DACH FRAUD REPORT 2024

What online fraud threats are banks in the DACH region up against? Dive into the latest trends and innovative strategies revealed at the DACH Fraud Summit 2024.

ThreatMark

DACH FRAUD SUMMIT 2024

Dear Friends,

In September 2024, we successfully hosted the DACH Fraud Summit 2024, a landmark conference that brought together professionals and fraud fighters from nearly 30 banks, representing not only Austrian, German, and Swiss banking but also beyond.

The goal of the Summit was clear: to unite and become stronger together against fraudsters who operate in organized groups, attacking with increasing frequency and sophistication. Over the course of a day and a half, with 9 presentations, engaging workshops, a panel discussion, and countless opportunities for networking during breakfasts, coffee breaks, lunches, and dinners, it became clear that we achieved our mission.

We leave the Summit equipped with a wealth of inspiration, expertise, and actionable insights from leading professionals. New contacts and partnerships have been formed. Throughout the conference, it didn't matter which country or bank attendees represented—collaboration and openness were the defining themes.

As is tradition, we've prepared a post-Summit Report summarizing the key points discussed. This document not only allows participants to revisit the valuable insights shared but also provides inspiration and education to colleagues who couldn't attend. Please feel free to share this Report widely to amplify the positive impact of the Summit.

Finally, I want to express my deepest gratitude to all participants and speakers. The speakers did an outstanding job, bringing their expertise and delivering presentations tailored specifically for the DACH Fraud Summit 2024. To all attendees, thank you for fostering such a welcoming and collaborative atmosphere and for providing amazing feedback. Your contributions made this event a success.

Thank you all, and we look forward to continued collaboration!

Jakub Zalman

TINO FUSTER

PostFinance

Inside PostFinance: Strategies & Technologies in Fraud Prevention

The first speaker from the DACH region was Tino Fuster, representing Switzerland. After introducing himself and his company, Tino's presentation centered on three key areas: the organization and technology of anti-fraud teams, the current threat landscape with attacks and emerging trends, and a special focus on the 'Benin Connection.' His insights provided a comprehensive look into how fraud prevention teams operate, the evolving nature of cyber threats, and the significance of global fraud networks.

Anti-Fraud Organisation

Tino began with an overview of the anti-fraud team's operational structure, which falls under the broader customer security division. The customer security team is divided into three specialized departments, each with a distinct focus. The Online Security department handles electronic payment transactions and digital banking. The Card Security department covers everything from debit card issuance and usage (including Apple Pay and Google Pay) to payment solutions like e-payment and PF Pay, as well as the Swiss mobile payment app, Twint. Finally, the Anti-Fraud department deals with special cases, including internal fraud detection and prevention.

Tino also highlighted the key participants involved in their anti-fraud operations. The team includes specialists from development and operations, as well as those managing bookings and payment transactions, handling case management, and overseeing transaction processes. Digital experts also play a critical role, focusing on customer communication and transaction clarification, ensuring smooth interactions and quick resolutions in fraud-related cases.

Anti-Fraud Technology Stack

Tino went on to discuss their use of operational intelligence (OI) for monitoring and fraud detection. This system works by identifying technical anomalies (OI.ADK) and verifying suspicious transactions (OI.TAU). Operational intelligence relies on a constantly updated ruleset that adjusts to new user activity, ensuring real-time monitoring and enhanced security for customer interactions, orders, and business operations.

Operational intelligence integrates with multiple tools to help ensure that online banking sessions are both secure and seamless, delivering the best possible user experience. This includes various indicators of compromise (IOCs) technology, and additional technologies such as the ThreatMark Platform, which is primarily responsible for critical insights into user identity verification through its behavioral biometrics, as well as applying its authorized push payment detection features.

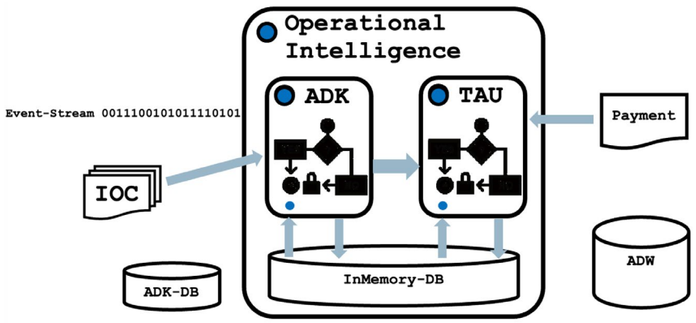
Tino also shared some of the measurements and figures resulting from the daily operations of the Operational Intelligence from the perspective of anomaly detection (ADK). The system provides insight into the number of suspicious online banking sessions. This allows for a clear understanding of how many sessions may require further investigation, helping to identify potential threats while minimizing unnecessary alerts.

When low to high-risk sessions are detected, Tino and his team can take proactive measures to uphold the highest security standards. These actions include terminating the session, switching the e-banking access to read-only mode, or blacklisting users. Additional security steps, like signing forms and blacklisting specific IP addresses, further enhance the protective measures in place.

From the perspective of transactional monitoring (TAU) within Operational Intelligence, the system processes nearly 2 million transactions per day. Only a tiny percentage—about hundredths of a percent (0.0X%)—of transactions trigger an alert, so only a small number require direct customer interaction, helping to streamline the monitoring process while maintaining security.

A top-down approach is employed for all transactions, applying black-and-white rules: black rules flag high-risk behaviors that exceed certain thresholds or fraudulent characteristics, while white rules focus on low-risk activities. After this initial screening, a machine learning (ML) component is applied, with potential for ML to play a larger role in the future. The system combines both ML and rule-based methodologies effectively. Manual review are managed within case management, with only a few cases requiring escalation to the bank for follow-up calls when needed.

Since its adoption in 2020, the Threatmark Platform has significantly reduced false positives. It is primarily used for user identity affirmation leveraging behavioral biometrics, and RAT (Remote Access Trojan) detection, particularly in the context of authorized push payment detection and other scams detection, enhancing the overall security framework.



Attack Vector Type Trends

Tino addressed the current fraud trends in Switzerland, noting that MitM (Man-in-the-Middle) and MitB (Man-in-the-Browser) attacks are no longer prevalent. Instead, Android malware is the most prevalent, with capabilities of keylogging and overlays by typically abusing accessibility services and SMS permissions. Among the threats, various forms of Android malware utilize techniques such as overlay attacks and keylogging.

Further, Tino discussed the diverse array of threat actors involved in phishing attacks, noting the daily attempts they make. Most of these attacks focus on real-time phishing, aiming for account takeover (ATO) and the registration of fraudulent devices. While phishing attempts predominantly occur through email, they also manifest via SMS, online marketplaces, and rogue search engine advertisements. Interestingly, a notable wave of phishing was executed through physical letters in Spring 2024. This information aligns with reports from other Swiss banks and counterparts in Germany regarding the resurgence of phishing tactics involving physical correspondence.

Voice phishing was also listed as a prevalent concern, particularly in the realm of classical technical support scams and bank-related voice phishing attacks. These scams often combine various tactics, including remote access to victims' devices, making it easier for fraudsters to exploit unsuspecting individuals.

Tino also shared his insights on the evolving scam landscape posing significant risks to individuals and businesses within the Swiss banking industry. Among the recordable cases and trends are investment scams, where fraudsters lure victims into fake opportunities promising high returns, and romance scams that exploit emotional connections to defraud individuals. Other notable scam types include goods and transferring fraud, where non-existent products are sold; credit scams that falsely promise credit opportunities; and forged payment orders that trick victims into transferring funds. Scammers also utilize messaging platforms like WhatsApp to deceive users, alongside lottery scams that falsely claim victims have won a prize, requiring them to pay fees to claim it.

Fraudulent Strategies Trends

Fraudsters are employing increasingly sophisticated methods to target victims within the Swiss banking industry. They utilize differentiated channels such as social media, classified portals, search engine ads, and fake shops to find potential victims. These attacks often occur through multi-level tactics, where initial contact may be made via SMS, followed by a phone call to further exploit the victim.

The monetization strategies used by scammers are also evolving, with multi-channel approaches that include tokenized cards and various payment providers to facilitate fraudulent transactions. Additionally, the use of victim databases allows for the multiple utilization of personal information, increasing the effectiveness of these scams.

Instead of traditional session hijacking, there is a growing trend towards account hijacking, which poses greater risks to individuals. Social engineering tactics are frequently combined with remote access methods, making it crucial for both individuals and banking institutions to remain alert to these emerging threats.

Benin Connection

One of the biggest money laundering networks operating in Switzerland, known as the Benin Connection, is comprised of money mules based in Europe but led by criminals based in Benin, Africa. At times, there have been as many as 2,000 active mules operating within the country, facilitating various fraudulent activities. This network is linked to a wide array of scams, including love scams, real estate scams, advance fee fraud, inheritance scams, goods fraud, and credit scams.

The acquisition of money mules is a significant concern in the context of the Benin Connection. In some cases, mules are aware of their actions and their role in the perpetration of fraud. They may respond to job advertisements promising commission-based income, often involving employment contracts that include wage payments redirected to other accounts. Similarly, mules may be recruited through real estate advertisements that offer overpayments, with instructions to forward the excess to another account.

The Benin Connection specializes in targeting individuals who are not creditworthy and are actively searching for private loans. These scammers often create Facebook groups that promise credit access. Within minutes, victims are presented with offers for loans of up to €15,000. They are then required to sign contracts filled with lengthy paragraphs, stamps, and signatures—despite the poor quality of the documents.

Before receiving any credit, borrowers must pay a contract fee ranging from €200 to €300, typically to German IBANs, but increasingly to Swiss, French, and Italian accounts. Additionally, they are often asked to provide copies of their identity cards. In some cases, individuals are instructed to open two bank accounts: one for receiving the loan and another for transferring amortization payments. Furthermore, borrowers are required to disclose their account credentials to fraudulent lenders. In another scenario, romance scam victims are manipulated into opening bank accounts to facilitate donation campaigns.

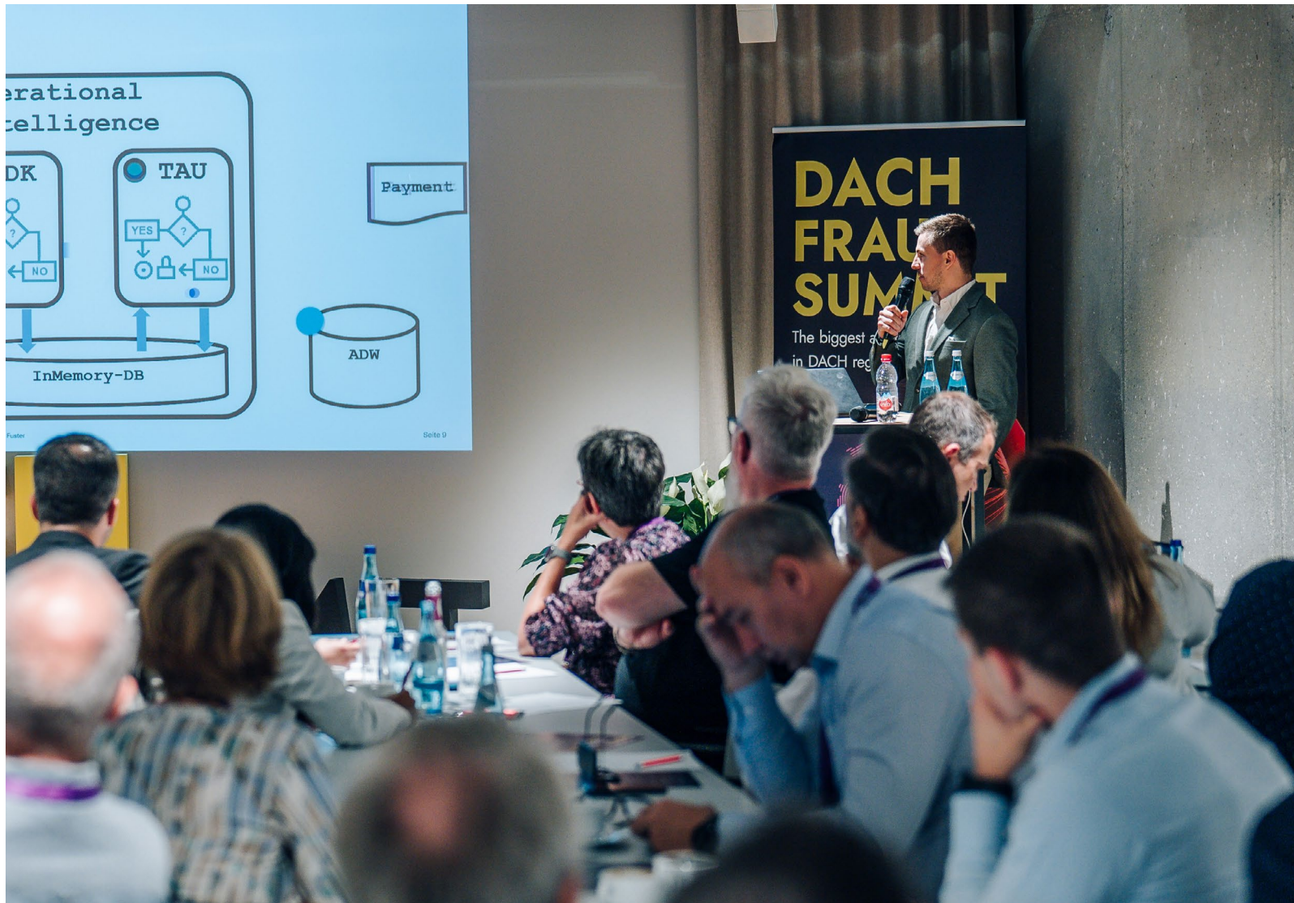
The cash stream from scams often originates in Europe before making its way to Africa, where it is ultimately cashed out, indicating the involvement of organized criminal groups. These scams frequently manifest through fake marketplace advertisements and hacked accounts on used goods trading platforms. Fraudsters typically obtain these accounts from the darknet, where they change email addresses, passwords, and recipient bank account details. They then create enticing fake advertisements that lure unsuspecting individuals into making purchases for items that are never shipped.

How to Fight Benin Connections

Fighting the Benin Connection within (not only) the Swiss banking industry requires a multifaceted approach that targets not only victims but also the money mules operating in this network. For effective fraud prevention, a universal strategy is to continuously monitor transaction patterns and account behaviors that deviate from the norm, focusing on geographic and linguistic inconsistencies, unusual login frequencies, and payment flows tied to regions associated with fraud. By adopting these proactive strategies, the banks can enhance their defenses against this complex network of scams.

Tino plays a key role in safeguarding customer security. Tino and his team play a pivotal role at PostFinance AG by safeguarding online banking services from potential threats and ensuring customers are well-educated on cybersecurity practices, making him an invaluable asset in the fight against fraud. PostFinance AG, established in 1906, is one of Switzerland's leading financial institutions, serving over 2.5 million customers.

Tino Fuster
Security Officer and Fraud Specialist, PostFinance AG



ROMANO RAMANTI

Zürcher Kantonalbank

Cybercrime in Switzerland

Romano Ramanti, an Ethical Hacker at Zürcher Kantonalbank, one of Switzerland's major banking institutions, shared the current state of cybercrime in his region, offering valuable insights drawn from his extensive career dedicated to outsmarting cybercriminals.

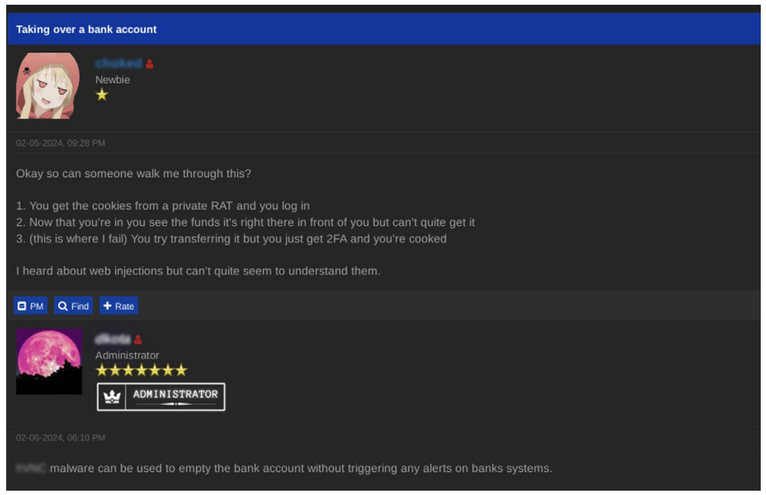
It is also important to mention that Romano presented his work at the DACH Fraud Summit 2024 as a representative of all Swiss financial institutions in the Payment Scheme Fraud Prevention Working Group of the European Payment Council. He elaborated on his responsibilities, which include overseeing an advanced fraud detection system that covers threat hunting, attack neutralization, and ongoing threat actor monitoring. His expertise also extends to darknet analysis and vulnerability research, ensuring that financial institutions remain vigilant against emerging cyber threats. Additionally, Romano mentioned his influence on customer awareness training to fortify defenses against fraud and enhance the overall security posture not only of the Swiss financial sector but also beyond.

Darknet Infiltration

Romano provided very insightful information on how he keeps pace with fraudsters. You do not necessarily have to battle fraudsters on a code level by hacking each other's attack or protective toolsets. Often, it is much more effective to infiltrate the adversary group to gain the most recent tricks, tips, and skills to ethically use them against their originators. And this is exactly what Romano does with delight, to a certain extent.

Romano shared a few real-life examples of his reconnaissance activities on a Darknet forum. The first one featured a post on a Darknet forum on how to take over a bank account and included several hints, such as specifying the proper malware to achieve this "goal."

An interesting observation from Romano's endeavors across the Darknet is that cybercriminals are



(12:31:29) xx@exploit.im: What functions are needed, make a full description.
(12:31:37) xx@jabim.com: Sorry, had problems with jabber
(12:31:41) xx@exploit.im: okay
(12:32:43) xx@jabim.com: I saw that customers in Switzerland use photoTAN, so I want to bypass this. Keylogger for password and i4 is also needed
(12:32:49) xx@jabim.com: do you offer more functions?
(12:33:37) xx@exploit.im: yes more
(12:36:03) xx@jabim.com: as I told you I am new in this field. my idea is to send banking malware with email to get access to their account. what do I need more?
(12:36:47) xx@exploit.im: while nothing else is needed, I'm ready to start writing software
(12:36:55) xx@exploit.im: and we will add functions in the process
(12:40:43) xx@jabim.com: ok. that sounds good for me. does this depend on the bank or all are the same?
(12:41:01) xx@exploit.im: Almost all work the same
(12:43:07) xx@jabim.com: that's good. i am leaving tomorrow for holidays. can i contact you when i'm back?
(12:43:21) xx@exploit.im: You can, but during this time I could already do most of the work
(12:44:15) xx@exploit.im: on your arrival it would be possible to test
(12:48:29) xx@jabim.com: pay 2-3k for expenses and I will start work today, by your arrival part of the work will be done
(12:48:43) xx@jabim.com: ok. thanks. I will let you know
(12:49:05) xx@exploit.im: forgot to say, it will be cheaper to upgrade the old gozi
(12:50:59) xx@jabim.com: cheaper and faster
(12:54:30) xx@exploit.im: but i need to have it. or have you an old gozi?
(12:55:55) xx@jabim.com: No, I have updated gozi
(12:55:59) xx@exploit.im: ok… i will keep this in mind

very collaborative, willing to generously share their malicious knowledge. They truly form a fraud community, or maybe even a family. The Darknet still incorporates a significant privacy layer that protects fraudsters' anonymity.

The Darknet is, not surprisingly, a broking platform that allows fraudsters to connect with potential customers. Romano's next example displayed a conversation between him and a cybercriminal on a well-known Russian cybercrime hub.. The cybercriminal offered to tailor specific banking malware that would allow users to bypass photoTAN security measures widely adopted by Swiss banking customers. He helpfully offered his services for an initial price of €2,000 to €3,000.

Swiss Threat Landscape

In the next part of his insightful presentation, Romano shared his assessment of the threat landscape from his perspective as the person responsible at Zürcher Kantonalbank (ZKB). Not surprisingly for the industry, investment scams lead in the total number of fraud cases. The positive aspect is that around 50% of such cases were detected by ZKB's anti-fraud teams. Unfortunately, the so-called romance scams appear to be more challenging in terms of successfully catching perpetrators. Due to the nature of this tactic, the detection success rate is below 20%. An interesting fact Romano mentioned is that investment and romance scams are often linked. In other words, the same victim and case might eventually fall into both of the aforementioned categories.

In comparison to investment scams and romance scams, other fraud vectors are relatively niche. Phishing attacks, however, are quite prevalent, both in number and intensity. They tend to evolve into more sophisticated forms that leverage advanced generative AI to produce deepfakes, primarily to obtain contact information from potential investment scam victims.

Trust is the Key

Romano presented key tactics that cybercriminals use to successfully execute their scams—particularly investment scams. First, the fraudsters need to gain the trust of potential victims. This is an absolute cornerstone to begin with. To achieve this, they tend to present multiple pieces of true information. If they cannot provide such information, they do their best to present the fabricated facts as credibly as possible. A helpful tool for this is generative AI, with its breathtaking capabilities to generate very credible-looking deepfake videos. It is no wonder that many cybercriminals offer their deepfake generation services on the Darknet. A very popular tactic is to take advantage of successful, well-known people from the region, typically celebrities.

Obtaining the potential victim's contact information is the first step—ultimately, after watching the deepfake video, the victim provides their contact information through the online investment forms. After that, the scammer initiates their scheme by contacting the victim for the first time and convincing them to invest.

To follow up on the topic of presenting credible information, the fraudsters are so sophisticated at this point that they possess fully functional mocked-up investment platforms that potential victims can browse, send, and withdraw money from. Most importantly, they also see alleged high returns, available just a few days after the initial investment. This motivates the victims to invest even more and further enhances their trust in the fraudster. If the fraudster reaches this point, the most difficult part of their job is done. It is then quite easy to manipulate the victim into spending the maximum amount of their available savings.

Investment Platforms: Legitimate or Fraudulent?

The problematic aspect of mocked-up trading platforms is that it is sometimes nearly impossible to distinguish legitimate trading platforms from fake ones. To mitigate this issue, ZKB maintains a warning list risky and potentially fraudulent investment platforms.

Those lists, of course, consider objective criteria to correctly assess each site's risk. Romano outlined a few of the methods. The first mentioned was the presence of multi-tier platform subscriptions that unlock better investments, return rates, and platform features—e.g., standard, premium, and VIP pricing plans that are available for different fees. Romano also mentioned the utilization of an open tool, urlscan.io. With every URL scan done using this tool, the content of the page can be browsed, including hashed resources. Fake investment scam platforms quite often share those hashed resources (i.e., content), making it easier to identify other fake investment platforms by using the same tool.

He Loves Me (Not)

Romance scammers do not have much true and legitimate information at their disposal, so they need to be skillful in psychology and reconnaissance. This is probably why they create elaborate profiles designed to encourage potential victims to view them as ideal romantic partners, according to Romano's research and experience. This is the optimal way to build trust with potential victims. Needless to say, romance scammers heavily exploit state-of-the-art technology to generate fake personal photos and videos to further persuade their victims of their trustworthiness. Overall, the common denominator for both investment and romance scams is the building of trust combined with the misuse of highly sophisticated technology.

When it comes to romance scams, their mitigation is complicated. This explains the relatively low detection rate that Romano shared in earlier parts of his presentation. However, there are some limited options for combating romance scammers. A good example is the scammer.info site, which hosts a

community that combats all types of online scams, including romance scams.

Phishing Techniques

Phishing is a cross-border problem affecting the industry, and the situation in Switzerland is not significantly different from that in other countries. Based on Romano's observations, a typical phishing attack begins with a deceptive email designed to lure the victim into clicking on a link that leads to a fraudulent e-banking login page. These fake sites closely mimic legitimate banking websites, tricking users into entering their credentials. Once the fraudsters obtain this information, they attempt to carry out an account takeover (ATO) by adding their own devices to the victim's online banking profile, thereby gaining unauthorized access to financial accounts and ultimately conducting fraudulent transactions.

Phishers often employ email beacons—tiny pixel-sized images embedded within phishing emails—to track recipients who open their messages. When the email is accessed, the pixel loads from the fraudster's server, revealing information such as the recipient's user agent, operating system, and email address. This technique allows attackers to compile verified email lists and sell them on the Darknet for significant profit. Additionally, phishers have been known to exploit Google Ads, paying to ensure that their fraudulent sites appear as the top results when users search for their bank's website.

Another common phishing tactic involves messages such as "Your e-banking is blocked," prompting victims to provide their phone numbers, which fraudsters then use to execute their scams through phone calls. In one case, a travel agency clerk in New Delhi was found to be engaging in phishing as a side job during his regular working hours. The key to uncovering this activity was monitoring web requests originating from India, which revealed the clerk's involvement in these schemes.

Hacking the Phishers

In the final part of the presentation, Romano focused on some ethical hacking tactics to effectively mitigate the efforts of phishers. The main prerequisite of ethical hacking is that fraudsters frequently neglect the security of their phishing sites, resulting in numerous vulnerabilities within these malicious pages. As a result, it is not uncommon to find issues like Cross-Site Scripting (XSS) present on these sites. Interestingly, when attempts are made to contact the alleged owner of such a page, the response is often automated through a Telegram bot, indicating the impersonal and mass-produced nature of these phishing campaigns. Fortunately, due to these vulnerabilities, it is possible to extract the chatID of the Telegram bot, the Telegram token, and possibly other useful Telegram bot-specific information. An ethical hacker can leverage this information in further API communication with the Telegram bot—specifically to reveal and contact phished customers.

Romano also pointed out that phishing sites are often hosted on vulnerable servers running outdated PHP versions, making them susceptible to exploitation. This weakness allows cybersecurity experts or even other malicious actors to use PHP vulnerabilities to hack into the hacker's own server. Once access is gained, it's possible to manipulate, take control of, and/or browse the files on the ethically hacked servers, which often contain phishing logs, including the credentials of the phished users.

Romano concluded his presentation with the observation that scammers often make mistakes and leave behind digital footprints, providing opportunities for detection. He emphasized the importance of international collaboration in combating these threats. As an example of successful cooperation, Romano highlighted a joint effort to uncover a Microsoft support scam, which involved a workshop with the Bangladeshi police. This collaboration revealed that the same groups of scammers were operating across different regions, demonstrating the effectiveness of cross-border partnerships in tackling online fraud.

Romano is a cybercrime expert with extensive experience in fraud prevention and ethical hacking. Since 2020, he has served as the Swiss Representative for the European Payments Council (EPC), contributing to key working groups such as the Payment Scheme Fraud Prevention Working Group (PSFPWG) and Verification of Payee (VOP). Since 2014, he has been the Business Responsible for Fraud Detection Solutions at Zurich Cantonal Bank.

Romano Ramanti
Certified Ethical Hacker, Swiss Banking Representative in Payment Scheme Fraud Prevention Working Group, European Payment Council

SANDY LAVOREL

Gen AI in Financial Fraud

The first speaker after lunch was Sandy Lavorel, Head of Community Scoring & Intelligence at NetGuardians, who provided valuable insights on generative AI in financial fraud to the gathered fraud-fighting community. Sandy also represented his colleague, Vivien Bonvin, Lead Data Scientist, who was not able to attend the event.

Deepfake but True Story

To emphasize the importance of generative AI in the context of modern scams, Sandy focused on a notable incident involving ARUP, a prominent global engineering and consulting firm. In this sophisticated scam, ARUP fell victim to a scheme that resulted in a staggering loss of £20 million. This case underscores the growing risks associated with advanced technologies, particularly the use of deepfake videos by criminals to impersonate trusted individuals and organizations.

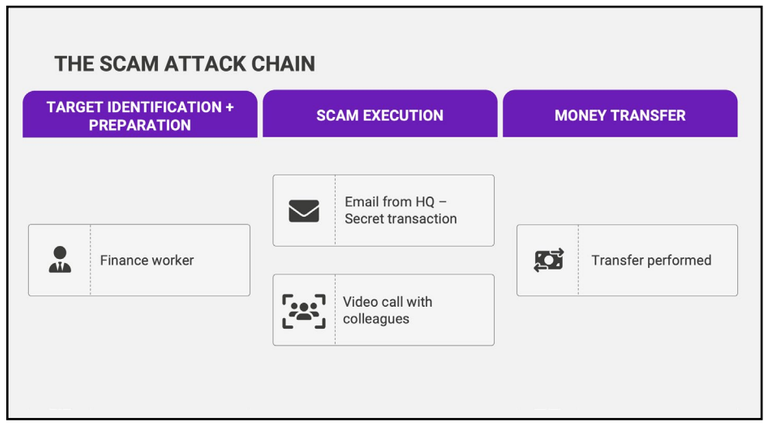
In this instance, the scammers leveraged deepfake technology to fabricate a convincing video of an ARUP executive instructing staff to transfer substantial sums of money. This deception led the company into the trap set by the fraudsters. The attack involved a thorough identification of a vulnerable target and meticulous preparation for executing the fraudulent scheme. The scam began with a forged email from headquarters, detailing a secret transaction of high importance and urgency. The finance employee who fell victim to the scam deemed the email trustworthy and quickly joined an ad-hoc video call with his superior. This is where the deepfake video, created using generative AI, played a crucial role. Watching the pre-recorded video of his superior instilled further confidence in the situation, leading the finance worker to be successfully manipulated into authorizing a transaction of £20 million shortly thereafter.

The event serves as a chilling reminder of the power of generative AI, which can produce hyper-realistic content that is often indistinguishable from genuine interactions. As technology continues to evolve, the implications for cybersecurity and fraud prevention become ever more critical.

In the next section of his presentation, Sandy explored the critical issue of how fraudsters exploit generative AI to carry out their scams. He also discussed how we can harness AI to enhance our efforts in combating fraud. By examining the tactics employed by criminals, Sandy shed light on the potential risks posed by advanced technologies, while also highlighting innovative ways to use AI as a tool for fraud prevention.

AI in Data Gathering

Sandy used the ARUP company scam as a case study to highlight how fraudsters effectively leverage generative AI in their operations. He pointed out several key areas where the misuse of AI significantly aids criminals during the initial phases of tar-



geting and preparation. These include data mining for personalization, extracting social engineering insights, and facilitating large-scale impersonation.

Regarding context building and data mining, Sandy further emphasized the challenges we face today, particularly due to the declining quality of information available online that is used for training generative AI. As websites compete for visibility on search engines, many prioritize search engine optimization (SEO) over content quality. This has resulted in low-quality sites often ranking higher, making it increasingly difficult to find reliable information. Consequently, when conducting research, individuals frequently encounter poor content that can mislead or misinform. The ongoing struggle for search quality raises a critical question: Is there a need for search middleware that could enhance the integrity of online information and help mitigate these fraudulent tactics?

Google recognizes the challenges posed by the proliferation of low-quality content and is actively working to refine its algorithms. However, the adage "garbage in, garbage out" rings true: if the majority of websites are filled with unreliable information, the search results are likely to reflect that. Moreover, high-quality content is increasingly hidden behind paywalls, such as those of reputable online newspapers, making it even more difficult to access trustworthy sources.

What we lack is an additional layer in our search capabilities—one that synthesizes information found across various websites. This is akin to what tools like ChatGPT offer, as they can distill and present data from multiple sources in a coherent manner. Implementing such a search middleware could enhance our ability to navigate the sea of online information, helping users find accurate and reliable content while minimizing exposure to fraudulent tactics.

Sandy illustrated his point by referencing a recent experience: instead of sifting through the NetGuardians website, LinkedIn, and other platforms, all while navigating pop-ups about cookies, data privacy, and newsletter sign-ups, he could simply ask ChatGPT to summarize the information he needs. This not only streamlines the research process but also allows for a more efficient gathering of relevant insights without the distractions often encountered online.

Sadly, fraudsters often misuse this technology. Instead of painstakingly gathering information from various sources, scammers now utilize tools like ChatGPT to quickly compile and synthesize data, making their operations more efficient and effective. This streamlined approach enables them to personalize their attacks with greater precision, as they can easily access and analyze information about potential victims. By leveraging AI in this manner, criminals can rapidly enhance their tactics, making it crucial for organizations to stay ahead of these evolving threats.

AI in Scam Execution

During the execution of a scam, generative AI (GenAI) plays a critical role, particularly in creating highly convincing and targeted fraudulent content. It primarily enables the crafting of authentic-looking emails, achieving large-scale personalization, and avoiding detection—tasks that can be quickly and efficiently accomplished using tools like ChatGPT or similar models. Fraudsters, however, must overcome a key obstacle: models like ChatGPT are programmed with safeguards and will refuse direct prompts such as "Create a phishing email." However, with a well-crafted prompt, scammers can manipulate the model to produce convincing content without raising red flags.

Another essential aspect of scam execution involving GenAI is the creation of highly realistic deepfake video calls, real-time voice cloning, and manipulation of facial expressions and mannerisms. For these scams to succeed, fraudsters must obtain quality video and audio recordings of the person they plan to impersonate in the deepfake. With enough content from the targeted individual, fraudsters can create an almost flawless deepfake, tricking the victim into believing they are interacting with a trusted person, such as a superior or colleague. The more personalized the data, the more believable the deepfake becomes, making it easier for scammers to carry out high-stakes fraud without requiring advanced technical or hacking skills.

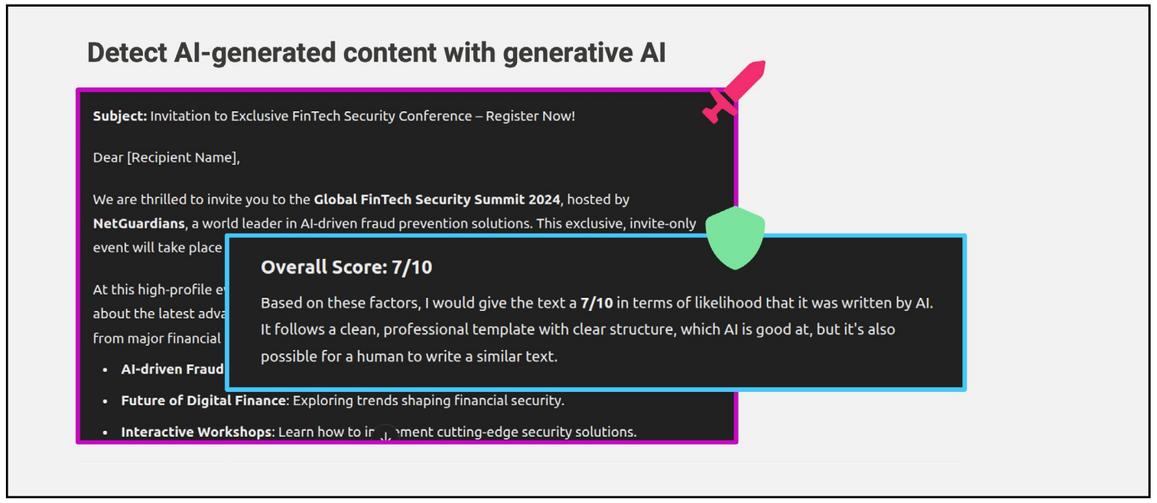
This shift in the use of AI tools means that even basic-level access to someone's digital footprint—such as a few recorded meetings or voice notes—can fuel sophisticated impersonation, turning simple scamming tactics into alarmingly effective and hard-to-detect operations.

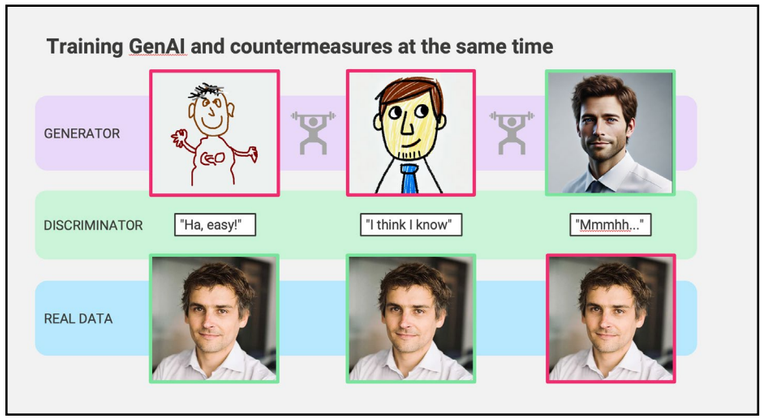
Once fraudsters successfully gain the trust of their victims by expertly leveraging AI tools, the final phase of the scam typically relies on psychological manipulation and real-time communication to close the deal. With the groundwork laid through convincing emails, deepfake videos, or voice cloning, scammers use techniques such as urgency, authority, or fear to pressure victims into transferring money quickly.

In this stage, the victim is usually led to believe that a high-stakes decision must be made immediately, leaving little room for doubt or verification. These real-time interactions—whether over video calls or phone—capitalize on the victim's trust and emotional response, ensuring that the fraudulent transfer is completed before the target realizes they have been deceived.

How to Use genAI to Detect Phishing?

After Sandy outlined the tactics used by cybercriminals, the next phase of the presentation shifted to how the same tools could be turned against them. Sandy emphasized the need to rethink the use of artificial intelligence for fraud detection. He proposed an innovative solution: leveraging language models to analyze and score suspicious informa-





tion based on its likelihood of being fraudulent or generated by AI. This involves implementing AI-powered phishing detection systems that use Natural Language Processing (NLP) to identify patterns associated with scams.

While this approach is promising, Sandy acknowledged its limitations, pointing out that it might produce false positives. He emphasized that such analysis should be treated as one part of a multi-layered defense strategy, not as a definitive fraud detector. Instead of relying solely on AI outputs, these results should be considered "weak signals" that complement other detection tools. He also noted that although AI can be used to identify potentially fraudulent content, it can still be outsmarted, making the fight against AI-powered scams a constant arms race.

Sandy concluded this part by reflecting on how the fight against generative AI and fraud essentially becomes a zero-sum game, where each advancement in detection is met with countermeasures by criminals and vice versa. The evolving landscape underscores the importance of a more holistic fraud prevention strategy, where AI is part of the toolkit rather than the ultimate solution.

Leveraging genAI for Deepfake Detection

In his exploration of innovative tools for fraud fighters, Sandy discussed the potential of leveraging generative AI for more advanced fraud detection and prevention methods. He focused on areas such as AI-driven deepfake detection, biometric and behavioral analysis, content verification, and AI-powered transaction monitoring systems. One of the most interesting points he raised was the use of generative AI to assist in callbacks, ensuring that fraudsters are not able to manipulate the communication channels in real time.

Sandy also touched on the concept of Generative Adversarial Networks (GANs) as the foundation for both training AI and establishing countermeasures. GANs consist of two models: one that generates data (such as deepfakes) and another that discriminates between real and AI-generated data. Over time, these models engage in a back-and-forth "zero-sum game," where each model improves by learning from the other's mistakes. As the generator creates increasingly realistic content, the discriminator works to identify even the subtlest signs of forgery.

This dynamic process is ongoing, as every advancement in generative AI leads to new challenges for detection systems. Sandy emphasized that while we can improve both models, there is unlikely to ever be a "perfect" solution—because with every improvement in detecting fraud, fraudsters will be able to leverage better tools to evade detection. This constant evolution underscores the ongoing struggle between fraudsters and anti-fraud efforts.

Sandy's presentation concluded with a crucial point: even though humans can still spot certain anomalies that AI struggles with—such as subtle visual distortions or poor-quality deepfakes—fraudsters know how to exploit situations where their victims are under pressure or distracted. As AI-generated scams become more sophisticated, the human element remains vital. It is clear, however, that the fight against AI-powered fraud will require ongoing vigilance and innovation.

Sandy is a seasoned expert in fraud prevention, leveraging over a decade of experience to drive innovation and deliver impactful results in the fight against financial crime. Currently serving as the Head of Community Scoring & Intelligence, Sandy leads innovative efforts to enhance fraud detection and prevention strategies. Previously, Sandy held key roles, including Team Leader & Practice Lead Business Analyst, where they spearheaded analytical projects and team development.

Sandy Lavorel
Head of Community Scoring & Intelligence at NetGuardians

RAISA FEDOROVSKA

Scams in the Shadow of War

The DACH Fraud Summit 2024 also provided insight into digital fraud from the perspective of different outside the DACH region. Raisa Fedorovska, Head of EMA Academy and CyberSecurity School in Ukraine, conveyed an alternate perspective of geopolitical events and the impact on fraud.

In her presentation, Raisa explored the evolution of digital fraud in Ukraine, emphasizing how socio-political factors have shaped the country's cybercrime landscape. She dove into phishing tactics, revealing how advanced these schemes have become. Raisa also gave insight into Ukraine's fraudulent call centers that target victims globally with manipulative social engineering tactics. Her talk highlighted the growing sophistication of fraud and the pressing need for stronger defenses and international cooperation.

Before the War

Creating a successful phishing campaign presents several challenges for the fraudster. First and foremost is the infrastructure itself: purchasing a credible domain and securing hosting, all under the veil of anonymity.

Before the invasion, Ukraine was already dealing with increasing fraud, mirroring global trends. Online scams and social engineering fraud were on the rise, with nearly half (45%) of users falling victim to online shopping fraud. Losses varied widely, with average amounts per scheme ranging from just €12 for basic scams to €825 for sophisticated SIM-swapping attacks. In a country where the average monthly salary hovered around €500, these losses were significant. Alarmingly, it is estimated that only 21% of fraud cases were reported, meaning the true scale of the problem was far greater than the statistics suggest.

Ukraine was also grappling with a range of evolving schemes like SIM swapping and bank impersonation. Scams involving Remote Access Tools (RATs) were also becoming more common, allowing criminals to gain access to victims' computers remotely. A particularly sinister method, known as "fake dates," involved scammers pretending to be women and luring male victims to fraudulent websites under the guise of a date, only to steal their card information and money.

How the War has Reshaped the Landscape of Fraud

In the early days of the war, everything came to a sudden stop. As Russian troops invaded Ukraine, even the country's fraudulent call centers and scam operations went silent. Scammers took what could be described as an "unexpected break," causing fraud activity to drop to zero temporarily. Meanwhile, despite the chaos, banks continued to function at full capacity, ensuring that financial services remained operational even during the conflict. This drop in scams was only brief, as new and more complex fraud schemes quickly re-emerged in the wake of the initial disruption.

In the second week of the war, Ukraine experienced a surge in opportunistic fraud. Scammers took advantage of the chaos and fear surrounding the invasion, using the crisis to deceive Ukrainians. Fraudulent schemes ranged from fake charity appeals and fundraising efforts to non-existent rental properties, fake transportation, and illegal border crossing schemes. Nothing was off-limits for these criminals. Even military equipment, counterfeit medical supplies, and stolen personal information were used as tools for fraud during this vulnerable time. The war had opened the door to widespread exploitation, with scammers preying on those most desperate for help.

In the first two months of the war, Ukraine saw a rapid surge in fraudulent activities. The number of exposed scams during this short period had already surpassed the total from the entire previous year. This sharp increase in fraud reflected the exploitation of the war-torn environment, as scammers quickly adapted to the new opportunities created by the chaos. At the same time, the

Ukrainian cyber police were overwhelmed, taking on numerous new wartime responsibilities not directly related to investigating scams. This added strain made it even more challenging to keep up with the growing wave of cybercrime and fraud across the country.

By the end of 2022, scammers quickly adapted to the war and doubled their profits. Ukrainian cyber police reported that around 10% of the victims were military personnel, showing how fraudsters targeted vulnerable groups. One common scam was SIM swapping, where criminals used soldiers' identities to take out loans. This scheme involved three steps: first, accessing any existing funds; second, taking out loans; and finally, demanding money from the families of the missing soldiers for information about them. Another tactic was taking over social media and messaging accounts. Since military personnel often did not use these platforms much, they became easier targets for scammers.

Fraud Schemes Adapted

Later, in 2023, one of the largest scam schemes involved fraudsters impersonating volunteers, soldiers, and even clergy members. These impersonators took advantage of people's trust, especially in a time of war, to gather donations or financial support for fake causes. These schemes played on the public's goodwill, exploiting the chaos of the conflict to enrich themselves at the expense of those trying to help.

In 2024, phishing delivery schemes have become arise as the latest threat. Scammers send fake delivery messages, tricking victims into clicking a link that leads to a phishing website disguised as a legitimate postal service. On this site, scammers quickly steal the victim's card details to tokenize the cards. They then manipulate the victim into providing the bank's SMS authentication code, which is entered into the fake site, completing the scam.

New Fraudster Tools

New tools are constantly emerging for fraudsters in Ukraine. AI-generated content is being used for romance scams, and a hybrid approach has emerged where scammers impersonate a boss via nearly identical Telegram accounts, followed by deepfake calls requesting urgent financial assistance from employees at odd hours. AI-driven schemes are not yet widespread, however. AI models, such as ChatGPT, are trained mostly in English, making phishing attempts in Ukrainian less effective. Bypassing facial and voice recognition checks during client verifications continues to be a challenge for fraudsters, despite the misuse of AI.

Today's Situation

While ATM-related crimes have dropped by a significant 70%, scams have surged by 10% during the war. In this same time period, it is estimated that fraudsters' profits have increased four times since the conflict began. However, there is also positive progress. Ukraine has made notable advancements in combating phishing, vishing, and smishing schemes, winning key battles on those fronts. Raisa shared data that recognizes a consistent drop in phishing and vishing incidents over recent months. There has been a noticeable decline in citizen complaints submitted to the cyber police, reflecting that Ukraine's efforts to combat these types of fraud are beginning to pay off. The numbers suggest that anti-fraud strategies are making a tangible difference, helping reduce the overall impact of these schemes on citizens.

Phishing Defensive Tactics

In Ukraine, combating fraudulent resources involves a multi-faceted approach, starting with continuous cyber awareness training to ensure that citizens and organizations stay informed about evolving scams. While education is essential, it is not enough to stop all fraud.

Ukraine employs blocking fraudulent resources at the registrar and hosting provider level, though response times can be slow, ranging from a few days to weeks. Organizations like ThreatMark help Ukraine in reporting phishing sites for the process of takedown.

Tools like Google Safe Browsing are effective in major browsers like Chrome and Safari. However, these measures are less effective in mobile apps such as Facebook and Telegram, where phishing links often spread through in-app browsers. Most phishing sites in Ukraine use Cloudflare (95%), making it difficult for Google's systems to detect and block these threats as they profile traffic from the USA or other countries. Statistics show that in the first three months of 2023, over 8,000 phishing domains were detected, though only 39% were blocked due to complications with registrars, many of which were based in Russia and the USA. This shows a significant challenge with the global infrastructure of phishing attacks.

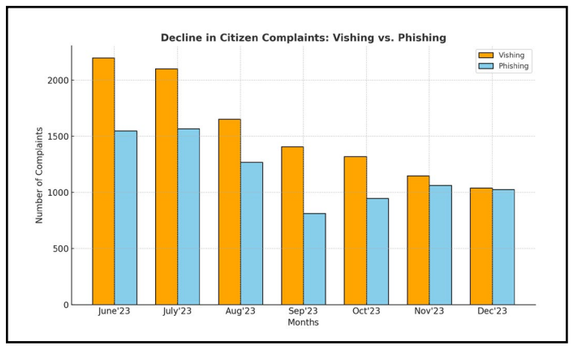
Ukraine also uses a DNS firewall to filter phishing domains at the telecom provider level. This initiative, managed nationally by Cyber Security Center of the National Bank of Ukraine. Ukraine hasn't been a pioneer in DNS firewall implementation, learning from countries like Poland and Switzerland.

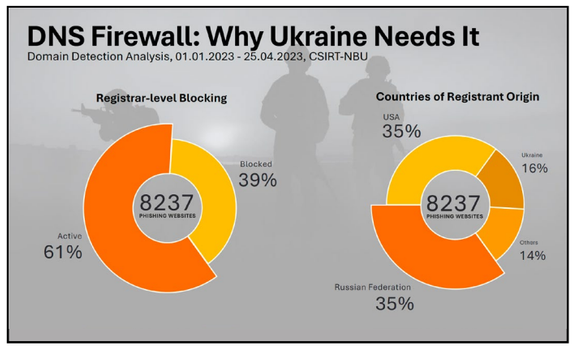
The MISP malware information-sharing platform at the National Bank of Ukraine receives alerts about harmful domains, malware, and phishing scams. This system is designed to prevent misuse for reputation attacks or competitive issues. Every 15 minutes, a DNS zone is created and shared with service providers. When a user tries to access a malicious site, they are redirected to a warning page that explains the site is blocked due to its harmful nature. Logs from this process are collected for further analysis.

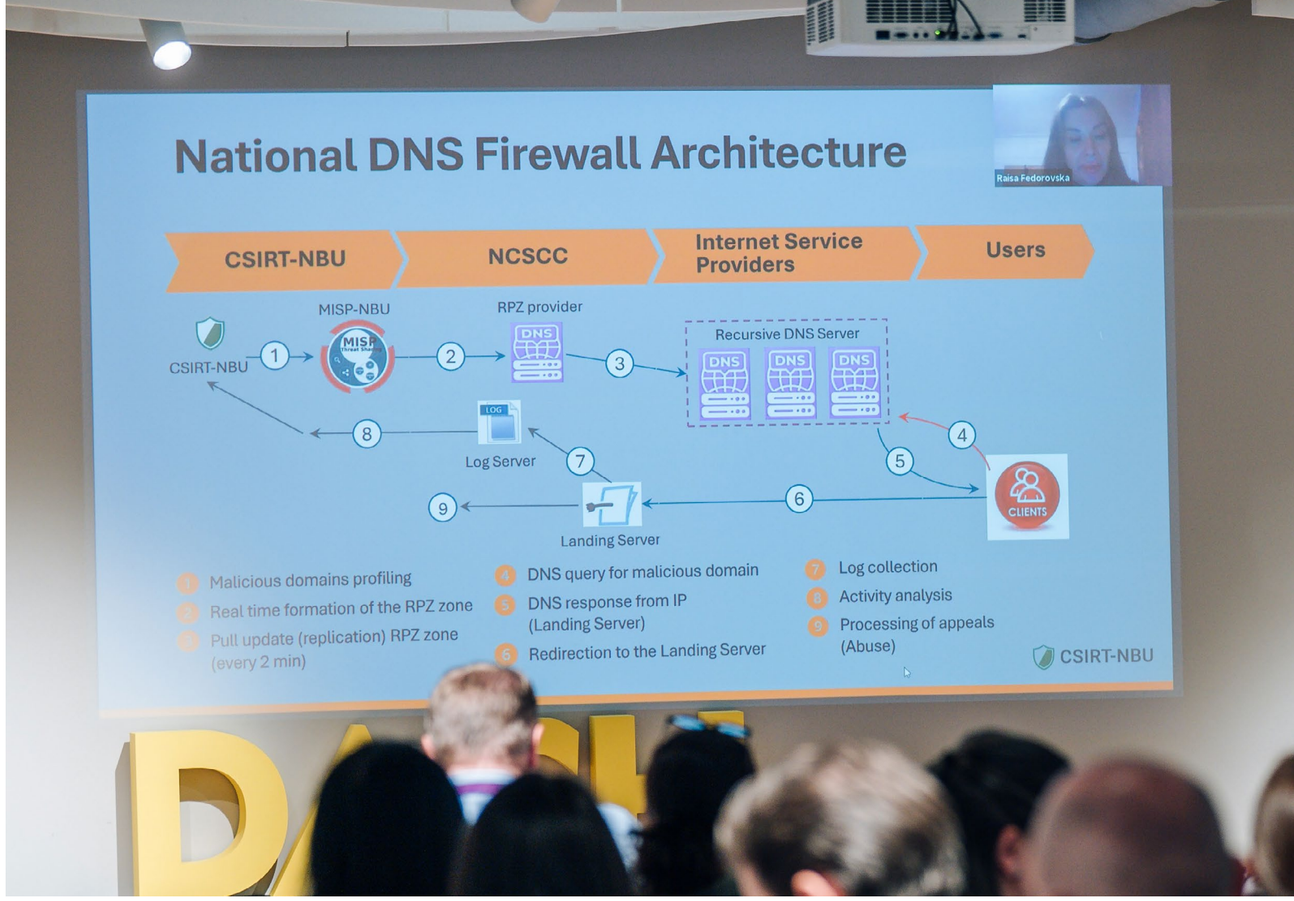
A notable achievement is the ability to block harmful sites within 30 minutes, much faster than the days or weeks it typically takes at the registrar level. The goal was to implement rapid blocking, and this has been accomplished.

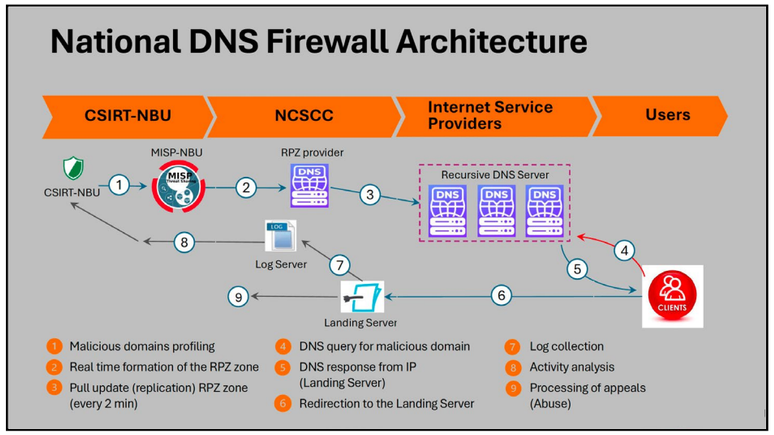
However, while the DNS firewall allows to block phishing domains quickly, it's not an ultimate solution. Raisa underlined the need of international cooperation, especially with partners like Cloudflare, and importantly, support from law enforcement and cyber police to catch and prosecute scammers operating in Ukraine. There are also other challenges to this approach. Some users bypass the blocks using VPNs, and iPhone users often do not use their provider's DNS services because of default settings that prioritize proxies. While most providers and mobile operators support this initiative, some are slower to adapt.

Despite the increase in fraudulent domains, there is positive news: the number of users seeing the warning message (certificate error pages) and secure landing pages is also rising. By the end of









last year, the total for certificate errors reached 2.7 million, while around 275,000 users were redirected to the secure landing page. This shows how many people were protected.

Fraudulent Call Centers in Ukraine

In the final part of her presentation, Raisa highlighted the concerning rise of fraudulent call centers in Ukraine, which have increasingly shifted their focus toward Russia, European countries and the USA.

Raisa revealed that much of the information regarding these call centers became available due to a mistake made by a developer working on the "CRM" systems used by these fraudulent call centers. One alarming statistic she provided is that there are approximately 1,100 contact centers operating in Dnipro, a city located in eastern Ukraine.

Raisa clarified that the figure of 1,100 contact centers in Dnipro does not represent the actual number of call centers but rather the number of IP addresses associated with the call centers. Typically, these centers employ between 10 to 150 people, with most employees being under 35 years old. Each center makes around 5,000 calls per day, but only about 0.1% of those calls result in a client engaging with a scammer for more than 10 minutes. The overall effectiveness rate of these calls stands at just 1%.

Further, Raisa highlighted some key characteristics of these fraudulent call centers, particularly the practice known as "pig butchering," where scammers aim to extract as much money as possible from their victims. She noted that entire call centers are sold complete with their processes, scripts, CRM systems, IP telephony tools, and caller ID spoofing capabilities, with a small center of 10 to 15 employees costing around $5,000.

Interestingly, these call centers do not only target Ukrainians; they often focus on citizens from other countries, especially Russians. In a reciprocal manner, Russian call centers are also targeting Ukrainians. Raisa pointed out that due to the ongoing war, there is a lack of real legal action, meaning perpetrators face little to no punishment for their actions. Additionally, Ukrainian call centers are increasingly targeting citizens from Poland, the Czech Republic, and other countries.

It's important to recognize that the operations of these call centers rely heavily on local individuals from the targeted countries. Knowledge of the language, banking processes, and the use of money mules is essential. Recruitment for these fraudulent call centers is often done openly through popular job platforms, as well as social media channels like Telegram and Instagram. The average salaries offered help ensure a steady influx of candidates, particularly as these centers expand into new markets. Language skills, especially Polish and Czech, are highly valued among new recruits.

Fraud Call Center Takedowns (Cyberpolice in Action, 2023)

Location	Call Center Specialization	Number of Arrests	Victims	Confirmed Loss (EUR)
Kharkiv correctional facility	Bank Impersonation, Safe Account Transfer Scam	10	Ukrainian citizens	No info
Vinnytsia correctional facility	Bank Impersonation, Safe Account Transfer Scam	10	Ukrainian citizens	25,641
16 regions, call center network	Bank Impersonation + Investment Scams	2,500	Ukrainian, EU, and US citizens	No info
Dnipro and Czech Republic	Bank Impersonation	10	Czech citizens	8,000,000
Ukraine + Donetsk and Luhansk	Bank Impersonation	No info	Ukrainian citizens	2,564,103
Kyiv, Dnipro	Charity Fraud for Armed Forces of Ukraine	8	Ukrainian citizens, 6000 victims	256,410
Dnipro	Bank Impersonation	40	Kazakhstan citizens, 18,000 victims	No info
Zakarpattia	Bank Impersonation, Missing Person Scams	No info	Ukrainian citizens	192,308

Call Center Ads

Several key red flags can help identify job advertisements linked to fraudulent call centers. Advertisements from anonymous organizations should raise suspicion, as legitimate employers typically identify themselves clearly. Offers of high salaries with weekly payments often seem too good to be true, as legitimate call centers rarely operate on this payment schedule. Job listings that require fluency in Ukrainian and Russian, combined with mentions of extensive training, and free housing, commonly included in such offers, may indicate fraudulent activity. Additionally, communication primarily through platforms like Telegram is a significant red flag, as reputable employers typically avoid this practice. By recognizing these indicators, individuals can better protect themselves from potential scams.

Scam Centers Operations

Scam call centers function with a structured hierarchy, where each individual has a defined role. At the top are the leads and senior staff who manage operations, recruitment, and security. They oversee the overall functioning of the center. Tech support plays a critical role, as they control access to vital systems, including computer logins and workstation configurations. Employees typically do not have access to these systems, making tech support a key target for law enforcement during takedown operations.

On the front lines are the callers, who make cold calls following one of the approximately 150 different scripts designed for various scenarios, including dealing with difficult clients. They initiate contact with potential victims, attempting to convince them to engage. The second tier consists of the closers, who finalize the deals, create any necessary fake documents, and coordinate with money mules to facilitate the transfer of funds.

Tools Used by the Call Centers

Fraudulent call centers rely on various sophisticated tools to carry out their operations. One primary tool is the CRM (Customer Relationship Management) system, which resembles those used in

Fraud Call Center Takedowns (Cyberpolice in Action, 2024)

Location	Call Center Specialization	Number of Arrests	Victims	Confirmed Loss (EUR)
Dnipro region	Bank Impersonation, RAT Scam	5	Ukrainian citizens	51,282
Chernihiv region	Bank Impersonation	21	Ukrainian citizens	138,462
Kharkiv	Cryptocurrency, Stock Market Schemes	8	Latvian citizens	282,051
Dnipro and Czech Republic	Bank Impersonation	10	Czech citizens	8,000,000
Kharkiv region	Bank Impersonation, Safe Account Transfer Scam	4	Ukrainian citizens	No info
Kyiv	Charity Fraud	3	Ukrainian citizens	128,205

legitimate banks but is specifically designed for fraudulent activities. This system collects data on victims from multiple leaked databases as well as from the cold calls made by the callers. Each entry in the CRM may have labels such as "money stolen" or "no funds," indicating whether they plan to contact the victim again later. A notable entry is the "umnik" label, referring to a victim who has figured out the scam. Raisa shared her firsthand experience with this; when contacted by fraudsters, she immediately instructed them to label her as Umnik. You should have heard the impression it made on fraudsters! It seems it worked, as Raisa has not received a scam call attempt since.

Additionally, these centers utilize IP telephony software, which allows scammers to spoof phone numbers. This makes it appear as though they are calling from legitimate banks, increasing the likelihood that victims will engage with them.

Another feature integrated into these CRM systems is the Banking Website Generator. This tool creates fake online banking dashboards tailored to individual victims, which scammers send to instill trust. If victims express any doubts, the fraudsters can send counterfeit banking documents through messaging apps. These documents are automatically generated by the CRM system, utilizing the victim's data to match the correct document format and issuing institution.

Fraudulent call centers take security measures seriously, employing multiple layers of protection to ensure their operations are not compromised. They utilize full disk encryption tools, like Veracrypt, along with passwords that are typically 20 to 30 characters long, making them highly resistant to brute-force attacks. Access to their CRM systems is restricted to approved IP addresses, and communication is often done through anonymous Telegram accounts. In addition to these digital security practices, they also implement video surveillance and physical security at their premises.

Interestingly, these centers' rigorous security protocols surpass those of many legitimate institutions, as not all banking employees, for example, use such long and complex passwords. There's a lesson to be learned from their approach to security, even when used for malicious purposes.

Busting the Call Centers

In 2023, a major breakthrough in combating scam call centers was the takedown of a network spanning 16 regions of Ukraine, resulting in the arrest of 2,500 scammers. This operation highlighted how these call centers were not only targeting the citizens of Ukraine, but also victims across Europe, the US, and Kazakhstan.

One particularly notably case involved cooperation between Ukrainian and Czech police, leading to the arrest of scammers in both countries for their involvement in these scams centers. Even more striking, some of these call center operations were run from within prisons.

Despite the challenges brought by the ongoing war, the Ukrainian cyber police have remained steadfast, dismantling scam centers and arresting more criminals throughout the year. Their efforts continue to push back against the rising volume of phone scams in Ukraine.

With 24 years of experience in fraud prevention, Raisa has built a career spanning banking roles in Ukraine and Canada, and now serves with the EMA Association, dedicated to promoting safe, cashless payments across Ukraine. A passionate advocate for cybersecurity, Raisa combines education and entertainment to make complex topics engaging and accessible.Recognized by Ukraine's Ministry of Internal Affairs for contributions to the Patrol and Cyber Police, Raisa remains steadfast in the mission to ensure safer streets and secure data.

Raisa Fedorovska
Head of EMA Academy and CyberSecurity School,
Ukrainian Interbank Payment Systems Members Association "EMA"

MICHAEL WACHERT-RABL

ERSTE Group

Explainable AI in Fraud Detection Systems

At the conclusion of the first day of the DACH Fraud Summit, Michael Wachert-Rabl from Erste Group Bank AG delivered a highly technical presentation. Drawing from his extensive expertise in artificial intelligence, he shared the latest insights and strategies for enhancing AI explainability to improve fraud detection. This focus on explainable AI aligns with the financial sector's growing emphasis on transparency and accountability in AI applications.

Black Box-less Approach

Michael began his presentation with s straightforward theory: transform the "black box" nature of typical AI into something more tangible and understandable for humans.

A primary driver for this shift is compliance. Regulations increasingly mandate transparency in AI and machine learning models used in anti-fraud—essentially eliminating "black boxes". This demand for explainable, traceable models can feel contradictory to the opaque nature of complex AI systems.

Beyond compliance, transparent models bring direct benefits to organizations. The more interpretable a model is, the easier it becomes to refine it and trust its accuracy. Understanding a model's decision-making process allows for precise adjustments, enhancing reliability and confidence in its outcomes.

Explainable AI Driven by Regulation

Michael highlighted three core motivations for considering Explainable AI: Regulation, Data Science, and Social Responsibility.

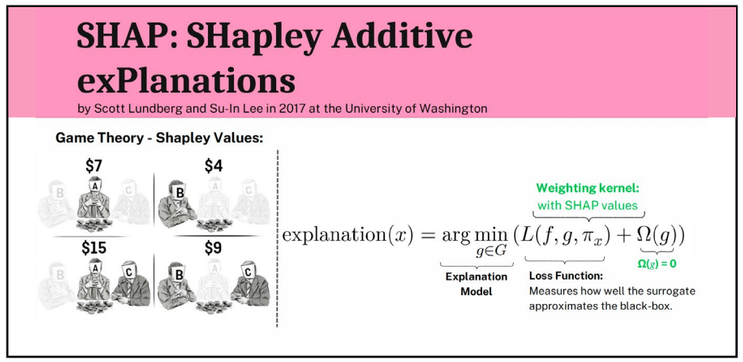
There are numerous regulations that mandate transparency in AI:

- PSD2 (2019) and PSD3 (2024): The Payment Services Directive requires banks to use machine learning for fraud detection, setting a high bar for transparency.
- GDPR (2019): Under the General Data Protection Regulation, data controllers must provide understandable information about the logic behind data processing.
- EU AI Act (2024): High-risk AI systems are required to implement transparency and human oversight measures.

While black-box models can effectively identify fraud, their lack of transparency conflicts with regulatory requirements, which demand clear, human-understandable explanations. This creates a strong case for the use of Explainable AI in fraud prevention systems.

Explainable AI Driven by Data Science

The second driver, Data Science, emphasizes the need for AI/ML models to be explainable to facilitate continuous improvement. It is as simple as that. Michael compared two common approach-



es used in fraud detection. The first, a traditional rule-based approach, was considered effective 10 years ago. However, Michael argued that maintaining such systems has become challenging in today's evolving threat landscape. As highlighted throughout the ThreatMark DACH Fraud Summit 2024, fraudsters adapt quickly, learning and countering new measures adopted by banks. They adjust their tactics based on past failures, often succeeding in their next attempt. Given this rapid adaptation, maintaining rule-based systems becomes inefficient and ultimately leads to inaccuracies.

An alternative approach based on machine learning is becoming more widely adopted. Unlike the rule-based method, the machine learning approach is more flexible and somewhat self-learning, allowing for automated adaptation. However, fraudsters continue to evolve their tactics regardless of the monitoring approach, necessitating frequent model retraining—much of which is automated. The challenge, however, lies in understanding precisely what was retraining as AI/ML models are inherently difficult to interpret. This brings us back to the critical need for explainable AI.

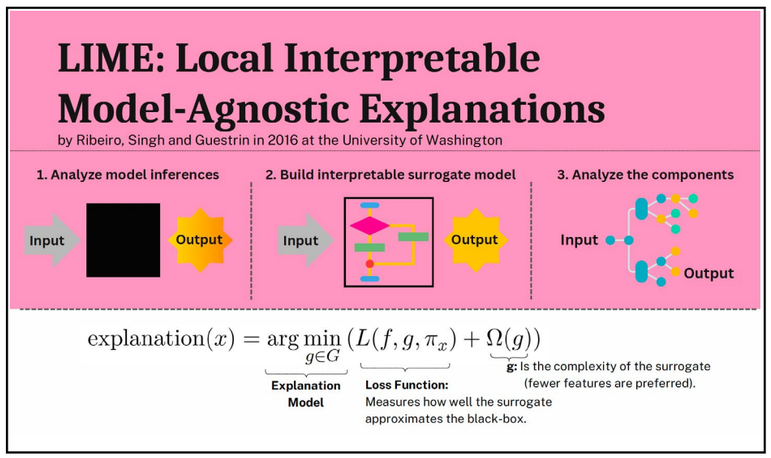
LIME, (Local Interpretable Model-Agnostic Explanations), is one of the most effective methods to address the challenge of interpretability. Particularly useful for explaining individual cases, LIME provide clear insight into why specific transactions are flagged as fraudulent. By generating local explanations, it focuses on interpreting the model's decisions for one transaction at a time rather than attempting to explain the entire model's logic. By adjusting the inputs around a single transaction, the user can observe how slight changes affect the model's output, helping to identify key features—like transaction amount, location, or frequency—that contribute to a fraud prediction.

However, LIME has limitations, primarily due to its reliance on a linear approach to interpretation. While linear models are simpler and more accessible, they may oversimplify the complex, nonlinear relationships within advanced fraud detection models. As a result, LIME may not fully capture the intricacies of these algorithms. Nevertheless, it remains a valuable tool for regulated industries that require interpretable explanations for black-box decisions, striking a balance between transparency and the simplicity of explanations.

Another approach to explainable AI in fraud detection that Michael mentioned is SHAP, or SHapley Additive exPlanations. Unlike LIME, SHAP doesn't shy away from model complexity and provides consistent explanations by assigning each feature a "Shapley value." These values indicate each feature's impact on the model's prediction, breaking down even highly complex models into comprehensible sections. By calculating each feature's contribution to the final decision, SHAP gives a clear view of why a particular transaction is flagged as fraudulent, whether due to transaction size, unusual locations, or other specific factors.

SHAP stands out for delivering both local and global interpretability, meaning it can explain individual fraud cases while also offering insights into broader model patterns. While this depth of insight is particularly valuable for highly regulated industries, it requires more computational power than simpler techniques like LIME. However, the additional complexity allows SHAP to capture detailed interactions between features, making it ideal for understanding nuanced decisions in advanced fraud detection systems.

Michael also outlined the future of explainable AI methods. Based on recent developments, he suggested the optimal path forward involves adopting Post-Hoc explainability methods. As the name suggests, Post-Hoc explainability techniques are used to interpret and understand a machine learning model's decisions after it has been trained.



Rather than altering the model's original structure, Post-Hoc methods provide explanations by analyzing the model's behavior on specific inputs or by examining patterns in its outputs. The goal is to turn "black-box" models, such as complex neural networks, into "white-box"—enhancing their transparency and interpretability.

Michael Emphasized that leveraging advanced Explainable AI algorithms within a "white-box" approach will be key to achieving this balance between model complexity and clarity.

Explainable AI Driven by Social Science

Michael concluded the presentation with the final driver, Social Science, which fuels the need do explainable AI. He emphasized that human explanations have specific qualities that should guide the development of explainable AI, making it more intuitive and relatable.

One key aspect is that explanations are contrasting; people often want to know, "Why this prediction and not another?" AI models that provide contrasting explanations can help users see why a particular outcome was chosen over others, aligning with natural human reasoning. Explanations are also inherently social; they need to fit the audience's background, whether the audience consists of experts or non-experts. Adapting explanations to the audience's level of expertise makes them more impactful and comprehensible.

Michael further examined how explanations are selected. Humans prefer a limited number of reasons behind an outcome, as too much information can be overwhelming. This selectivity can be applied in AI to focus on the most relevant factors, improving clarity and trust. Lastly, explanations often align with prior beliefs; people are more likely to accept explanations that fit with what they already understand. By incorporating these principles, explainable AI can become more effective in delivering insights that feel natural and credible to users, bridging the gap between complex machine logic and human intuition.

In the context of the human explanation, Michael highlighted the influence of Explainer Bias—where explanations generated by an AI model, or by a tool designed to interpret the model, can be shaped by the preferences or assumptions of the person creating or selecting the explanation, rather than accurately reflecting the model's true behavior. This bias can distort the interpretation of the model's decisions, either by oversimplifying, exaggerating, or omitting critical aspects of how the model works.

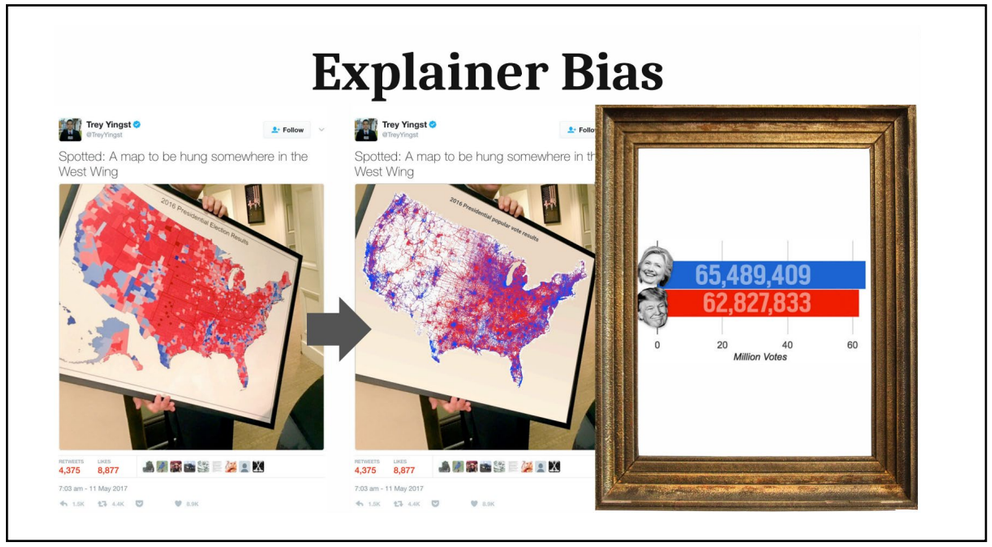
In practice, explainer bias can arise in a few ways. For example, when using post-hoc interpretability methods like LIME or SHAP, the person creating the

explanations might select features or results that align with their own understanding or beliefs, rather than presenting a more neutral or complete view. This can lead to explanations that feel intuitive or satisfying but may not fully represent the model's reasoning.

Takeaways

In closing, Michael brought together the essential points from his talk, sharing key takeaways for building anti-fraud systems with a focus on Explainable AI. He stressed the importance of integrating explainable AI tools like LIME and SHAP in the development process, ensuring that both developers and stakeholders can understand and trust the system's decisions. By using these tools, teams can create fraud detection models that don't just make accurate predictions but also provide clear, understandable insights into how those predictions were made.

Michael also pointed out that this transparency can be strategically advantageous in high-stakes situations, such as legal disputes. With explainable AI, you have a rich source of data to interpret and present as evidence, leveraging explainer bias to frame the interpretation in ways that support your case. He emphasized the value of hybrid models, which combine machine learning with rule-based signals to identify fraudulent activity. In this approach, machine learning can handle detailed, specific tasks, while rule-based systems flag known red flags of fraud, creating a powerful and versatile anti-fraud system.



Michael Wachert-Rabl is an AI Security Officer at Erste Group Bank AG, where he oversees the secure development and deployment of AI and machine learning-based IT solutions. His recent academic research centers on the application of explainable AI techniques within complex algorithmic decision-making, providing human-readable explanations for AI system outputs.

Michael Wachert-Rabl
AI Security Office, Erste Group Bank AG

LUKÁŠ JAKUBÍČEK

ThreatMark

From Fraudsters to Fraudsters

How (un)easy is it to launch and manage a phishing campaign? Do fraudsters have something at their disposal today that makes their lives easier? This is exactly what Lukáš Jakubíček, Lead Principal Solution Consultant at ThreatMark, decided to explore in the first presentation of the DACH Fraud Summit 2024.

To conduct the research, he collaborated with a team of security experts from the ThreatMark Cyber Fraud Fusion Center (CFFC), whose main agenda is the detection and elimination of phishing sites targeting ThreatMark's customers worldwide. They guided him to a service called FraudApp*, which Lukáš examined in more detail and shared the results of its usage.

Challenges in Creating a Phishing Campaign

Creating a successful phishing campaign presents several challenges for the fraudster. First and foremost is the infrastructure itself: purchasing a credible domain and securing hosting, all under the veil of anonymity.

Next comes the creation of the site itself, which will collect information from unsuspecting users. It must meet certain criteria, such as:

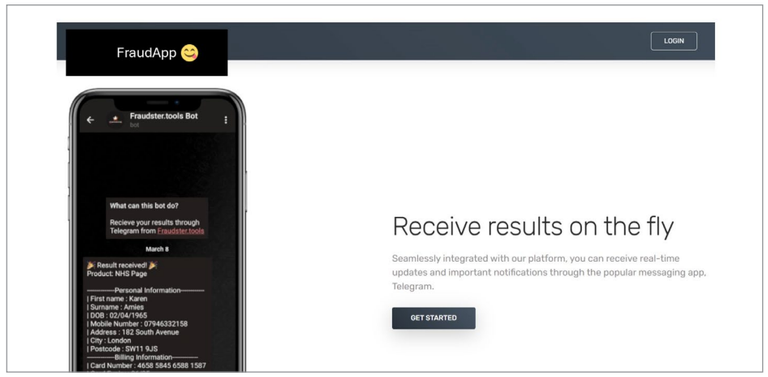
- ·Ensuring the anonymous transmission of data from "phished" users to the fraudster (e.g., to Telegram account).
- Developing mechanisms to disguise anti-phishing services. This includes, for example, restricting the availability of the phishing page only to users from the country targeted by the fraudster's campaign, complicating the efforts of various online services aimed at detecting phishing sites.
- Maximum possible similarity to the legitimate site, including functionality.
- Quickly deploying another phishing page in case the original one is detected and taken down.

Another challenge for the fraudster is acquiring a database of contacts (e-mails or phone numbers) to which messages with a link to the phishing site will be sent. Such a database can be relatively easily obtained on Darknet. A compromised e-mail server or SMS gateway can be utilized for distributing e-mails or SMS.

Finally, the functioning phishing page must be constantly updated to accurately reflect the appearance of the legitimate site with the bank's login dialogue. As can be seen, there are numerous challenges, and at many points in the process, the attacker risks exposure.

Phishing as a Service

As As is apparent, creating and maintaining a phishing campaign presents significant technical chal-



*To avoid unintended promotion of the service or misuse of information in the text, the name of the application was intentionally changed.

lenges. However, this is changing with the advent of FraudApp (and others). FraudApp represents a highly sophisticated, easily scalable, and, not least, highly profitable business that requires no special knowledge – Phishing as a Service (PhaaS).

Using PhaaS does not even often require visiting the Darknet. FraudApp attracts potential customers with a professionally looking website on a Clearnet where interested parties can find a catchy description of all its functionalities. These emphasize user-friendliness, efficiency, and security. All the texts carry the tone of typical "marketing lingo" we are used to seeing on legitimate service websites.

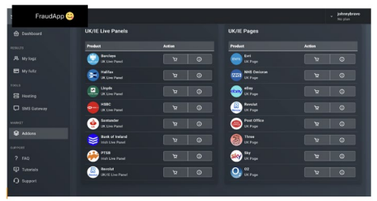
But here is where all similarity with the legitimate world ends. Features such as sending SMS messages with the ability to change the Sender ID, sending information about victims to Telegram in real-time, and many others, speak the clear language of fraud.

The lofty marketing description effectively assures the customer that with this service, virtually anyone from anywhere can very efficiently launch and run a phishing campaign, all in complete anonymity. And it must be said that it is not deceptive advertising...

Fully Functional Platform

After a quick registration and login to FraudApp, users are surprised by the impeccable craftsmanship and the multitude of features, which understandably exceed the capabilities advertised on the homepage. Fraudsters can easily purchase phishing templates (so-called phishlets) tailored to specific banks and other services in the user interface. They even have the option to filter selections by the countries in which the banks operate and examine in detail what can be stolen using the given template (e.g., credit card information, OTP, PIN, activation codes for app onboarding, and more).

Of course, there is also a list of already phished users, including data needed for further actions. Provision of hosting and SMS gateway features are also possible, with the option to purchase additional feature packages as add-ons.



Lastly, there is access to customer support (via Telegram), tutorial videos, a frequently asked questions (FAQ) section, and the option for remote support. All of this points to a lively user community.

The fact that FraudApp is very customer-centric is evidenced by a suggestion button. Users can use it to highlight missing functionality and thus provide invaluable feedback to the author/authors of the service.

Investigation – Additional Banks Targeted by Fraudsters

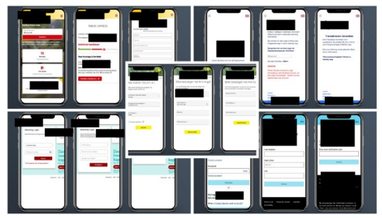
During his investigation, Lukáš noticed that in the phishlet preview tab, there was a reference to an image whose URL looked approximately like this: *"…/incl/assets/images/previews/13.png"*.

It then made sense to manually check for additional images (expecting numerical sequence in the URL). By doing so, Lukáš accessed 39 different previews (compared to the 16 published in the GUI).

It was evident that the previews included banks (specifically 23) that are not yet officially available in the service but will be soon. ThreatMark, of course, contacted these institutions and informed them about the potential increase in phishing sites.

In conclusion, it is worth mentioning that the ThreatMark CFFC team discovered a vulnerability in FraudApp, which makes it possible to extract the data of all victims from the service and subsequently prevent financial losses in cooperation with the banks.

Finally, it is fair to say that FraudApp thankfully does not seem to be available on Clearnet anymore. It is, however, disturbing that it lasted there for several months and that it is quite sure that similar services will be popping up massively in the future.



Lukáš has over 15 years of experience in IT and the online world. His close collaboration with security experts at ThreatMark has given him deep insights into cybersecurity and a comprehensive understanding of the technologies that fraudsters use online. Working alongside machine learning experts, programmers, and fraud analysts, he contributes to the development of next-generation fraud prevention solutions for digital channels.

As a speaker, he regularly participates in both domestic and international cybersecurity conferences and provides training to fraud analysts worldwide. He works closely with the ThreatMark Cyber Fraud Fusion Center (CFFC), which is at the forefront of combating online fraud. Through daily communication with cybersecurity experts and fraud analysts, he maintains a comprehensive overview of current cyber threats and effective prevention methods.

Lukáš Jakubíček
Senior Solution Consultant, ThreatMark


DACH
FRAUD
SUMMIT
The biggest anti-fraud conference
in DACH region
ORGANIZER:
ThreatMark

CLAIRE MAILLET

Key Insights & Strategies from the UK Banking Sector

The second day of the DACH Fraud Summit 2024 was kicked off by Claire Maillet, a counter-fraud expert from the United Kingdom, who aimed to share key insights and strategies from the UK banking sector. Claire's presentation focused on three key aspects of counter-fraud. She began by outlining the UK regulations for fraud offenses, highlighting how legal frameworks are adapting to the complexities of the digital landscape. She then delved into her PhD research on insider fraud, exploring the risks posed by internal actors and the strategies that organizations can employ to detect and mitigate these threats.

Claire also addressed stuttering, a condition that can pose challenges for counter-fraud and verification systems. She explained that stuttering often leads to false positives, complicating efforts to accurately identify legitimate cases of fraud, and emphasized the need for greater awareness and inclusivity within the industry.

UK Regulation for Fraud Offences

The timeline of counter-fraud legislation in the UK showcases the country's evolving efforts to tackle digital fraud. The first significant milestone was the Fraud Act of 2006, which officially recognized digital fraud as a criminal offense, coming into force in 2007. This was quickly followed by the Serious Crime Act of 2007, which focused on anti-money laundering (AML), and then by the UK Bribery Act of 2010. After some delay, the well-known PSD2 directive was adopted in 2018, incorporating numerous anti-fraud measures aligned with GDPR regulations.

Most recently, the Economic Crime & Corporate Transparency Act (2023-2024) represents the UK's latest attempt to combat fraud. This act, which came into force in 2024, aims to increase transparency by mandating the registration of businesses. However, concerns have been raised about the lack of checks on the listed companies and the absence of proper fraud prevention mechanisms on the registration website. Alarmingly, it is possible to create a fake company in under 30 minutes for as little as €15, exposing a lack of data protection in the system. Despite this, the legislation introduces penalties for large businesses if fraud is perpetrated from within the company. The act is expected to be fully enforced by November 2024, marking a significant step in the UK's fight against economic crime.

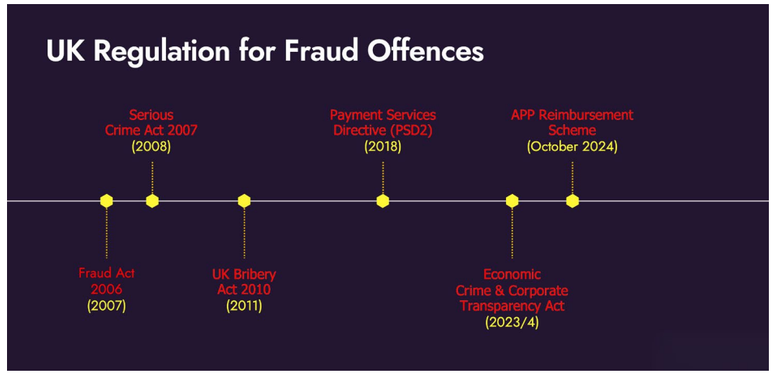
The APP Reimbursement Scheme is undoubtedly one of the hottest topics in the global anti-fraud community right now. Set to come into force on October 7, it aims to tackle authorized push payment fraud, a growing concern in the financial sector. The scheme introduces a threshold for negligence, meaning that banks will find it very difficult to prove customers are at fault in most cases.

Additionally, the APP Reimbursement Scheme mandates that both sending and receiving firms split the reimbursement cost equally and process these refunds within five business days. This creates a shared responsibility between institutions, promoting more diligence on both ends of a transaction. Moreover, firms are expected to adopt the Confirmation of Payee (CoP) system, a measure designed to ensure that payments are made to the correct account holders, further reducing fraud risks.

For vulnerable customers, the scheme goes even further, offering reimbursement without assessing gross negligence or first-party fraud. This ensures that those who may not have the means or knowledge to protect themselves from complex fraud schemes are protected, emphasizing a strong focus on consumer welfare. While it is promising that regulators are acknowledging the severity of fraud, there is concern that the scheme could unintentionally encourage complacency. By ensuring people are reimbursed for fraud losses, some worry that it might teach individuals not to be as vigilant with their money and could even open doors for people to exploit the system by mimicking fraudulent activities. Despite these concerns, the scheme represents a critical step in recognizing and addressing fraud on a wider scale.

PhD Research into Insider Fraud

In the next part of Claire's presentation, she delved into her PhD research on the equally critical issue of insider fraud. Her research aims to explore the vulnerabilities that FinTech companies face regarding insider fraud and to propose strategies that can mitigate this growing risk.



The primary objectives of her research include identifying the underlying reasons for insider fraud within FinTechs, analyzing the weaknesses and vulnerabilities in existing fraud control systems, and exploring how FinTechs can better protect themselves. With FinTechs being highly data-driven and fast-paced, understanding and addressing these internal risks is key to their long-term resilience against fraudulent activities from within.

Claire's PhD research was particularly timely, beginning during the onset of the global pandemic, which drastically altered the way we work and reshaped the fraud landscape. One of the key justifications for her study is the limited research available on insider fraud, as most fraud studies focus on individuals as victims rather than organizations.

Existing research has largely explored insider fraud as a crime affecting long-standing financial institutions, such as banks, or has focused on understanding the causes. However, there's a significant lack of practical, empirical-based solutions for reducing insider fraud within newer, fast-growing sectors like FinTech.

Claire's research bridges the gap between academia and practice by offering actionable, operational controls and measures to combat insider fraud. Her work is unique because it draws on both academic insights and real-world business experience, providing a holistic approach to tackling insider fraud, especially in the post-COVID era.

The research builds on existing studies that explore the often-overlooked issue of insider fraud. Prior research, such as Shepherd's (2016) work, highlights how some organizations passively accept internal fraud, while others take a more aggressive stance. However, many employers use various rationalizations to justify their inaction when dealing with fraud, as noted by Shepherd and Button (2019). The fear of addressing fraud often generates more anxiety than the fraud itself, underscoring the discomfort organizations feel about launching investigations.

Furthermore, Killingsworth's (2013) research reveals that individual morality can be easily influenced by social and situational factors, suggesting that even morally strong employees may be susceptible to committing fraud under certain circumstances. In the UK, insider fraud is rarely discussed, as employees are often hesitant to report it, and companies fear the repercussions of a fraud investigation more than the fraud itself. This reinforces the idea that everyone has a breaking point, and even trustworthy employees might engage in fraud if placed in compromising situations.

Initial Insider Fraud Research Findings

Claire's initial findings on insider fraud underscore a key challenge: denial. Organizations struggle to accept that their own colleagues or friends might commit fraud, making external fraud easier to anticipate than internal. Surprisingly, trust emerges as a primary counter-fraud control in many organizations. However, this reliance on trust often leads to a lax approach toward formal policies, as employees believe trust alone is a sufficient safeguard. While trust fosters a sense of security, it ultimately proves to be an ineffective measure in preventing internal fraud, as adherence to established policies is compromised, leaving companies vulnerable.

Claire's research further highlights several pressing issues facing FinTechs, starting with their priorities. These companies are often laser-focused on rapid growth and profit, putting customer satisfaction ahead of everything else. As a result, risk management, compliance, and financial crime prevention are often relegated to the background, leaving gaps in their fraud prevention strategies. Fraud is not seen as a pressing issue, as it is overshadowed by the drive for financial success.

The topic of whistleblowing also surfaced as a significant weakness. Employees often feel discouraged from reporting wrongdoing, assuming that if they do not hear back after filing a report, nothing is being done. This silence erodes their confidence, making them less likely to report future incidents. Additionally, staff members who are designated as whistleblower contacts are often unaware of their responsibilities or the process itself. The whistleblowing framework in the UK is perceived as broken, with little protection for those who report, which deters individuals from coming forward.

Lastly, Claire critiqued the pervasive "tick-box" culture in FinTechs. Compliance and fraud training are often reduced to mere formalities, where the focus is on completing a task rather than ensuring employees truly understand the content. This lack of engagement harms retention of critical information. In the UK, the rising cost of living and other external stressors are causing employee well-being to deteriorate, further increasing the risk of internal fraud. When personal struggles bleed into the workplace, employees may be more inclined to commit fraud, compounding the vulnerabilities within these organizations.

Claire is a counter-fraud expert with 10 years' experience in financial crime prevention, specializing in FinTech fraud. Pursuing a PhD in Criminal Justice Studies, she explores insider fraud and has led award-winning initiatives in counter-fraud and inclusion. A sought-after speaker, Claire shares insights through keynotes, a video podcast, and webinars.

Claire Maillet
Counter-Fraud Expert, UK PhD Student of Insider Fraud

DANIELE SANGION

Bank Austria
Member of UniCredit

Fraud in the Age of AI and Deepfakes

Daniele Sangion, Chief Security Officer at UniCredit Bank Austria, delivered his keynote on the second day of the summit, aiming to connect the dots between broader cybercrime trends and specific cases of online fraud. In his presentation, Daniele also addressed several important topics, including the evolving cybercrime landscape and its impact on fraud. He highlighted the increasing threats posed by AI and deepfakes, emphasizing the urgent need for stronger international cooperation.

Additionally, Daniele outlined Austria's collaborative efforts in combating cybercrime and shared actionable insights on how joint initiatives can effectively tackle these emerging challenges. These key points formed the foundation of his presentation, underscoring the importance of a unified approach in the fight against cybercrime.

Evolving Landscape of Cybercrime and Impact on Fraud

Based on his research and experience, Daniele identified several pressing issues. He pointed to the increasing cyber inequity between organizations that are cyber-resilient and those that are not, with small to medium enterprises (SMEs) showing a significant decline in resilience. In other words, SMEs tend to overlook fraud. He warned that emerging technologies will likely exacerbate existing challenges to cyber resilience.

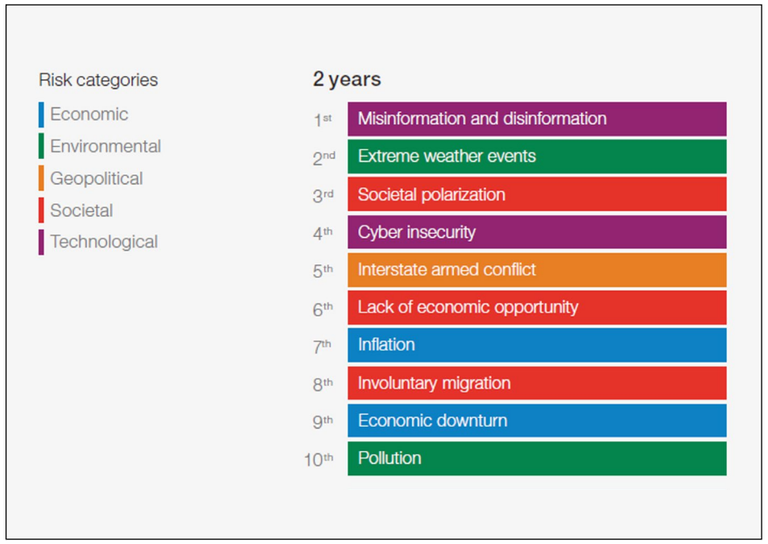
Furthermore, Daniele highlighted the growing shortage of cyber skills and talent, which is expanding at an alarming rate. While the alignment between cyber and business strategies is becoming more common, he noted that this largely depends on the sector. Finally, he discussed the growing risks within the cyber ecosystem, particularly in supply chains, which are becoming increasingly problematic.

Daniele continued by pointing out the alarming rise in cybersecurity attacks, which are setting new records in both the variety and frequency of incidents, as well as their increasingly severe consequences. He stressed that ongoing regional conflicts remain a major factor shaping the cybersecurity landscape, with hacktivism steadily expanding, particularly around significant events like the EU elections. There are seven key cybersecurity threats: ransomware, malware, social engineering, threats to data, availability attacks (such as denial of service), information manipulation, and supply chain attacks. He also noted that organizations in public administration, transport, and finance were the primary targets of these attacks.

Daniele concluded this part of his presentation by referencing the World Economic Forum's Global Risk Report 2024, which highlighted the growing dominance of technological risks. According to the report, misinformation and disinformation were ranked as the top global risk over the next two years. Cyber insecurity also rose significantly in the rankings, moving from 8th place last year to 4th, underscoring the escalating urgency of cybersecurity challenges in today's increasingly connected world.

Threats Posed by AI and Deepfakes

Daniele transitioned to discussing the growing threats posed by AI and deepfakes, providing compelling examples to highlight their alarming impact. In 2019, a CEO in the UK was targeted by fraudsters using voice-generating AI software to impersonate the CEO of the parent company, resulting in an urgent wire transfer of £243,000. By 2024, these attacks had become even more sophisticated, as shown by an incident at a multinational company in Hong Kong, where a clerk was deceived during a video call with deepfaked colleagues and the chief financial officer, leading to a fraudulent transaction of €23 million.



Daniele further explored the implications of deepfakes in the context of fraud, highlighting several critical risks.

1. One significant concern is the use of deepfakes to deceive customers or staff into authorizing fraudulent transactions, making it easier for fraudsters to execute unauthorized activities.
2. This has led to an increase in fraud attempts, as these technologies provide new opportunities for malicious actors.
3. Additionally, the risk of data breaches rises when deepfakes are used to trick employees into revealing passwords or sensitive information, or even granting remote access to computers.
4. The potential damage to a company's reputation is another serious issue; if systems are compromised through deepfake technology, it can severely undermine the organization's credibility.
5. Lastly, Daniele noted that these challenges create compliance hurdles, complicating efforts to adhere to regulatory requirements.

Urgent Need for Enhanced Cooperation

Daniele then shifted his focus to the urgent need for enhanced cooperation in tackling the escalating costs of cybercrime, which are projected to reach a staggering $10.5 trillion annually by 2025 as estimated few years ago by Cybersecurity Ventures, attributing this dramatic increase to several critical factors, including the rise of nation-state-sponsored cyber activities, organized crime, the rapid expansion of the attack surface, and a growing reliance on digital infrastructure across various industries. Emphasizing collaboration, Daniele argued that a unified approach is essential for effectively addressing these complex challenges and mitigating the associated risks.

Continuing his presentation, Daniele highlighted key takeaways from the ISC2 Cybersecurity Workforce report. He revealed that the global cybersecurity workforce currently stands at approximately 5.5 million professionals. Alarmingly, the workforce gap is expanding even more rapidly, having grown by 13% since 2022. This means that in 2023, there was a pressing need for roughly 4 million additional cybersecurity professionals worldwide. Daniele emphasized that addressing this gap is critical to strengthening global cybersecurity efforts.

Austria's Collaborative Efforts and Actionable Insights

Concluding his presentation, Daniele focused on Austria's collaborative efforts and actionable insights aimed at combating online fraud. He introduced a new alliance designed to bolster protection against phishing, highlighting a recently established platform that facilitates collaboration among banks, payment services, and law enforcement agencies. This initiative aims to strengthen cyber defenses against potential fraudsters, embodying the motto "exchange and networking for the benefit of customers." The launch event for this platform against data phishing took place in November 2023, hosted by the Federal Ministry of the Interior and the Federal Criminal Police Office, marking a significant step forward in Austria's fight against cybercrime.

Daniele emphasized that the common goal of this collaborative effort is to defend the financial system against phishing attacks and online fraud. He asserted that individual efforts are no longer sufficient; instead, intensive cooperation is essential for effectively combating cybercrime and minimizing its impact. In an increasingly digitalized economy, such collaboration becomes crucial. Together, banks, payment services, and law enforcement aim to close gaps in defense strategies, identify threats at an early stage, and apprehend as many perpetrators as possible. Daniele's insights underscored the importance of a united front in safeguarding the financial sector and protecting consumers from online threats.

CISO/CSO and Head of Digital Transformation at UniCredit Bank Austria, with over 25 years of experience in digital transformation and cybersecurity. He has led key initiatives within UniCredit Group, including GDPR compliance and Third Party Risk Management. A Board Member of KSÖ and advisor to cybersecurity organizations, he holds a distinguished Computer Science degree and multiple certifications in IT and management.

Daniele Sangion
CISO/CSO and Head of Digital Transformation,UniCredit Bank Austria

DANIEL STIRNIMANN Switch

Unraveling the Phishing Puzzle

The concluding speaker of the DACH Fraud Summit 2024 was Daniel Stirnimann, a Security Expert at Switch. He began by briefly introducing Switch and Switch CERT, a non-profit foundation based in Switzerland that employs around 180 people. They serve the Swiss National Research and Education Network (NREN), which includes approximately 400,000 students, staff, and researchers. Switch provides a variety of services, including academic backbone infrastructure, security solutions, identity management, and cloud services.

In addition to these offerings, Switch manages the domain registries for Switzerland (.ch) and Liechtenstein (.li). The Switch CERT team, made up of over 40 professionals, focuses on cybersecurity for Swiss universities and oversees the security of the registries. Furthermore, Switch CERT operates as a multi-sector cybersecurity entity, providing services to the finance, energy, industry, and logistics sectors across Switzerland.

Phishing Trends in Switzerland

The core of Daniel's contribution to the gathered anti-fraud forum was about phishing detection and mitigation possibilities with the highest possible level of automation. First, he shared some trends around reported phishing within the Swiss financial industry.

Another pretty straightforward approach is to simply examine the HTML source code of the phishing site. Quite often, it contains the Telegram token as well as the chat ID.

After exploring multiple phishing kits, Daniel concluded that they typically follow specific frameworks, which allows fraud fighters to increase automation of the mitigation process and enhance overall anti-phishing countermeasures.

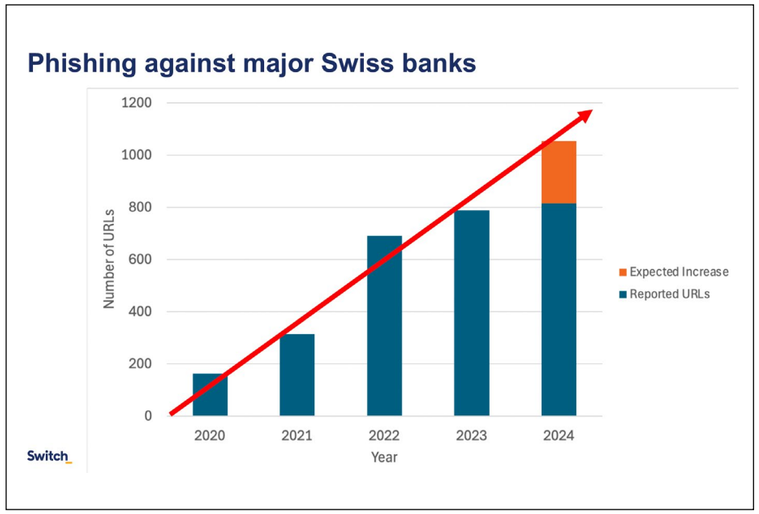
Daniel formulated three key pillars for making phishing detection and mitigation more effective. The first is information gathering. In summary, this involves collecting as much information from the phishing sites as possible, including scanning the HTML code for certain structures and keywords. This is followed by phishing kit identification, after which appropriate measures are taken to exploit the vulnerabilities that fraudsters leave open for automated and semi-automated ethical hacking.

Daniel concluded by sharing some surprising statistics about vulnerabilities in phishing kits, which are seen as positive for ethical hacking. He revealed that more than half of all tracked phishing kits targeting the financial sector contain vulnerabilities. Even more promising, many of these have vulnerabili-

ties that offer a very high chance of data recovery, demonstrating opportunities for ethical intervention and sector protection.

Finally, apart from the three key pillars of the framework, Daniel revealed the rest of the steps that form it. The entire framework then looks as follows:

1. Phishing URL detection or reporting.
2. The phishing kit used in the attack is identified, allowing for a better understanding of the threat. Any deployment errors associated with the phishing site are then detected, which may provide insights into the attacker's methods.
3. The next step involves exploiting vulnerabilities present on the phishing URL to gather further intelligence.
4. Monitoring of drop data from the phishing page is conducted continuously.
5. This data is shared with the victim bank to help mitigate the impact of the attack.
6. Finally, steps are taken to initiate a domain takedown or report domain abuse, aiming to disrupt the phishing operation and protect potential victims.



Surprising Statistics

Daniel concluded his presentation by sharing some up-to-date statistics from the ongoing phishing hunt in the Swiss region.

What was surprising were the phishing detection and, more importantly, the drop data reports when looking outside of the financial segment. Daniel and his team also monitored the drop data for other sectors. It turned out there were far more drop data reports than for financial institutions. The conclusion drawn is quite clear: fraudsters tend to be far more successful when targeting non-financial institutions for collecting personal information from citizens.

Daniel Stirnimann is a security export at Switch. He is responsible for the DNS infrastructure at Switch including the ccTLDs .ch/.li and works on e-crime and malware incidents for the financial sector.

Daniel Stirnimann
Security Expert, Switch

How Participants Rated the DACH Fraud Summit 2024?

The summit was preceded by great preparations, but also by some uncertainty. Many registrants had attended some of our Fraud Summits in the past, but for most it was their first time. Although the agenda and topics looked very promising, without prior experience they did not know what they were getting into.

However, any fears were allayed by the very friendly atmosphere from the very morning and the very first presentations which made it clear that we were all in the same boat, here with the same goal and that the presentations would focus on passing on quality know-how without any sales presentations from the organiser or anyone else.

The good feeling of the conference was enhanced by the results of the questionnaire survey, which aimed to collect qualitative and quantitative feedback:

- **100%** of participants answered "Yes" when asked if they would attend again.
- **9.2/10** is the average rating of the conference.

The most common response to the question "Could you indicate what you liked about the conference?" were:

- **Networking and Collaboration:** Excellent opportunities for networking and informal exchanges with colleagues from other banks and countries.
- **Valuable Content and Speakers:** High-quality, practical content with insightful presentations and discussions, particularly on emerging trends.
- **Great Organization:** The event was well-organized, with a relaxed yet professional atmosphere, and excellent catering.
- **Open and Engaging Environment:** Open discussions and a collaborative spirit among participants, with a focus on sharing knowledge and experiences.
- **No Sales Pitches:** The conference maintained a focus on valuable content without any sales presentations, enhancing its usefulness and relevance.

The evaluation, which was completed by dozens of participants in the questionnaire, can be summarized by the following answer: ***"As I am receiving a lot of conference invites, I was hesitating to come, to be honest. But I had a fantastic time at the conference! Thank you very much for bringing so many anti-fraud experts from different banks together. The networking was great, and I connected with many colleagues from other banks and countries. Presentations were fantastic and practical, I have so many notes and inspiration, and the organization was top-notch. I appreciated the open discussions and the absence of sales pitches, which made the event even more valuable. The best conference I have attended in past years. Great job, looking forward to the next one!"***


SPORT
LACK OF CENTRALISE


Vít Zeman
How is Erste Bank utilizing the machine learning approach - in combination with rule base syst
Latest question
Alexandra M
Could you ples re about the phishing lette tioned in his presentstion? W
content of the how successful they were?


DACH
FRAUD
SUMMIT
The biggest anti-fraud conference
in DACH region
10-40%


SUMMIT

Head: Jakub Zalman
Copy: Vojtech Hodes
Correction: Katerina Matesova,
Kate Elizabeth Burwood
Design: Tomas Halajcik
Photo: Petr Hrubes