HOW CRIME IS NURTURED ONLINE – EPISODE 03

SEASON 3

INTRODUCTION

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

We see that online fraud is reaching epidemic levels.

Tamara Schotte, Head of Analysis & Strategic Coordination Unit at Europol

Almost everyone knows someone who has been a victim of online fraud.

Sebastian Bley, Head of the Serious Fraud team at Europol

With more and more AI tools like voice cloning technology, deepfakes, LLM-generated scripts, AI-driven translations, we will see a lot more of frauds happening, especially romance frauds, investment frauds targeting millions of people because the technology doesn't need to sleep.

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

In Operation Raptor, 270 people around the world got arrested.

Narrator Europol

Data is the new currency of power; it's stolen, traded and exploited by criminal actors and we are currently living through a fraud epidemic. Fraud is increasing in scale, diversity and sophistication, at a pace we have never seen before.

Online fraud can have an absolutely devastating impact on victims – both financially and psychologically – with many people being targeted by criminal networks multiple times.

These fraud schemes are leveraging new technologies to become even more convincing. And once they've completed their scams, these fraudsters have to launder this money. For this, cryptocurrency is key. It's becoming the financial backbone of the digital criminal underworld.

Cyber-attacks play an important role, too. These criminals frequently target not only individuals, but critical infrastructure, governments, and businesses.

There are platforms and online forums, dark markets, and other places online for criminals to help other criminals. There are guidebooks on how to carry out crime. The online sphere is now the world's largest criminal theatre.

Welcome to The Europol Podcast, the official podcast of the EU's agency for law enforcement cooperation.

Today's episode: how crime is nurtured online.

OVERVIEW OF FRAUD SCHEMES

Narrator Europol

It's Olivia here and I am meeting Burkhard Mühl, the Head of the European Financial and Economic Crime Centre. What does the centre actually do?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

The European Financial and Economic Crime Centre was established with the main goal to follow the money, to actually identify, trace, freeze and seize the profits from criminal activity. All serious and organised crime is profit driven. And it gives us an important angle of attacking serious and organised crime.

And we see this on a daily basis that, due to the rapid technical developments, introducing, artificial intelligence or cryptocurrencies, there is a shift now in organised crime using these methodologies and providing money laundering as a service by specialists in those in the use of those digital tools to criminal organisations. So, this is going to be more and more outsourced to professional service providers.

Narrator Europol

Right, and just how widespread is fraud, and what kind of share does this criminal money have in our economy?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

We see that wide parts of our society are affected by this type of crime. If you think about your family or, people you know, you certainly know somebody who has fallen victim to a fraudster. And this has an impact, not only financially on the victims, but also psychological. We even are aware of cases where people lost their entire life savings and as a result of that committed suicide.

The overall criminal revenues from the nine most important criminal markets is about €139 billion. And we see that is a little bit below the EU budget. The EU budget in 2024 was €189 billion. So, in a theoretical situation where we could prevent those criminals taking profit from crime and defrauding or victimising EU citizens, actually, we almost could double the EU budget - to give you a perspective of the amount of criminal money that is floating around.

Narrator Europol

That's quite astonishing. So, is fraud actually bigger than the drug trade, for example?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

I can give you some figures here. Actually, MTIC fraud, which stands for Missing Trader Intra-Community fraud. This is, in essence, VAT fraud and customs fraud. And the estimations, it amounts up to about €50 billion annually. And if we take the example of drug trafficking, the estimations amount up to €30 billion. So, VAT fraud and customs fraud is larger than the drug trafficking market. This does not yet include the online fraud.

Narrator Europol

So, it's already highly lucrative but there is more money to be made through automisation. how are fraud schemes changing to keep up with trends and technology?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

Today, the methods are very sophisticated, language barriers no longer exist because of the use of artificial intelligence. Now, the products, the websites are designed in a very professional manner. And for the customer, it is not that easy to detect.

We see that today, the call centers are using artificial intelligence, so it's much easier for the criminals. If I go back in time, about 30 years ago, we had those letters coming from Nigeria, offering you millions and millions from some prince who wanted to hide his money. So those days are gone.

Sebastian Bley, Head of the Serious Fraud team at Europol

And over the time we see in fraud that it's always following the new trends. So, fraud is always like picking up new trends in a very quick way.

Narrator Europol

That's Sebastian Bley, the head of the Serious Fraud team at Europol.

Sebastian Bley, Head of the Serious Fraud team at Europol

We've seen this when crypto came out. Yeah, people not understanding crypto but seeing, hey, the bitcoin is going up. So, people want to benefit from this as well. So, we see that people are being approached into crypto investments, not understanding the technology, not understanding how it works, so that is perfect for the perpetrators to convince someone, hey, I can help you to invest into crypto. You don't need to do something. I help you and I make you rich.

So, you can also be sure that perpetrators, fraudsters will already offer you something to invest into AI. But at the end it's just picking up the new trends, the latest investment opportunities. And you transfer the money. But it's never going into anything. It's going into their pockets.

SHOCK CALLS

Narrator Europol

Are we seeing more people becoming victims of online fraud because of AI?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

Definitely. We had a case last year where the law enforcement agency we cooperated with actually detected a server, and they had, on a daily basis, 20,000 phone calls, so-called shock calls that were routed via one server, attacking one big European country and its population. So, it's just one server,

20,000 calls, on a daily basis. So, this gives an indication of the magnitude. And that was just one organisation. And there are hundreds out there trying to defraud people.

Sebastian Bley, Head of the Serious Fraud team at Europol

Operation Pandora is a German-led investigation into shock call fraud. Fake police officers, for example. And those - the perpetrators made thousands of calls per day.

Narrator Europol

What's the modus operandi here, where were these call centres based?

Sebastian Bley, Head of the Serious Fraud team at Europol

In many cases, we see that there's a call centre located in the country, and there's no victims in the same country. Also, they make this so that the law enforcement of that country is not targeting the call centre directly. We see also that the call centre, they're usually located in countries where the salaries are comparably low.

Narrator Europol

How much money were people losing via these shock calls?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

Usually, the individual losses ranging a couple of thousand euros. So, for the individual, this is still big money. But if we count the entire damage it is huge because there are thousands and thousands of victims.

Narrator Europol

There are thousands of victims, but how do these criminals find their targets?

Sebastian Bley, Head of the Serious Fraud team at Europol

They find information about the family structure. Oftentimes they simply use the telephone book to look for old names, and they call the people, crying basically and saying, hey, mom, dad, I'm really in trouble. And they just take the chance.

From the cases that we have supported so far, usually, they traditionally make the phone call from a mobile phone from call centres. They sit there, they make those calls. They make calls to vulnerable people, often the elderly, and persuade them to believe that a close family member of them has a problem. Having caused an accident, for example, or being in a very bad situation and that it's necessary to make a payment to get that person out of jail, and out of trouble. So those people, they really want to help out, oftentimes they have money at home, or they would go to a bank and they provide thousands of euros to the perpetrators.

And this is very much exploiting, of course, families. We have seen, for example, that perpetrators also exploit. They see, for example, in the newspaper, someone has died. So, from that information they can see the family structure more or less. There's like children, there's uncles, there's grandchildren. And with that information about the family, they could target someone, make a call and say, for example, I already tried to reach Uncle Michael.

But we are also convinced that in the future, people will use language models to do these calls like you have for companies. We can also speak to an operator, for example. Those tools are getting better and better, and we are convinced that in the future they will use this technology as well to make shock calls.

Narrator Europol

In Operation Pandora, 12 phone call fraud centres were shut down and 39 suspects were identified. To find out more about how Europol is targeting scam call centres. Check out season 1 of the Europol podcast, episode 7.

ROMANCE FRAUD

Narrator Europol

These call centres operate online. These types of centres often carry out other types of fraud too, like persuasive investment fraud or even romance scams. It's all about relationship building and earning trust.

Sebastian Bley, Head of the Serious Fraud team at Europol

I think that romance scam is the fraud that benefits or benefited the most from technology. In the past, if someone was approaching a person, like a wedding fraudster, for example, the person had to be close to the person, build up a relationship with the person, make calls, meet the person. Yeah, it's a lot of investment by the perpetrator.

Nowadays, with communication, with technology, the perpetrator can target someone at the other end of the world without having costs. If you made a call 20 years ago from here to Asia, for example. Yeah, it was a lot of money that you had to pay. Nowadays, using internet phone calls, you don't have these costs anymore.

You can do like so many scams on a day, in parallel. Yeah, because if you have an AI tool, that person can have like various conversations at the same time. That is a great crime enabler.

In the future, I think with more and more AI tools like voice cloning technology, deepfakes, LLM-generated scripts, AI driven translations, we will see a lot more frauds happening, especially romance frauds, investment frauds, targeting millions of people because the technology doesn't need to sleep. The technology can do this all day, seven days a week. Yeah, in parallel with various conversations.

Narrator Europol

Do these scammers often have people on the hook for years?

Sebastian Bley, Head of the Serious Fraud team at Europol

Definitely. Yeah. So, building this relationship is the essence, I think, of the fraud. That the perpetrator gains the confidence of the victim and persuades the victim to take an action, that is to his or her own disadvantage, paying money to the perpetrator. And we see this in investment fraud, where the person is contacted by the broker, has the trust, makes the payment. But when we look at romance

fraud, which is closely linked to investment fraud, this is even more extreme, because then we have the component of believing there is a personal relationship. There might even be love involved. And so, the person is in a fictitious online relationship with someone.

INVESTMENT FRAUD

Narrator Europol

Could you give a real-life example of what investment fraud could look like?

Sebastian Bley, Head of the Serious Fraud team at Europol

Think about investment fraud. If you think about the movie The Wolf of Wall Street, I think that's a very good example of how investment fraud works in practice, how this is also linked to legal business structures.

Because in that movie, it shows that he's there. He starts from a legal side, and then he goes more and more into that grey zone. He thinks hey, I'm going to sell that stock of that company that is not that good or just overpromise a little bit, but at one point, this goes to an extent that there's no chance for the investor to make any profit at the end. Because if we speak about investments, there's always a risk associated with it. So, people invest into something, there's a risk. But the fraud begins, of course, where there's no chance for the victim to ever make a profit because there's nothing behind it.

Narrator Europol

Let’s go back to Burkhard to hear more about how Europol is combatting investment fraud.

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

Well, I could mention here the operation called Juicy Fields. Honestly, I like the name. It's quite a good indication of what is going to happen here. It's a large-scale Ponzi scheme. Ponzi scheme is a famous fraud scheme where you actually attract investors and, if they want to receive the investment, you know, they get the investment paid in by new investors. So, it's a scheme that is luring people into investment. At a certain point in time, of course, there's not enough money in the scheme to pay out new investors, and it will collapse in the end. But in the beginning, those investment schemes are highly successful and profitable.

And in this case, the suspects lured victims into fraudulent crowdsourcing investment in the cultivation and disruption of cannabis for medical purposes. It was quite interesting. You could online see a cannabis plant. You literally could watch them grow so the investors believed actually that the investment is paying off because they saw the plantations. And upon the purchase of a cannabis plant with a minimum investment of €50.

The platform was not the only present in the digital world but upheld the image of a trustworthy legal business structure with physical offices, staff, and representation at cannabis events. Initially, the 500,000 e-growers, as they were called, all digital growers, were receiving their investment returns. So, this Ponzi scheme, they got the money back in the beginning. And in July 22 the criminals behind

the scheme abruptly removed the company profile from social media and stopped users from logging into their accounts and freezing the cash withdrawals.

Narrator Europol

What was the total reported damage in this case?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

The scheme actually impacted a very high number of victims throughout the European Union, and the damage is really staggering. Estimated to be around €645 million. So, enormous damages. They even could be higher, according to our intelligence.

And the criminal network has a very strong cross-border dimension, being led by Russian masterminds, with strawmen in Germany and money laundering activities in Cyprus. We even supported an action day in the Dominican Republic. There, one of the main suspects was arrested, and we deployed the case officer to provide the support there.

Narrator Europol

And what was the idea then – that you would invest €50 and then what happens?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

People were made to believe that the €50 investment will multiply, because when the cannabis plants are being sold, the profit margin will be very high. And, they believe they could double or triple the investment. And in the beginning, you know, they got the money back. And so, they were starting to trust the business. And it was very professionally run, in big marketing events. And also, an indication of the fraud is when the organisers of those kinds of events, you know, they show up in expensive sports cars, they flex expensive Rolex watches, for example, which happens actually quite often. And so, they demonstrate wealth and giving the indication that, by investing there, you can get rich in no time. So that is also an indication where people should be very concerned and cautious.

Sebastian Bley, Head of the Serious Fraud team at Europol

And that's, I think, also why it's important to target these types of frauds, because that's about the economy and that's about what we all depend on. We all depend on a working and functioning economy with a fair competition and with business that works.

And there's trust. That's the most important thing. Because if there's no trust in the economy, there's no trust into investment, then people would not invest. And without investment, Europe could not be as wealthy.

Narrator Europol

Let’s turn our attention to some of the ways cybercriminals open the doors to carry out these fraudulent activities. We’ll look at cyber-attacks, cryptocurrency and money laundering. Let’s talk to Marijn Schuurbiers, Head of Operations at the European Cybercrime Centre at Europol.

PHISHING AND CRIME-AS-A-SERVICE

Narrator Europol

So, the criminal world has become about crime-as-a-service, criminals offering each other help online. Is that right?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

You have to imagine that there are basically specialties in every area. So, anyone that wants to perform cybercrime, you don't have to be a top expert anymore over the whole broad landscape. So, because you have experts in sub-areas. So, you can imagine that if you, for instance, a ransomware attack typically happens in different stages.

So, first you need initial access to a company via, for instance, a phishing email. How to do a phishing email or how to fish for credentials? Well, there's basically phishing services out there that provide complete toolboxes, which help you how to build a nice, reliable or a credible, phishing page of a company. And that maybe even targets two-factor authentication, all kinds like that.

So, for that initial access, you already have specific service providers. Then, there are anonymous anonymity providers that provide secure communications - VPNs, for instance.

Narrator Europol

We know these criminals gather in dark web platforms. What's Europol doing about it?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

So, in Operation Raptor, there were various of these dark markets, they were targeted. So, like, the door-to-door market was a big one. Bohemia Market, Kingdom Markets and Nemesis. All of these four were these typical dark markets that were somewhere on the TOR network. In different locations with law enforcement agencies, these were in the end tracked down and taken down from the internet.

So, located, then the administrators behind the websites, they were arrested, and then these services were taken down. That's already effective because you take down this major market. So, this market cannot be used anymore for, in this case, illicit drug trafficking. But again, because then we have this dataset and then we can see all the people that the sellers, so the drug dealers that sold their drugs on that market, and also the people that bought the drugs on the internet. And they, you can see are mostly the transactions, probably logins and username, passwords and all of these types of things. And based on that data, so in the second phase in this investigation, we started to analyse, see, okay, who are the biggest sellers on these markets? Who are the biggest buyers on these markets, which can often be then local drug dealers, then again resell it in whatever neighbourhood they live.

And then with a follow-up in the Member States, they can identify them definitely. In Operation Raptor, 270 people around the world got arrested.

Narrator Europol

DDoS stands for distributed denial of service. It's a cyber attack where multiple sources flood a network or website with traffic to make it unavailable to users. Are DDoS attacks one of the ways criminals can get initial access?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

Yeah. So, a DDoS attack is basically overloading a service on the internet with data and then causing it to go out of function. That could be a website. That's the most common thing that you would think of. There are also a lot of digital services connected to the internet, not the website, but just a functionality that can be banking, traffic, or there can be logistical, communication streams or whatever.

Money is not made via DDoS attacks. So, the vast majority of money that is currently being made is either through ransomware attacks. So, you would steal the company's data, and maybe in addition, you encrypt their data and then you ask money for, in return to unlock it or to not to publish that data. And then there's also a method called business email compromise, where you basically get into the systems of a company and then try to trick the company into making large payments on behalf of the CEO, which the CEO did not even order, but because they're so deep in the systems that makes you really credible. These are the vast majority of criminal money that is being made.

Sebastian Bley, Head of the Serious Fraud team at Europol

And the big challenge, of course, is also for the perpetrator that once he has the money in his pocket, he wants to keep the money.

Yeah, so of course, we also see fraud very closely linked to money laundering. Many use money laundering services, for example, once they have the money in their account to wash it then, so that the police or the law enforcement cannot get the money back. And to hide the traces. So, money laundering is very closely linked to fraud schemes.

Narrator Europol

So, then criminals have got your money via a fraud scheme or cyber-attack, but they need to clean the money before they can use it. When it comes to criminal profits, cryptocurrencies can operate as a main monetary vehicle. Burkhard, what is the role of cryptocurrency in nurturing fraud online?

Burkhard Mühl, Head of the European Financial and Economic Crime Centre (EFECC) at Europol

We see that the use of virtual currencies in our investigations is now reaching a level that we no longer talk about single, locations or random use of virtual currencies. On the contrary, today we see that in almost all the criminal investigations, at a certain point, we see virtual assets, virtual currencies being used.

It is a tool that is being used by criminals, for laundering their money, basically. And we have to invest in training investigators, in tracing virtual currencies. Also, together with the private sector. One good thing about virtual currencies is that nothing gets lost in the blockchain, so the criminals shouldn't assume they are safe and they use virtual currencies. We will get them. We have top experts, and we will go after them. And we have quite some significant seizures. So, we invest, this is a priority. And also the Member States are now, very, very, committed to investing in following virtual currencies.

CRYPTOCURRENCY AS A MONEY LAUNDERING TOOL

Narrator Europol

How has money laundering changed since the advent of cryptocurrency?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

So what we saw in the past when some type of crime was committed and money was collected with it, you need to somehow get your hands on that money. What happened back then? A lot that there was a use of so-called money mules. Because you had the banking system and somehow use the banking systems to get money overseas or to receive it from overseas, and then maybe to cash it out. Then, money mules were recruited, so often young people or poor people that that would be tricked into offering their bank account, receive some money and then withdraw that from an ATM, and then it's cash.

And when it's cash, you can easily, you know, make it more anonymous because then the trail ends. This was basically sort of a weak point for the criminals because, of course, the banks could monitor. They could they could spot it. They could often maybe even stop it when it was reported early enough.

They could maybe call the other bank where it's been transferred to. So, you had, banks that had some a certain amount of control, on that money stream. With cryptocurrencies, there is no central entity anymore that can stop one transaction from going through. There's nobody to go to because it's a decentralised system. That's the whole architecture of it. And this architecture is also, it has many benefits, but it's also, very beneficial for criminals because there is no bank or authority anymore that can freeze an asset. So this is what makes it a very, well, basically the vehicle currently for when you have ransomware criminals. The fastest things they will do is somehow to transfer it or to convert it into cryptocurrencies.

Or basically when it comes to ransomware, to demand in cryptocurrency in the first place. So, then it's immediately on that blockchain that is nobody can control, and they can move the money around the world from one continent to the other, from one jurisdiction to the other, without anybody able to stop them. The blockchain does have an advantage because when you compare it to the classic monetary system, that is not open by default.

Narrator Europol

So, there are no disadvantages for criminals when using cryptocurrencies?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

If the law enforcement wants to get an insight in payments, we would have to send court orders to banks in order to figure out where this money went. In the blockchain, this is not necessary because the blockchain is public information. So, basically if you have the right tools, and of course at Europol we have them, you can track the cryptocurrencies from one wallet to the other, from one crypto address to the other. So that becomes relatively transparent. So that is the advantage.

But, of course, the criminals also realise that and well, then they need a way to launder that money or to obfuscate the money trail. Well, what happened there is that specific crypto laundromats started appearing like chip mixer, for example, which was a very large cryptocurrency mixing service. And you have to imagine that basically it's a service. You send cryptocurrency in there, then it goes into a black box, which is not a public thing you can follow up upon. And then basically it spits out the money, it drops out each of the cryptocurrency basically in smaller amounts and, and then chops and then spits it out to other addresses.

And because they do this en masse, they have multiple, you know, hundreds or thousands of transactions per day going in and hundreds and thousands going out, then it is for law enforcement not clear anymore what went in and what went out and how to connect to each other. And then basically the criminals have, with that service, anonymised their money. And then from that point on, they can try to cash it out somehow.

THE CHIPMIXER LAUNDROMAT CASE

Narrator Europol

Is there a specific case regarding a chipmixer laundromat that Europol was involved in?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

Well, in the example of the chipmixer case, the amount of money that flows through it, they were staggering.

Narrator Europol

How much was going through that crypto mixer?

Marijn Schuurbiers, Head of Operations in the European Cybercrime Centre at Europol

So, through this crypto mixer in a period of not even six years, almost €3 billion worth of crypto was laundered through the service. So, if you would divide it into the years of existence, it would be about €500 million each year.

Narrator Europol

The investigation into the criminal service suggests that the platform may have facilitated the laundered of 152 000 bitcoins. A large share of this is connected to dark web markets, ransomware groups, illiict goods trafficking, the procurement of child sexual exploitation material and stolen crypto assets.

So, from the initial attack to get your data and money – whether a DDOS attack, another cyber-attack, or online fraud, to the laundering of criminal money via cryptomixers, the entire life cycle of crime is now online. But how does this all come together?

Here’s Tamara Schotte, Head of Strategic Analysis at Europol on how crime is nurtured online.

Tamara Schotte, Head of Analysis & Strategic Coordination Unit at Europol

So indeed crime, organised crime is increasingly nurtured online. Is this new? No. We are seeing since 15 years that serious and organised crime is enabled by the internet, is facilitated by the internet. But what is the big difference? In the past years, the online environment has become the main stage of serious and organised crime activities of criminal networks.

Almost every criminal network, criminal activities has an online component today. You see dedicated online apps, platforms that are created for criminal communications to hide, in fact, detection from law enforcement.

So, you see that the online environment is not only to hide communication, is not only there to facilitate crime, to speed up crime, but it's increasingly the platform where, in fact, all the stages of the criminal activities are taking place, from the recruitment of a criminal to the execution of the criminal activities, to the laundering of the money even, it's happening online.

Narrator Europol

So, we are seeing more and more victims due to the tools available now?

Tamara Schotte, Head of Analysis & Strategic Coordination Unit at Europol

So, the tools that they are using today make sure that they can speed up the crime and that they can make more victims. More victims means more profits.

Today in 2025, we are sure online frauds - because of the acceleration of technology and the exploit and the use of AI - will certainly become one of the biggest threats that we are facing in the EU. And it has a massive impact because I think almost everyone knows someone who has been a victim of online fraud.

Narrator Europol

So, what would you tell our listeners about how they could avoid getting scammed?

Sebastian Bley, Head of the Serious Fraud team at Europol

The most important thing is to know these people who call you, they don't care about you. That will promise you anything. They will tell you the best story. And I think the most important thing is to not be rushed, to really take a moment to think about if you're being approached by phone, for example, why is that person calling me?

Narrator Europol

And if someone has been scammed, what should they do?

Sebastian Bley, Head of the Serious Fraud team at Europol

If you have been scammed by someone, you can be sure that you're not the only victim.

You are one of many. And with this, it's very important to inform the police, because if they investigate the people, it also increases the penalty. It also increases the chances that you may get back some of the money if the police is able to do its recovery measures.

I'm also convinced that the role of Europol contributes to fighting these types of crimes, because our role is to enable international police cooperation. And I think that this international police cooperation is the key to target the fraudsters. They act from one country into another, and that requires cooperation among the law enforcement.

WRAP-UP

Narrator Europol

You've heard all about how crime is nurtured online – from fraud to cyber-attacks. Stay tuned for our next episode, where we will dive into how criminal networks are accelerating their nefarious schemes and how their activities are being turbocharged by AI. We will go find out about large-scale cyber-attacks, and crime-as-a-service, and will look at the exploitation of children online.

Thank you for listening to this episode of The Europol Podcast. Please subscribe and give us a rating on whatever platform you're using to listen, and if you enjoyed the show maybe consider sharing the podcast on your social media.

If you want to hear more about our work Making Europe Safer, you can always check out our website – that's europol.europa.eu.

Thank you very much for listening. We'll see you soon.