disarming Alex and increasing the likelihood of initial compliance.

IF ALEX HAD TRUSTED THE CALL..

This story ended well for Alex, but what if the scam had succeeded?
Let's explore the possible steps the fraudster would have taken to gain full access to Alex's bank account and steal money. Before any fraud, the scammer needs both the username and password, often the trickiest part of the scam. Then, they would also need the One-Time Password (OTP) to complete high-value transactions. Here are some common methods.

Phishing via Spoofed Login Page
After the initial SMS, the scammer could have sent Alex a link appearing to lead to the bank's login page, but it would actually direct him to a fake, identical-looking page. Entering his credentials there would give the fraudster the details and access to Alex's account.

Emotional Manipulation: The fake page might include a message creating urgency, like "Immediate action required to protect your account," pressuring Alex to act without checking the link's legitimacy.

.

Social Engineering via Phone Call:
The scammer could guide Alex to log into the real bank's app and use psychological manipulation to pressure him into providing his username and password. For example, the fraudster might claim the login is necessary to "verify his identity" or "protect his account."

Emotional Manipulation: The scammer might apply fear tactics, warning of a "security breach" that could lead to lockouts or unauthorized transactions, pushing Alex to share his credentials.

Triggering and Stealing the OTP
Even with Alex's username and password, the scammer would still need the OTP for high-value transactions. Initiating a transfer would trigger the OTP to be sent to Alex. The fraudster, still on the phone, would pressure him to read the OTP aloud, bypassing the security and completing the transaction.

Emotional Manipulation: The scammer could further pressure Alex, claiming the OTP is the final step to "secure his account" or "confirm his identity," making Alex feel responsible for the account's security.

Installation of Remote Access Tools
Scammers might also install remote access software on Alex's device, convincing him to download an app like TeamViewer or AnyDesk under the guise of fixing a security issue.
Once installed, the fraudster could control the device, bypass security, and make transfers without further input from Alex.

Emotional Manipulation: The fraudster would reassure Alex that the app is necessary for security, making the process feel legitimate.

AWARENESS IS FAR FROM ENOUGH

As we've seen from Alex's story, today's banks continuously educate their customers on staying alert to fraud. A key message from all financial institutions is pretty clear: "Our representatives will never contact you to request personal data or ask you to carry out transactions." If your friends, family, or loved ones aren't yet aware of this, sharing this crucial information with them could be helpful. That said, while customer awareness is important, banks must shoulder a responsibility they can no longer overlook, one that cannot be addressed with mere warnings. The reputational damage and financial consequences of failing to protect customers are too severe.

Implementing next-generation AI-powered fraud prevention solutions like XTN's Cognitive Security Platform® isn't just an option, it's imperative for securing both their clients and their reputation. XTN's platform goes beyond traditional fraud detection by **monitoring every transaction and interaction contextually**. For instance, during an Authorized Push Payment (APP) scam, when a fraudster convinces a victim to install remote access tools, taking control of their device, XTN **immediately identifies the ongoing phone call**. By cross-referencing the device's location and behavior, the platform **detects any anomalies** and actions that don't align with the user's normal patterns. If the fraudster attempts to carry out a transaction from this different device, XTN detects it, triggering an alert before the fraud is finalized.

XTN employs **sophisticated behavioral analysis** to flag abnormal transaction amounts, unfamiliar payees, or activities that differ from a user's usual behavior. This ensures even the slightest signs of fraud are detected and stopped in real-time. Long story short, while customer vigilance remains vital, banks must equip themselves with solutions like XTN's for proactive fraud detection.

Awareness is not enough. Prevention must step in.

Visit xtncognitivesecurity.com
Contact sales@xtn-lab.com

TIPS FOR END-USERS

How to Protect Yourself

Verify Messages and Calls

If anything feels off, contact your bank directly. Even if the number looks legit, hang up and call back using official channels.

Don't Share Personal Info on Calls

Never, ever share sensitive information, like your PIN, passwords, OTPs, or any personal data, when you're contacted by someone claiming to be from your bank.

Monitor Account Activity

Review your account activity frequently and report anything unusual to your bank. Acting quickly helps stop fraud and protects both your money and your peace of mind.

Read Bank Fraud Alerts

Always read fraud alerts and security tips shared by your bank. They help you stay aware of the latest scams and how to protect yourself.

TIPS FOR BANKS

Protect Your Customers and Reputation

Deploy AI-Driven Systems

Adopt advanced, AI-driven solutions to monitor transactions in real-time and detect anomalies based on user behavior.

Monitor Contextual Interactions

Use behavioral analysis to track interactions and transactions, flagging suspicious activities like abnormal payments or unfamiliar recipients before they escalate.

Act Proactively

Invest in real-time fraud detection that goes beyond traditional systems. Identifying fraud attempts early helps protect your customers and safeguard your bank's reputation.

Educate Customers

Ensure your customers are well-informed about fraud. Regularly remind them that your representatives will never ask for personal data over the phone.

Since 2014 XTN Cognitive Security® develops Behavioral-based Threat and Omnichannel Fraud Protection solutions made unique by breakthrough Behavioral Biometrics technology. Through the award-winning Cognitive Security Platform®, XTN helps digital businesses, such as Banks, Fintech, e-commerce, and Automotive, to quickly identify transactional anomalies using proprietary AI algorithms, Machine Learning, and Behavioral Analysis.
In 2024, XTN joins the Cy4Gate Group, which operates across the cyber market.
For more information, please visit xtncognitivesecurity.com

Milan | Padua | Trento | New York

xtncognitivesecurity.com
sales@xtn-lab.com