Episode #08: English Transcript

Whatsapp-Signal

“Hey mom, my cell phone isn't working. Please text me on this number.”

Host Anna Wallner:

Have you ever received a message like this? Probably. This is what it sounds like when scammers target someone using the classic son or daughter trick. It usually starts with a few harmless messages back and forth and at some point comes always the request for a transfer. The son, daughter, or even grandchild supposedly can't access access their online banking anymore because of a new phone, but urgently needs to make an important payment. And that's how it begins. By now, almost everyone knows someone who has nearly or actually fallen for a scam. An online Romeo who after weeks of flattery suddenly needs money. The investment advisor who's discovered a new cryptocurrency promising unbelievable returns. Callers who tell mostly older people that something terrible has happened and that they are in danger. An entire industry has grown around this in some countries even operating under political protection. Therefore, we ask can the EU fight back? This is Lens EU episode 8. My name is Anna Vina. I've been a journalist at the Vienna Daily Depressive for about 20 years and among other things I'm responsible for. our audio section. So today I get to guide you through this episode. In the first part, we draw on an investigative series that ran in the press in early July with reporting by Christoph Zotter, Theresa Wirth and interactive tools by Kathrin Nussmayer. More on that later.

In this episode, we want to introduce you to two concrete areas of cyber crime. First, I'll talk to my colleague Theresa Wirth about her research into a massive fraud network that was uncovered after many years, the so-called Milton Group case. In the second part, we'll hear from Frida Thurm. She's senior reporter at one of our partner outlets, Corrective Europe in Germany.

A bit more about the context of this episode: The Global Anti-Scam Alliance, an organization whose members include big tech companies like Google and Apple, as well as banks and consumer protection groups, estimates that Around $442 billion US were lost to scams worldwide last year, roughly 386 billion euros. That means scammers generated an economic output comparable to that of an EU country the size of Denmark. What this actually means for Austria and the EU is what I'm about to ask my colleague Theresa Wirth. She's been a reporter at the press for several years covering stories from and around the capital Vienna. We started with a pretty basic question. What exactly do we mean when we talk about scams?

Speaker 2, Terea Wirth: The term is used for a scam where a perpetrator exploits

the trust of people of other people and it's about money or personal data. That's what they always want to get and it's well especially in German speaking countries actually often used in the context of the internet. So, anything that happens in cyber crime and fraud is called a scam. But also fake SMS or fake WhatsApp messages or calls, they are also meant by this collective term like the ones we heard at the beginning of the episode. Exactly. How many cases are there in Austria and the EU? Yes, that's a bit difficult to say in terms of numbers. I looked at that for Austria from last year, there were just over 30,000 reports of pure internet fraud. And then there's an extra point uh fraud offenses that includes all sorts of things including social benefit fraud, but also fishing SMS or WhatsApp messages, fraudulent calls are also included. And that was about 60,000.

Host, Anna Wallner: Hard to say, but in this range you could say because probably many of these cases uh involve a large number of unreported cases because many people are ashamed and don't report it.

Speaker 2: Exactly. That's what I was about to say. So these numbers don't sound like that much and that's because many people don't even report it to the police.

Host: And at the EU level?
Speaker 2: At the EU level I actually didn't find any numbers probably for a similar reason because it's such a huge field but the global anti-scam alliance released a report that published a damage figure for the past year and that was about 57 billion euros that were caused by scams in the EU in 2025. That's a lot. And they also did a survey according to which 3/4 of Europeans were confronted with fraud attempts last year. Of course, not everyone fell for it, but that is a really broad field.

Host: Can you say which countries or states are particularly affected?
Speaker 2: Well, I'd say all of them, but especially Western Europe, the richer countries, clearly France, Germany, the Netherlands, in Spain, there's also a lot. So, large amounts of damage. Also, Great Britain, which is not in the EU, but they also have really big, yes, always big amounts that are lost there.

Host: For your research on the topic, we had a big focus on the whole topic with a view to Austria, but also Germany and the EU. You spoke to a man who hunts million-dollar scammers in Europe. That was also the title of the story. Who is that?
Speaker 2: That's Nino Goldbeck, a senior public prosecutor in Bamberg, Germany, in Bavaria. And he is part of the central office cyber crime Bavaria and is really specialized in this this type of fraud scams. So, especially in these big investment fraud cases because uh I wanted to say that earlier that's really where the big money is made by the scammers. It's about huge amounts in Austria too. That's the sector where the most damage is caused.

Host: So that's for example when in large transactions between two companies an attempt is made to intercept and divert the money via the internet where suddenly millions so it's no longer about 5,000, 6,000, 10,000 or 30,000 of a private person but really about millions or billions.
Speaker 2: Exactly. Although it's also about a lot of money from private individuals. So it's really about this investment fraud where private individuals so to speak in invest in something or trust or something trust and are lured by great offers where they can invest money now and then lose huge amounts. In Austria for example there was a case where someone lost 11 million euros through such fake crypto investment fraud.

Host: I think many of us know cases with smaller and larger damage also in the family or circle of friends and you always have the feeling that you are so powerless because it's anonymous on the internet uh quickly gone. You can't find the criminals unlike the classic pickpocket who used to pull your bag out of the subway whom you might still not always but may be caught. So the question is how do you hunt these criminals?
Speaker 2: I asked Nino Goldbeck that and he also said yes in the beginning it's a huge opaque jungle so every case that happens in Bavaria goes across his desk and that's really very hard work to get to the perpetrators so what you have to do or can do is simply categorize all these cases systematically and see if there are any overlaps, the same the same account number, a phone number that is somehow the same.

And then, if you're lucky, a clearer picture emerges little by little and certain similarities of certain fraud cases or scams and see if there are any overlaps, the same account number, a phone number that is somehow the same.

International cooperation is also very important he said so when they realized okay there's a case where first of all half the world is affected also a lot of cases in Germany in Austria and also in the whole of Europe they then joined forces with other European countries and compared notes what do they know what do they know and then after years it must be said so it doesn't happen overnight They realized ah that's a big network of scammers who are just spinning the web.

Host: What is also well known by now is that in many of these scam cases hundreds of employees small fish are actually made to sit in call centers and lure people in. That is so to speak the connection to the physical world because they are real. These are like factory halls where many people sit in front of computers and are supposed to do these things. How does a razzia look like? How do you find a call center like that and how do you bust it, which was just recently successful?
Speaker 2: There are different ways. So either you follow technical clues as they call it in jargon. So those are either the voices of people like actual clues to specific people calling you or even names and so on although those are usually fake names it

must be said or IP addresses, email addresses or you follow the money trail. Account numbers to which companies, what are the names of the companies and so on and yeah, if you're lucky, you eventually find these scam centers or find out where they are. I'd also like to say really quickly, you already said there are hundreds of people, so it really is sometimes there are 600 people sitting in there and and really calling people around the clock promising them big money.

Host: Lets go back to Nino Goldbeck and to a very specific case, namely around the scam network Milton Group. What's that all about? Who were they?
Speaker 2: That was really a huge network. So, Milton Group was one of the names under which they appeared, but there were about 150 other names of certain investment groups and and companies under which they also scammed. They really got people to invest all over Europe.

Host: What I find particularly absurd is that one group, a platform belonging to this network even acted as a sponsor for the Spanish football club FC Sevilla. So that means they were really able to maintain the appearance of respectability quite well in individual cases.
Speaker 2: So not just in individual cases, there were really billions in damages. So really many people invested hundreds, thousands and at some point they had no money left and then they realized something was fishy. But that also took years first of all to get to that point.

Host: But the case is also so exciting because they actually found someone responsible. **Speaker 2:** Exactly. That was really a big fish actually which is rare that the masterminds actually get caught by investigators because they often disguise themselves and or sit somewhere else. But this one is a Georgian Israeli citizen stood trial in Germany and they were able to prove that he had on the one hand set up a scam center or scam centers in Albania and on the other hand had also developed a scam software so to speak to make it even easier to pull off certain scams. He then sold that to other scam centers and other scammers and that's how he made a lot of money.

Host: Mikael B. is his name. And how did the trial turn out?
Speaker 2: He was convicted. He made at least a partial confession and and is now in prison. Exactly. Which was also interesting because they were actually I mean they got on to him relatively quickly. Well, quickly is an exaggeration, but they got on to him early on, searched him in his apartment and so on during that one big razzia, but they couldn't apprehend him then because that was in Georgia. He is Georgian and you can't just arrest a Georgian as an international investigation team and German police. But then for some reason he traveled to Armenia and Armenia and Germany have an extradition treaty and that's how they were able to get hold of him.

Host: Where do the criminals actually set up these scam centers?
Speaker 2: Yes, mainly I mean if we're talking about Europe then it's Eastern Europe. So Albania, Georgia, Ukraine, …

Host: Southern Europe mainly.
Speaker 2: Southern Europe, yes. There is of course this is a a global problem. So Southeast Asia is also a very big market in that regard. It's a real industry there too. Exactly.

Host: And what exactly happens in these scam centers? Can you tell us? We can kind of imagine it. It's somehow you've already described it. Phone calls a lot of contact via various digital channels. But how do you picture it a scam center like that?

Speaker 2: Exactly. It's set up relatively professionally. That's also what the German investigator told me. First of all, there's an onboarding process. So those are the lower employees so to speak who call customers I mean prospective customers introduce themselves what's it about they have a a proposal for an investment then their details are taken down there might be a small initial deposit a lower amount so that it's not such a high barrier and if that was successful then these these customers are passed on to the conversion department and that is like the heart of the scam model that's where it's really about the big big amounts too. That's also where these supposed financial experts sit who who are then supposed to invest and multiply the money. And of course, they present themselves that way. And I then asked Mr. Goldbeck if the people working there all know that they are actually scamming people, that they are doing something illegal. And he said, "It could well be that in this first department when you call customers, you don't know what it's about. But as soon as you actually go further into this into this second in this…

Host: … conversion phase, right? Or is it already the third one?
Speaker 2: Exactly. Well, sorry. Conversion was the first, it’s the retention phase is the second. And there they also use fake names. Of course, you have to introduce yourself and say you're in Vienna, but actually you're in Tirana, in Albania, and there sooner or later everyone actually knows what they're doing. And It's also the case that they really earn extremely well. I mean, you can't compete with that with a normal salary in Albania, for example. So, we're really talking, he said, yeah, really good people who rake in a lot of money there. They earn 40,000 to 50,000 Dollars a month.

Host: Did he also say anything about whether so to speak in times like these AI has given a big boost to the whole industry because It's easier, for example, with translations that it's just much easier to say if I'm in Tirana and can speak German and English myself, but French and Spanish are already tough that I can do all of that more and more easily with both voice imaging and text.
Speaker 2: So, he didn't say that specifically, but in my other research, it also came out that this is really a new level of scamming. On the one hand, as you say, it's

about translations and also the messages are getting much better. So you don't have emails anymore with a thousand mistakes in them, but really perfectly formulated things, but also these fake platforms that you end up on, they're also perfectly made up to, you hear this in the media all the time anyway, fake videos being created, AI videos of celebrities who then, yeah, advertise for certain investments…

Host: With Armin Wolf, for example, the ZiB 2-Anchorman from ORF there was a case. Exactly.
Speaker 2: And influencers are also very popular targets for that to be exploited for.

Host: Tell us your opinion. Is the EU prepared enough for this problem?
Speaker 2: Well, definitely a lot is happening. They're really on top of it with international cooperation with Europol. So, that works relatively well. This one case I followed, there were actually ten countries involved, which then carried out raids in five other countries simultaneously. It must be said what is always a challenge is that now the local authorities also have to play along. So in some countries there are problems with certain criminals also having connections to decision makers through corruption and then maybe being protected.

The German investigators have said though that in most cases it does work out somehow. Maybe not perfectly as they had planned, but it does. But what also has to be said is that the authorities are lagging behind quite clearly. So this case I looked at the first scams were in 2016 and 2017. The razzia happened in 2022. The first major convictions were just this year practically ten years later. And that's just the beginning. So, it's going to go on. So, it's just always lagging behind. And Mr. Goldbeck also told me, you can be sure, you shut down one scam center and the next one pops up somewhere else immediately.

Host: So, this is like the hydra, you chop off one head and they're already back again.
Speaker 2: Exactly. Because it's just such a really lucrative business.

Host Read Anna Wallner:
Yeah. That doesn't exactly sound like confidence. One scam center gets shut down and the next one pops up somewhere else. The business is simply too lucrative which makes it all the more important that the bodies meant to coordinate these crossborder cases actually work in the European Union that's mainly one agency Europole. Our colleague Frieda Thurm from Corrective.Europe spent months investigating together with partner outlets in the UK and Greece how Europole actually handles sensitive data behind the scenes. Her findings shed new light on whether the EU is really equipped to fight networks like this.

Speaker 3, Frida Thurm:

I am Frida Thurm, a senior reporter at Corrective Europe in Germany. Through our investigation, we were able to show that the European Police Agency Europol has built a shadow IT system.

We at Corrective researched this together with Computer Weekly from Great Britain and Solomon from Greece.

So shadow it that is what the former Europol employees who told us about this system call it and that is because this involves an IT environment that ran parallel to the official systems and in it personal data was processed without any regard for data protection or IT security rules. You have to understand Europol is not a police force that can go out and investigate on its own. It is based in the HEG in the Netherlands and from there supports the police authorities of the European Union member states specifically when it comes to serious crossborder crime such as terrorism for example or organized crime.

So a great deal of information flows into Europol which is sent for example by the federal criminal police office from Germany or by the police authorities of other member states. However, the countries do not just send information they also receive analyzed findings in return.

Europol is therefore a kind of information hub and what the investigative authorities from the member states send can be quite sensitive. personal data, IDs, photos, phone connection records.

These are data that Europol is allowed to have but must handle very carefully. For example, quickly deleting data of completely uninvolved people. And that is exactly what did not happen as our research shows. And there is more. Because member states send increasingly large amounts of data, for instance, after the 2015 Paris terror attacks, there was a special permit at the time allowing this data to be processed and analyzed in an environment Originally intended only for rough presorting. That was the computer forensic network, the CFN. They wanted to evaluate quickly and provide findings to solve the crimes and potentially prevent further attacks. Understandable. But our research now shows it did not remain an exception.

But gradually the CFN developed into the platform of choice where the actual analysis work was done. Evaluating and drawing connections between people and places without Europol for first sorting which data we are allowed to keep and which not.

We have an internal report that documents this. In 2019, 99% of Europol's operational data was in the CFN. We recall a system that was actually only intended as a transit point. One of the former Europol employees we spoke with said, "A parallel system like that without security measures is simply cheaper and faster, but you are also at the mercy of the person behind the screen.

This means that who could access sensitive data and how it was used was apparently largely left to the discretion of individual employees. And that is also a problem because these mountains of data contain many people who have nothing to do with any crimes. For example, this could be phone connection data from people who happen to be nearby when an attack occurred and who could then end up in an analysis that Europol sends back to the member states. And that can of course have consequences for pretty much every area of life.

The European data protection supervisor also warns against this. It was not just the whistleblowers, the former Europol employees who spoke with us. We also have reports from an internal Europol task force that were never published and which we obtained through a freedom of information request. They show the conditions that prevailed in the shadow IT. It involved some quite serious security vulnerabilities. There was no proper logging of what users did in the system nor of what administrators did. That means it was unclear who accessed the data and also whether anyone had changed or deleted it.

So you can perhaps imagine why one of the whistleblowers described the system to us as a black hole. This internal task force then concluded that to solve the problems, Europol would actually have to abandon the system and set it up completely from scratch, but that did not happen. There were efforts to contain it. Some things have improved, says the European data protection supervisor.

But even today, 15 of the 150 problems he identified in this context remain unresolved. That is not all. We have found clear evidence including written proof that the CFN was not the only unregulated system. That is why the term shadow IT used by insiders is in my view entirely accurate.

The European Parliament has known since 2020 that there is a fundamental data protection problem at Europol. Back then, the European data protection supervisor reprimanded Europol for storing large uncatategorized data sets.

But as far as we know, Parliament was never informed that 99% of Europol's data was in the CFN and the public certainly was not. Nor were they told about the massive security problems. What was new to the European data protection supervisor from our research is that it apparently continued even after this, shall we say, partial admission by Europol.

You have to imagine while some of the parallel systems are being investigated, Europol it staff and an operational unit are arguing by email about a tool called pressure cooker and it is quite clear from these emails that this is not an official tool.

Europol by the way maintains the position that it always provided transparent information about its systems and that pressure cooker was just the nickname for an official system. But that does not align at all with the reports from insiders or with the emails we have. Insiders tell us that pressure cooker is also a shadow IT system

used to analyze sensitive data. In 2022, for example, someone from Europol's IT department warned by email that the European data protection supervisor might soon learn of the quote irregular situation with the pressure cooker and that their department had long warned against it. It becomes perfectly clear a system was kept secret from the European data protection supervisor for years.

The European data protection supervisor then responded to our investigation with interest. Two days after publication in May, the shadow IT was a topic in the European Parliament's Committee on Civil Liberties.

The European Data Protection Supervisor was there and confirmed that the allegations went beyond what he had previously known and that he intends to investigate.

Saskia Brickmont, who sits on the Committee on Civil Liberties for the Greens, said, quote: "The findings are shocking after so many years of oversight and alleged efforts to respect data protection and fundamental rights and Sipple, who sits on the committee for the Social Democrats, also said that the shadow it undermines trust in the reliability of evidence and the rule of law in European law enforcement."

Birgit Sippel, who sits on the Interior Committee for the SPD, put it this way: the shadow IT undermines trust in the evidentiary integrity and rule of law of European law enforcement.

And furthermore, quote, "Before we even enter into the discussion of whether Europol's mandate should be expanded, we need real parliamentary oversight and full clarification of what has remained hidden until today."

The relevant question now is whether the shadow IT is still being used today. There is significant evidence to suggest it is. One of the former Europol employees told us that an allegedly new tool which Europol just presented to the European data protection supervisor is actually not a new tool at all, but an attempt to retroactively legalize the pressure cooker. If that were the case, it would mean it is still in use today.

Europol, by the way, denies this. But even if it were just a planned tool, the data protection supervisor says it would pose a huge risk of becoming a complete parallel structure. That is what he wrote in his assessment. So one can say the problem is far from solved today and this at a moment when the commission is actually planning to double the budget and staff of Europol.

Meanwhile, a team of human rights lawyers has filed a complaint with the data protection supervisor on behalf of three people who assume they have ended up in this shadow IT. And as the legal team from the NGO front legs puts it quote with the result that she criminalized and intimidated the lawyers want to force Europol to shut down its shadow IT immediately.

The European data protection supervisor now has three months to respond to the complaint from those affected. If they do not issue a ban on processing for these parallel IT structures within this period, the lawyers have announced they will take the case to the European Court of Justice. They have already done this successfully against Frontex once before.

Host Anna Wallner:
So much about the corrective Europe investigation into Europol's shadow IT system. It shows us that even the agency meant to coordinate the fight against crossborder crimes like scams has its own blind spots. You'll find the full articles from Corrective.Europe in both German and English in the show notes for this episode.

Host Anna Wallner:

To wrap it up at the end of this episode, I want to come back to the question one more time. How do scammers manage to get parents or even grandparents to transfer thousands of euros to a stranger's account within just a few minutes. How do they even get cautious tech-savy people to miss the warning signs and fall into the trap? We at Depressive built an interactive simulation where for once you get to step into the role of the perpetrator. Unfortunately, the game is currently only available in German, but for German speakers, it's a fascinating tool well worth trying out because you can choose from different messages and experience step by step how the classic hi mom WhatsApp the one we opened this episode with is built up and which psychological mechanisms are behind it. The scammer messages you can choose from as well as the victim's replies are based on real chat logs.

Some shared online, others provided to us by the fraud unit of the Austrian Federal Criminal Police Office. Names have been randomly chosen, of course. Along the way, explanations pop up showing which manipulation technique was just used and why it works so often. Your simulated scam attempt can play out in different ways. Not every choice leads to success. I'll also put the link to the scam simulator in the show notes for this episode and say have fun trying it out.

Outro Host:
That was episode 8 of LensEU produced by “Die Presse”.

Thank you to Liliht Grul and Frieda Thurm, they both are colleagues from Corrective. Europe in Germany. And a big shout out to Christoph Zotter, inus Maya and Theresa Vit from my own newsroom in Vienna at Depress. You can read more on this topic in our newsletter this Friday put together here in Vienna by Tina Stani. Thank you to her as well. If you liked what you heard, tell others about it. And if you are interested in our topics, don't forget to check the Lens EU channel regularly. Next week, episode 9 comes from our colleagues at Okress in Poland. The week after that, it's TVNet from

Latvia and then we'll take a short summer break. before bringing you new episodes and newsletters again starting in September. My name is Anna Wina. I'm glad to have guided you through this episode. You'll find more press podcasts in our player in our app. Thanks for listening and see you next episode.

SOURCES

Sources, Episode 8: "Die Presse" article: Fake texts, shock calls and manipulated AI videos: scammers' tactics are getting more sophisticated. How criminals deliberately exploit fear, stress and trust: https://www.diepresse.com/36380272/ich-dachte-das-passiert-mir-nicht-wie-scam-opf er-manipuliert-werden The man hunting Europe's million-euro fraudsters: https://www.diepresse.com/36380534/der-mann-der-europas-millionenbetrueger-jagt The EU should do more to protect us from "scam states": https://www.diepresse.com/36433766/die-eu-sollte-uns-besser-vor-scam-staaten-sch uetzen https://fra.europa.eu/en/news/2026/1-4-europeans-are-victims-online-fraud Link to our scam simulator at DiePresse.com: https://www.diepresse.com/36480851/versuchen-sie-sich-als-online-betrueger-hallo mama-neue-nummer On the CORRECTIV.Europe segment: Investigation in English: https://correctiv.org/en/europe/2026/05/05/they-protect-the-law-while-breaking-it-insid e-europols-shadow-it-system/