The Neighbourhood Watch Podcast Episode 4 with Kaf Okpattah

Hello and a warm welcome to the Neighbourhood Watch podcast. I'm Alfie Moore, stand-up comedian, former police officer, host of the long-running Radio 4 series It's a Fair Cop and now host of this podcast. This series is all about the Neighbourhood Watch's ongoing mission to support and enable people and communities to be connected, active and safe.

In each episode, I'm joined by a special guest to find out about their neighbourhood that they grew up in, and then our thoughts turn to crime, specifically in this episode, cybercrime and the new generation of online fraudsters. Investigative journalist Kath O'Patter is my guest today, and she'll be telling us about the extensive research that he's carried out for his book, Scam Nation. Kath went undercover into this shadow world to learn about how teenage fraudsters use tools like AI, encrypted messaging and social media platforms to extort people's money.

And he'll share what he's learned with us. Artificial intelligence and the rise in deepfake technology means not only can you clone numbers, so I could clone your number and pretend to be you, Alfie, but I could also, with enough information and patience, clone your voice. So not only call someone from your number, but also sound like you.

So if you're keen to protect yourself and your loved ones of all ages from online fraud, and you want to get to grips with these sophisticated methods used by scammers, keep listening. A little later, we'll be joined by Detective Sergeant Ben Hurley from the Dedicated Card and Payment Crime Unit. This is a specialist unit comprising of City of London Police, Metropolitan Police and UK Finance, which concentrates on new emerging threats in the cyber-enabled fraud landscape.

And speaking of those threats, here's a quick question. By 2023, how much online fraud, including online scams and fake adverts, has been spawned on social media? Is it 60%, 70% or 80%? I'll reveal the answer before the end of this episode, but for now, let's welcome Kath O'Patter. Kath, you grew up in Ghana before moving to London as a teen.

What were your fondest memories of the neighbourhood you lived in over there? Fondest memories would be, so I grew up there, I moved to the UK when I was 12, and I think it would be pushing my brother on his tricycle up and down the road we lived in, mainly because I pushed him very, very fast and he was screaming, stop, stop, and me being the older brother that I am, decided not to stop. It was like our after-school ritual, and I still remember it to this day, he less so, thankfully. Brotherly love, brotherly love.

And how did your neighbourhood in Ghana compare to where you moved to, which I understand is Ferry Lane Estate in Tottenham. I'm assuming that Ghana had a better local football team. Yes, of which I was the star striker.

No, it was, I mean hindsight is a beautiful thing, but I absolutely loved growing up there. It was safe, which I've only realised since becoming an adult. It was sunny, there was a community, people would often drop by unannounced, neighbours would drop by unannounced, and we'd all have dinner together, we all knew each other, we would often pivvy back.

Is this Ghana we're talking about now? No, this is Ghana, yeah. And well, Ferry Lane Estate, it was also nice, but... Not quite as sunny. Not quite as sunny, and not quite as safe, I saw a lot of knife attacks, a lot of gang behaviour, drug dealing, antisocial behaviour.

I also witnessed on that estate the shooting of Mark Duggan. Wow. So how old are you now, Kaf, when this was happening? Mark Duggan was shot 2012, I believe, or 2011.

2011, yeah. So I was 10, because I'm an August-born, he was shot that summer, but I'm a late August-born, so I was 10. And of course, that led to, well, national public unrest and rioting, really.

So was that something that happened where you were? Yeah, big time. And in fact, a lot of the people, there was one moment where we were watching the News at Six, BBC News at Six, and I actually spotted someone who lived in the same estate as me, filmed, rioting, walking around during that time, during the time of unrest, any loud bang, and my dad or mum would just pull me a bit closer, thinking that either it was a gunshot or something else. Yeah, scary, scary times.

And you're now in North, Crouch End now, North London? Crouch End, yes, we like to call it. That's nice. That sounds nice, is that alright? It's quite nice.

It's a lot similar to Ghana, in the sense that everyone knows each other. No one drops violent nouns, that's not very British, but it's a proper community. And has the area, has it been consistent, the area? Has it changed since you went through your teens? It's more or less stayed the same.

The waitress there has had a bit of a refurb, so we were without a waitress for three months. Well, that is a challenge, I should think. Crouch was empty, poor man, are you OK? It's fine, I'm an Aldi shopper anyway, down in Greenlace.

But yeah, it's pretty much stayed the same, because the secondary school I went to was in Highgate, not too far away from Crouch End. So I'd always travel from Tottenham through to Crouch End, over to Highgate, and think, I'd quite like to live here one day. The houses are the same.

Some of the people I saw whilst I was going to school are still there. The big issue lady is still the same one I saw whilst I was in secondary school. Crouch End hasn't changed much, but in our new, fancy new waitress.

You're listening to the Neighbourhood Watch podcast with me, Alfie Moore. In this episode, we're looking at the new generation of cyber criminals. Detective Sergeant Ben Hurley from the Dedicated Card and Payment Crime Unit will join us shortly to tell us about his work.

But first, Caf, let's talk about Scam Nation. How did your book come about? So, I'm an investigative journalist, and one of the... Actually, my first ever investigation for the BBC was about fraud. But it was different to what I was seeing on the news and what most people might be privy to.

Whilst most stories look at the victims, rightly so, and we should never forget the victims, because what they go through is absolutely horrible. I looked at it from a different angle. The perpetrators, the scammers themselves, and the reason I did so was because these scammers were my friends, my classmates, and regrettably, I nearly became one myself.

Right. So, are these the college years we're talking about? Secondary school. So, as early as 12 through to Sith form, up until 18.

My earliest memory of seeing fraud up close was when I was in Year 9. I was 13, and this guy who I'll call Cranks Corleone was just brandishing a large number of bank cards. I mean, even at 13, I thought, why the hell do you have five bank cards, none of which are in your name, but it turns out what he was doing with those bank cards were holding it for an older, older is a slang term for someone higher up in the criminal organisation, often older than you, holding those cards for this senior member to put money in from other people in our class and then cash that money out. Obviously, I didn't know this at the time, but what he was doing was basically money laundering.

And was that a one-off or was that... Oh, no, no, no, no. It was quite common. In fact, that was only one example of one of the types of things people got up to in secondary school.

Another common one was deetsing, which is when you go on the dark web, well, now sometimes on the open web, and find people's full financial information, their card number, account number, sort code, CVC code, and use those details to go on an online shopping spree. And some people can scrape that from open source. Yeah, well, back in my day, not that old, it was the dark web.

Now you can scrape it very much on the open web, even on social media. Wow, yeah. And yet we think we're... Well, we'll talk about some of the security measures.

And you mentioned some of the terminology. I mean, it's good for the listeners to know, I guess, because a lot of people listening to this will have young people at school, at college, maybe even at uni. So have you got any more terms we can throw out that I've never heard of that might be red flags? Yeah, so obviously deetsing is one of them to commit fraud.

Falls, full financial information. Squares is one which comes up a lot. Squares is basically slang for your bank card.

All right. So if someone says, swing me those squares, they're saying, give me those bank cards. And if you see in your child or the person you're caring for their search history on social media, squares, they're not looking for geometric shapes.

They're probably looking for falls and people who can swing them squares. Okay. So to write the book, and I don't know what stage you decided whether you were having a sort of getting involved with the scammers to write a book from the get-go.

Did it happen like that? Or are we just curious and then the book idea came along? I was tricked into writing a book off the back of one investigation where I hunted down a prolific social media fraudster. And the suggestion from both my agents, Toby, and other people I knew was this should be a book a lot of people don't know about this world. A lot of people don't know that it's teenagers who are committing cyber-enabled fraud.

Obviously for me, it was part and parcel of my life. It was something that I knew quite well. It wasn't something that I was so shocked by.

So you're automatically accepted into that world, presumably. Yeah. Yeah.

I still try to not feign shock, but more empathise and sympathise a bit more when people are shocked by some of the things I've seen and some of the people I've seen doing these things because it's embedded so deeply into youth culture. And that's why I realised maybe I should write about this to not just inform parents about the potential criminality that your children might be getting involved in, but also inform young people about the risks and dangers of getting into what seems like a victimless crime, a risk-free crime, because the sentences are quite huge for this kind of stuff. And presumably risk-free, the mentality, the thinking being that the banks tend to foot the bill for the victim of fraud? That's one aspect.

Often what I've seen in these fraud group chats on social media is, oh, it's fine, the holder, holder being the bank card holder, will get their money back. The banks will refund them. But also in the sense that cyber-enabled fraud, especially, isn't a physical crime.

You're not seeing your victim up close. You're not actually interacting with them. It's not like stabbing someone.

A lot of these kids start off in game modding, game modification, hacking games, and then they progress into cyber-enabled fraud. It's like a game for them, pushing numbers on the screen and cashing out. And you mentioned empathy.

I understand from some excerpts from your book, you have empathy for some of the younger people involved in this. Yes. Yeah.

And I want to clarify that my book and I are not apologists for scammers. Right. However, like I said, some of these people were slash are my friends.

And even though I grew up, I went to school in a very affluent, posh part of London. The people who attended that school were a lot like me. They weren't posh.

They weren't from the surrounding area. They were from council estates. They were sharing bedrooms with their siblings.

And these are very, very clever people. Fraud is becoming easier to commit. But back then, you needed a bit of technical know-how.

And the teenagers doing this are clever people. They've just been dealt a bad hand in life. And so they're using their skills for nefarious means.

Well, I'd like to talk about what we can do about intervention later. But I think this would be a good time to bring in Detective Sergeant Ben Hurley from the Dedicated Card and Payment Crime Unit. Welcome, Ben.

Tell us about the role of your unit. So I work for a unit called DCPCU, the Dedicated Card and Payment Crime Unit. We essentially deal with online payments and banking fraud.

We get our work direct from the banks. Right. So when they identify a particular person of interest who may be committing fraud against them or their customers, then that's when it comes to us.

And we pick it up from there. So it's a proactive element by the sounds of it. Yeah, exactly.

We have two strands, really. We have the more reactive side, which are referrals from the banks and financial institutions. But yeah, we do have proactive elements and capabilities as well.

So we try and take the fight to the fraudsters where we can. Right. Okay.

So we hear a lot about, well, was action fraud, now report fraud. But you're a completely independent unit, are you? So we are a unit made up of officers from the City of London Police, the Metropolitan Police, and we also have UK Finance staff as well. So we are a collaborative unit with all those three organisations.

So some people get a little bit confused, I think. So the Metropolitan Police, that's the London surrounding areas, and the City of London Police, the financial mile, the square mile in the middle? So yeah, the City of London Police is the police force for the square mile. However, it does also have national functions.

So it is the national, it's the lead for fraud nationally. So it has a large responsibility in tackling fraud nationally. And my unit is part of that strategy.

And we've heard Caf explain how easy it is for young people to fall into committing fraud. I'm hoping you're going to tell us how easy it is to stop them. Yeah, fraud is obviously, as Caf said, it's becoming easier.

And one of the biggest challenges is the volume of fraud that's happening. I mean, at the moment, numbers and figures do vary slightly, but you're looking upwards of 40% of all crime is fraud. Massive.

Yeah, and at the moment, the resources allocated to tackling fraud are comparatively small compared to a lot of more the violent or traditional crimes, we'll call them, that the police deal with. So that is one of the biggest challenges, the pure volume. Yeah, and if you're running a business, forget it's called the police, but if you're in a business and 40% of your work is one area, you know, the staffing in that should reflect in an ideal world, shouldn't it? If you want to be a successful, effective business.

Yeah, absolutely. Of course, there are competing priorities within law enforcement. And fraud, while it is a huge issue, and more is being done to tackle it, however, it's not the only problem.

And we recognise that, you know, that there are other challenges out there, whether it's violent crime, acquisitive crime, that also need dealing with. So it is a challenge having the resources to be able to deal with all of that well enough. But fraud is one of the ones that in recent years, as I'm sure Kaf will attest to as well, it's becoming far more, people are realising that just the damage and how much of an issue it is, more than they have done previously.

And the resources allocated are a reflection of that understanding. So just to clarify a few, some terminology, I might be wrong. My understanding is cybercrime, that's all digital technology-enforced crime.

And then the fraud aspect of it is part of that. But I should imagine it's 90% of all cybercrime, isn't it, fraud? There's certainly a very large overlap. It'd be wrong to say, well, fraud is cybercrime.

And in the same way, it'd be wrong to say, well, cybercrime is fraud. But there is a massive overlap. A large proportion of fraud is these days cyber-enabled.

With the, you know, the increase in technology, it's easier. And what common forms do they take? What's your most common types of fraud that you get involved in? The most common types that we deal with will be what we call social engineering type frauds, which is a very broad term. But specifically, we will deal with more of the phishing type fraud.

So for instance, if you receive a text message from someone saying that they're trying to deliver a parcel, click this link to get it redelivered at a different date. But actually, you click the link and you go to a malicious website. So that's what we call phishing or smishing, if it's a text.

And what's a malicious website after from you? It can be a number of things. It depends on the aims of the fraudster behind it. But often, it will be to harvest your details.

So it'll be personal details, security details, banking details, that in itself, not necessarily you won't realise anything's happened, perhaps. But those details will then be used at a later date, or possibly sold on to someone else to use, to then essentially do the fraud. And that phishing is mainly email and messaging texts? Phishing is, traditionally, we would associate phishing with email, but that was because that was really the, or exploded.

But obviously, with the advent of text messaging, direct messaging, social media, and all the rest of it, that spread. So phishing is more of a general term when we talk about text message, sort of suspicious text message. We refer to those as smishing, so SMS phishing, essentially.

And just to bring Kaff in, is that your experience? Has that evolved since you've been involved, Kaff? Or was this a sort of setup when you were looking at it? Yes. And what was interesting was, I mentioned how technically able these young kids are. They were actually building their own malicious websites to harvest data from people.

They were sending out the smishing text through burner phones, connected to these malicious websites. What's changed is a lot of it is now automated for starters. So you can have websites which will blast out a lot of these smishing and phishing messaging.

And you can also hire people who can build you these malicious websites. So you don't actually have to know how to do it. You just have someone doing it for them.

And of course, I guess the scary bit is the development of AI. Yeah. Artificial intelligence and the rise in deepfake technology means not only can you clone numbers.

So I could clone your number and pretend to be you, Alfie. But I could also, with enough information and patience, clone your voice. So not only call someone from your number, but also sound like you and say... This is why I talk funny, Kaaf, dear friend.

Give me half an hour. So to both of you, really, what information would you like to get out there about frauds and techniques that people might not know about that we need to know? I'd say be sceptical. And it's sad that we have to say this now, but trust no one.

Because as I mentioned, numbers can be cloned. Voices can be cloned. Faces can be cloned.

That person texting you, pretending to be your wife, may in fact be a fraudster. In fact, with my wife and I, we have a safe word where if she's saying something... And what's that, Kaaf, the safe word? Good try. But yeah, it's the equivalent of a security question.

You know, those things like mother's maiden name, your first pet. Yeah, nice. Obviously, something that's not obvious, something only you and that other person would know, but something the scammer wouldn't know, even if they are pretending and sounding like your partner or your relative.

Got you. And if I could ask Ben, a typical example, Ben, maybe a text message from somebody claiming to be from the HMRC and the recipient clicks a link before realising they've been duped or they shouldn't have clicked it. What should they do then, Ben? What would your advice be? The first thing to say is, if you click on a link in a text message, don't panic.

The fact that you've recognised that it's suspicious is the best first start you can have. It's important to know, if you just click on a link in a message as well, that in itself won't necessarily cause any problems. The purpose of the link is to take you to a malicious website to then harvest your details most of the time.

So just click on the link if you realise after you click on the link, but before you put any details in, then it's important to realise you're probably okay. Right. Report the matter to your bank.

If it's from HMRC, you can still report it to your bank. You can report it to your telecommunications network. But is that an easy process? It is, yeah.

If you get a forged in text message, one of the quickest and easiest ways you can report it is to forward that message to 7726, which is the number. Easy way to remember that is 7726 on an old sort of alphanumeric keypad. I remember back in the day when we all used to text, it used to take five minutes to type out three words.

7726 actually spells out spam. So if you forward that text message to 7726, it will get reported to the network and get flagged by them. So who's on the other end of that? Is that the police side or is it... So that is the mobile network operators.

They will have all that information. But that is information that they can then feed into the police or to a report forge to help build the picture. And identify those numbers that are sending out the forged messages.

And that's how they can get blocked. That's how investigations can start to target them and how forges can get caught. So the more it gets reported, the more information we have to be able to act on it.

So the system sort of joining up by the sounds of it, where you speak to each other, whether it be the police and the banks and the... Absolutely, yeah. And that is something I would say is absolutely key. Forward is unfortunately quite underreported, but it might not seem like much getting a text message, but it could just be that little piece that will add that to that intelligence and provide some vital information for, whether it's my team or someone else.

To help others, yeah. To help, exactly, yeah. It's worth mentioning as well, if you do click on a link and you do end up putting your details in, again, don't panic.

Report the message as you would. Report it to your bank. Cancel your card.

If you've given over any of your banking details, cancel your cards, report to your bank. And that's the best way to deal with that. Often these forces will be harvesting information to use at a later date.

So if you're quick, if you act on it quickly, there's nothing to say that you're going to actually fall victim to fraud, but it's about being decisive and it's about getting that report out and cancelling your details, changing your passwords, whatever you think might have been compromised, take action against it. Right. And Cath, you've already given us a great tip about a safe word for the scary AI developing world of deepfake and voice clone technology.

What else would you like readers to take from your scam nation book, Cath? Just that fraud has a financial and emotional effect on victims. And the emotional side is often less spoken about. A lot of victims I've spoken to have become, rightly so, very, very paranoid, afraid to pick up the phone, jumpy when they see a text from a number they don't recognise, or even one that they do recognise.

And I think it's important to know that you're not stupid. You shouldn't feel guilty. It happens to fallen victims of a scam.

You are a victim. It happens to the best of us. You've been tricked.

It's happened to me. And I'm probably the most paranoid person on Earth. Yeah, wow.

With your knowledge as well, I think that shows you how convincing these things are. What would your advice be to a young person approached or people attempting to lure them into this world? What would you say to that person? It ain't worth it. It's not worth it.

It might seem like quick, easy money. But firstly, imagine if someone did that to your parents. You wouldn't like that at all.

Secondly, you can go to prison for a very, very long time. And it has a disastrous effect on your financial autonomy. There are organisations which monitor bank accounts.

If you're using your bank card to claim money for a quick hit of £100, that can put a marker on your name. And that can affect you getting a loan in the future. It can affect you applying for bank cards or even getting a student loan.

Yeah. And I'm glad you mentioned the emotional damage as well, because it's easy to, I'd suggest, to convince themselves, as you said, about that the banks don't foot the bill. But the banks don't foot the emotional damage bill, do they? No.

And likewise, a similar question to parents and grandparents who think there might be something going on. How would you advise them? That's a good question. I'd say, and this is something I'm realising now that I'm a parent myself, don't go in guns blazing.

Firstly, understand why your child or grandchild is involved or thinking about or potentially being involved in this crying. And see it from their point of view. Ask them about it.

And I know some parents don't like to sneak on their kids. There's a time and place to do that. Yeah.

Yeah. Have access to your kids' social media accounts, because there are people out there who are trying to lure them into this world. And you want to be aware of that.

Right. An expression I found interesting that I'd never heard before from your book was mule herders. Could you just explain what that means? So we all know about drug mules, people who smuggle drugs into the country.

We have the same thing, money mules, people who clean money using their bank accounts. Mule herders are the people who are trawling the internet, glamorising this flashy lifestyle that fraud can fund. And basically trying to use that flashiness to recruit in money mules.

Right, got you. So on one hand, you have the money mules, and on the other hand, you have the mule herders. Got you.

Okay. So I've got a background in policing, and many of that was spent in neighbourhood intervention work and diversion work. When the young people are at that tipping point into criminality, my experience was that if you spend some money to engage with them then, it's a good business model because they're going to cost you a lot of money as an adult if they go into criminality.

So this is a question to both of you, because I understand that your department gets involved in preventers as well, Ben. How can we intervene? If you've got a pot of money, how would you spend it? You can't arrest the way I afford. So I think prevention and education is really key.

And we have very talented individuals who spend a lot of time educating at all sorts of levels, businesses, banks, but then also schools, colleges, and that sort of thing. And I think the really key thing is to, as Kaff's already really said, is to educate and make them realise that, yes, it might seem an attractive proposition, making a couple of hundred quid for something that seems like a victimless crime. No one's getting hurt.

But actually, the effects that that can have, not just the people who are going to be the victims of that, but for those individuals doing it as well, the knock-on effects. We see, sadly, a lot of university students succumbing to this sort of temptation. And actually, that can have a real knock-on effect for career prospects and lots of other things down the line.

And that's key, and that's what we try and do in the department, try and educate to divert.

This file is longer than 30 minutes.