EP 03: Digital Danger: The Rising Threat of Sextortion

Sue: Welcome back to Navigating the Digital Jungle with Sue Atkins and Friends, where we help families find their way in the ever-evolving landscape of technology. I'm Sue Atkins, your guide on this journey, author and broadcaster, and I'm here today with Angeline Corvaglia, creator of Data Girl and Friends, empowering young minds with online safety and AI literacy videos, games and educational materials.

We're here to guide you through the digital jungle. And this week we're going to be looking at something rather unpleasant called sextortion. In today's episode we're confronting one of the most pressing digital dangers facing young people and families, sextortion. So, this episode is a cautionary, deep dive into a critical online threat that can have lasting, harmful effects if not addressed openly.

And we'll explore what sextortion is, how it happens, and most importantly, what parents, teens and young adults need to know to protect themselves in an increasingly digital world. We'll be covering the regular segments that you love, including family change, listeners questions, weekly quick tips and script of the week.

And there's an extra mention of extra content that you can access after the episode.
So, sextortion is a form of blackmail, where someone threatens to reveal intimate images or information unless their demands are met, often for more explicit images, money or personal favours. It's a malicious form of exploitation that preys on vulnerability. And unfortunately, it's on the rise as more young people use social media and online communication.

Now, the challenge is that sextortion often occurs on platforms that feel private or anonymous because predators may initiate contact through social media, gaming apps, or private messages and they gain your trust before manipulating victims into sharing compromising images. And once they have something to hold over their target, well, that's when the cycle of threats and demands makes young people feel isolated, afraid, and unsure of where to turn and what to do.

Sue: So, today's episode is all about empowering families to recognize the warning signs, approach online relationships with caution, and understand the importance of open communication. Because by understanding the risks and knowing how to respond, families can work together to build safer, online habits. So, today we have a very special guest, Paul Raffile, an intelligence analyst focused on global cyber threats and transnational organized crime.

He has worked on government and private sector projects to detect and investigate terrorist networks, fraud, black markets, violent crime, and human exploitation. So, today we're going to be discussing sextortion. So, thank you for joining us very much, Paul.

Paul: Happy to be here.

Sue: So, Paul, could you briefly share your background and what led you to focus on global cyber threats and transnational organized crime?

Paul: Well, I've kind of always been interested in that topic. I went to school for national security studies, global studies. And, you know, a lot of folks in those programs going to like the CIA, the FBI, I decided to go into the private sector. First role was tracking terrorist activity across seven countries.

Then I moved more to the corporate side, have focused on cyber criminals, fraud actors, and I just find this area so fascinating.

Sue: Gosh, yes, absolutely fascinating. So, tell us in your own words, really, for those that don't know, I even said it to my daughter that was recording my podcast about sextortion.

She's 30 and she said, gosh, what's that? So, it's an increasingly concerning issue. Can you explain what it is and why it has become so prevalent?

Paul: Yeah, so sextortion is not exactly new. Sextortion is a crime that involves blackmailing someone using typically their explicit images or photos or videos in order to get them to do something or pay you.

But what we're seeing right now, why this has become such an urgent threat is there has been a massive explosion in a new form of sextortion called financial sextortion or financially noted sextortion where these criminals are blackmailing hundreds of thousands of people to get money from them.

Sue: Gosh, and how do cyber criminals then target children and young people and teens?

Paul: Well, oftentimes these criminals approach teens and young people on social media accounts where we are every day, places like Snapchat, Instagram, and they strike up a conversation. It starts out normal at first, but it quickly turns flirtatious. These criminals often, they're very tricky. They end up sharing a nude photo of the person that they are pretending to be.

Paul: They're catfishing, of course. And then they ask their victim to return with a photo of their own. And as soon as that happens, that person realizes they have been catfished and the blackmail begins. It's very relentless. These criminals, you know, they share playbooks and scripts, basically. About how to blackmail their victims, what to say to make them pay money, or else their photos will be leaked to all their friends and family.

Sue: So, I mean, this is such a terrible thing, isn't it? So, what can parents do to sort [00:06:00] of talk about this, protect their kids, make them aware of it without totally terrifying them? And also, you know, having those conversations, so if anything awful does start to happen, they come to the parent to start doing something about it.

And then my next question would be, what do you do about it?

Paul: So, preemptively, I think, all parents, you know, have that conversation where don't send photos to anybody you just met online, don't send nude photos online, ever. I think that has been done, that has been said a hundred times. But I think there needs to be a part two to that conversation, where when this does happen, you can come to us.

We will support you. We'll figure it out. You know, if something bad does happen, it's not the end of the world, and we'll take care of it together. These criminals are actually using the shame, the embarrassment, the fear, thinking that the kids can't go to their parents for help in this situation. And tragically, this crime just in the past couple of years has led to at least 41 teens taking their own life.

Sue: Yes, I saw that on your post around this whole topic. I mean, it's so, so sad and so, sort of scary, isn't it?

Angeline: Thank you so much for your work, Paul. I really learned so much from you, and it's just extremely helpful. One thing I wanted to ask you, how much are these criminals using, utilizing, like AI, for example, the ability to even have conversations?

I know that they obviously, through chatting and sharing images, is it also an issue that they're actually using voice as well to catfish?

Paul: Yeah, we are definitely seeing all of those components. Right now, I would say the majority of financial sextortion schemes are being perpetrated without the use of AI.

But we are seeing an increasing number and I think that threat and that risk is only going to increase further. One way that we're seeing AI being used is these criminals are creating or nudifying nude images of victims. People that are just finding on Instagram, they have never spoken with them, that person they have never taken a photo, and they are using these artificially generated nude images of these people to exploit them and extort them.

Angeline: You know, when I think back of being a teen, it does feel like things are the end of the world, right? I mean, that's a time in your life where it just feels like your small world, everything can fall apart. And I think that is the huge difficulty with this.

Angeline: How can a parent help them really understand, like, it feels like your world is falling apart now. And I, I did read one article about a parent who actually, she did everything right, actually, they reported it. They did everything, and, and the boy, unfortunately, after a few months, he just couldn't handle the shame anymore.

So, in your experience, what's the most effective way to really handle that incredible, incredible shame that teens and kids will feel?

Paul: Let's start with what the criminals say. They are telling these teens; I am going to get you kicked out of school. I'm going to share these photos with your parents. I'm going to post it all over social media.

You're going to be in the news headlines. They're accusing these teens that they were sexting, you know, a six-year-old or a five year, something crazy. You know, with accusations, anything to get these teens to not tell anybody. So, I think step one, it's the hardest step is just to talk to somebody about it, talk through it.

And in these cases, most of the time they are bluffing. They don't intend to actually leak the photos. It's actually bad for their business if they do. And at that point, they lose all the leverage. So, in that case, it's important for Any victim of this crime to block the perpetrator, talk to someone, report the account to the social media platform, also report it to authorities.

The Internet Watch Foundation over in the UK is seeing a huge spike in this crime. The National Center for Missing and Exploited Children here in the U. S. has seen an 18, 000. Percent increase in the past three years of this crime. So yeah, definitely report it to authorities so that way they can do something.

And, you know, worst case scenario, if, if the criminal does end up sharing your photos, it is not the end of the world. There are tools available to take this sort of things down. The Nikuman has one in the U S called take it down. And there are also, you know, helplines that have access to that sort of thing in the UK, Australia, other countries that are highly targeted by this crime too.

Sue: I mean, are there any privacy settings then, or parental controls as well, that should be used on kid's devices, or is it more than that? What are the ste I'm so interested in the steps, because if this starts to happen in a family, it's devastating, isn't it? And then you hear of suicides and all sorts of things.

So, what can parents actively do then? Step one, step two, step three, you know, spell it out.
Paul: Preemptively, I think just having that conversation we mentioned earlier, where if this crime does happen, talk about it as this is an emerging threat to be aware of. If you are aware of how a scam works, you're 80 percent less likely to fall for it.

Sue: Okay, that's good.

Paul: So, it's not foolproof.

Sue: Yeah.

Paul: But definitely just being aware that this exists and you are a target. I'll talk about the two platforms where this crime is most prevalent on right now, and that is Instagram and Snapchat. This data is well recorded in the US, Canada, UK, and Australia. It's pretty much all the same.

These are the top two platforms by design, actually. These criminals oftentimes approach teens and young people on Instagram specifically to harvest their friends lists, their follower lists. On Instagram, once you have connected with someone, there is no way to actually keep outlets private.

Sue: God.

Paul: So, talking about parental settings, you know, I think there's not a whole lot that actually are effective against the financial sextortion scam.

Sue: Right.

Paul: So, if you get an unknown friend request, definitely deny it. But we know a lot of kids do not deny it, especially if that friend request has 10, 15 mutual friends in common. These criminals know that, and that's why they target entire communities at a time, to make their profiles look authentic. So, just being careful about who you accept on Instagram, because the moment that you accept someone's friend request, they can see your entire followers list, your entire social network, and potentially use that against you. On Snapchat, that's an app known for disappearing photos, and kids and teens think that Snapchat is, if they're going to exchange in something risky, Snapchat is a safe place to do it.

Sue: They'll go there, yeah.

Paul: Yeah, unfortunately these criminals know that, and that's why they oftentimes direct kids from Instagram to Snapchat for the photo exchange. And, you know, unfortunately, I think we all realize at this point these criminals are able to screenshot and capture those photos without the kids being aware of it, so.

Angeline: Yes.

Paul: Just, just some more platform design.

Angeline: Yeah.

Paul: Issues with Snapchat.

Angeline: This one thing about Instagram, it made me absolutely insane. Instagram put in the security settings that the youth couldn't send nudes without clicking on are you sure you want to send it. And, and this was all in the news that, you know, this was a step against sextortion, but for me it was absolutely ridiculous because what teen, if they already gonna send a send a nude, then just a little pop up isn't gonna stop.

Do I remember correctly that Meta was announcing that?

Paul: Yeah, Meta, Instagram announced quite a few different safety features over the past year since we've been raising this nationally and internationally. Most of their solutions, I would actually say are performative. Some of them might help a little bit to some extent, but like you said, you know, this, this teen nudity protection feature that they were touting as this, this great feature, all it does is it detects if a teen is sending or receiving a nude image. It blurs the image and it gives the sender or the recipient the option. Hey, tap this image to unblur it.

Sue: Oh my God, oh my God.

Paul: So, there's absolutely no, you know, blocking of nude images and to be honest, that's even worse because they're saying, hey, we are detecting a teen sending a nude image and we're actually allowing it to go through.

Sue: Oh, how depressing.

Paul: Instead of detecting it and blocking it, they're detecting it and blurring it, but still making it easily accessible.

Angeline: I can't understand why that's legal, because it shouldn't be illegal, you can't, but anyway, yeah, that makes me absolutely crazy.

Sue: Clearly now, tech companies are not really playing their part, are they, in preventing sextortion. Is that right, in your opinion?

Paul: In my opinion, yes. I think some teams at some of the tech companies have made some strides, but by and large, I do not see this crime decreasing anytime soon.

Sue: How depressing, isn't it? I mean, it really is. What is your thoughts globally then? Are there any particular countries doing more than others?

To protect young people.

Paul: Oh, that is quite difficult. And the difficult part of this is oftentimes these criminals are overseas in places where we don't have extradition or we don't have a large law enforcement presence. Great majority of the financial extortion that is targeting teens right now is coming out of West Africa, specifically Nigeria and the Ivory coast and the cybercrime group behind a large majority of this, they call themselves Yahoo boys.

Angeline: I'm always a little bit focused on kind of the worst-case scenario, how to react in a worst-case scenario. And what really interests me, and I wasn't aware that you said before, that actually they often aren't motivated to share the images. Because what comes out obviously in the news, I had the impression that they actually almost always share the images.

And I think this is actually one of the really important messages that parents can give, right? So, what's the reason that they are not financially motivated to actually share images in many cases?

Paul: Well, we see these criminals just moving on very quickly. This is a scam of numbers, and the more targets that they can get, the more money they can get.

So, if a teen decides not to pay, and blocks the criminal. The criminal is much more likely to actually move on and communicate with 10 other people that same day trying to get money out of them versus spending their whole day just trying to ruin one person's life. That doesn't get them any money.

Especially, you know, once they send that photo out or share that photo, they lose any leverage that they had against that victim, and they know they aren't going to get paid at that point. So, most of the time it is a bluff, and I think that is reassuring for victims, just to know that the criminals aren't actually, you know, out there to leak the photos and just to get paid.

Angeline: Yeah, it is, really. I wasn't aware of that. And how about the international collaboration in terms of trying to support in the countries like Nigeria and the Ivory Coast to help the governments there kind of shut that down at the source. Do you have the feeling that the different countries are working together?

Paul: One thing I thought that was super encouraging, the FBI director, Chris Wray, visited Nigeria for the first time ever as the director of FBI on an official trip to that country. And he had two things on the agenda, terrorism and sextortion. So, you know, the fact that this has elevated up to that level, I think is definitely encouraging in the eyes of law enforcement.

As a counterpoint to that, we are aware of 41 teen suicides globally since, since the end of 2021. During that time, there were over 30, 000 reported cases of teens getting sextorted. Multiply that times 10 for the number of unreported cases, probably. And we've only had a handful of folks arrested from these countries who are doing it.

Two folks were extradited from Nigeria. They are now serving 17 years in federal prison in Michigan for the death of a teenager there. There was a Canadian boy who died via the scam, and the criminal in Nigeria is serving his time for that. That's it, really. The other 39 cases are unaccounted for, and those criminals are still at large. So, we need to do better.

Angeline: Yeah, because if you would manage to shut it down in one country, they would just move to another one, right? Do you see that happening?

Paul: Once we're able to solve this crime in Nigeria and the Ivory Coast, you know, who knows where else it's going to pop up next.

Sue: So, are there any resources or hotlines or organizations that you recommend for families affected by sextortion, or they're looking to learn more?

Paul: Yeah, in the UK, there's the Internet Watch Foundation that oversees safety issues like this for minors. There's also the Revenge Porn Helpline for folks who are over 18, dealing with this issue. If you're in the United States, the National Center for Missing and Exploited Children is your best resource. And if you're in Canada, the Canadian Centre for Child Protection is there to help.

Sue: If you could leave parents with one critical piece of advice about protecting their children from sextortion, what would it be?

Paul: Talk to them. Talk to them today. Let them know this scam exists. Let them know that they are active targets right now, today, for this scam. Let them know that if they do end up getting in a situation and they're in trouble, they can come to you and it's not the end of the world and you will help them through it.

Sue: Thank you so much for your time and joining us on Navigating the Digital Jungle, Paul.

Paul: Thank you so much. Really appreciate it.

Sue: Let's hope we make some differences with families around the world. If one or two or three just start those conversations today, we've done some good.

I'd like to tell you a bit more about my new book. As a parent myself, I know firsthand how overwhelming it can feel to keep up with the digital world our kids are growing up in. That's why I wrote Navigating the Digital Jungle Essential Scripts for starting meaningful conversations with toddlers, tweens and teens about smartphones or social media.

My book is bursting with ready to use conversation starters that make it easier to guide your kids through everything from screen time and social media to the tricky terrain of online safety and artificial intelligence. It's like having a roadmap for those critical and important chats every parent needs to have.

My book of digital jungle scripts is all about giving you the tools to start those difficult but important conversations, no matter your child's age. Easy, practical scripts to help you feel confident and connected. So, if you're ready to feel more self-confident around discussing Roblox, Snapchat or WhatsApp, grab your copy of Navigating the Digital Jungle Essential Scripts and start transforming those tough tech talks into meaningful family moments.

And let's get those conversations started at navigatingthedigitaljungle.com/resources.

Angeline: So, now it's time for our family change segment where we talk about a simple but effective way to increase online safety and prevent situations like sextortion. Obviously, we've been talking a lot during this episode about having conversations, being open, and that's basically it. How are we going to have the difficult conversations?

And our proposal is to have a weekly online safety check in just to have some kind of conversation, you know, just how it can work is that you choose a specific time each week where everyone is relaxed, maybe before dinner, after dinner, something like that. And encourage openness, obviously you can openly explain that isn't meant to be invasive, it's not meant to be, you know, you coming in like big brother, but it's just simply a very difficult topic.

And obviously, think in advance how you're going to respond if something goes wrong, if someone contacts them. And ask for inappropriate things or if they unfortunately make the wrong decision and you have to decide together what to do. So, that kind of regular check in can really do a lot to establish trust and keep your children safe.

Sue: Yes, and I think educate yourself and your child. Explain sextortion really clearly, help your child understand what sextortion is, emphasizing that it involves someone threatening to share private or sensitive images or videos unless they comply with their demands. So, it's age-appropriate conversations, of course.

Tailor your discussions to your child's age and maturity. And ensure that they do understand the risks without feeling overwhelmed. I found a really interesting post on Instagram this morning. It said a child who has been educated about how to reject pornography and sextortion is safer from sex traffickers and sexual exploiters of any kind.

And that was by Lisa Thompson. So, if you go to Navigating the Digital Jungle on Facebook, you can see that poster and you can read a bit more about it.

Intro: Listener's Questions

Sue: And that now leads us into listeners questions. How can I explain sextortion to my teen without scaring them? Well, Penny from Brighton, I hope we've kind of covered some of this, but it's important again to reiterate that talking about any sensitive topics like sextortion can be tricky.

But, here are a few tips to help make the conversation productive rather than scary. So, frame it as awareness, not alarm. Let your team know that you want to talk about sextortion, not to scare them, but to empower them. Emphasise that just as they take precautions in the real world, online awareness is equally important.

Also, be honest, but be age appropriate, you know, tailor your explanations based on your teenager's age, but not only their age, their maturity, because for younger teens, focus on the importance of not sharing private information with strangers, and for older teens, get into sextortion scams work, and why they should always be wary of sharing anything intimate online.

Even with their friends, when they're playing these games, just have that kind of distrust mindset a little bit, and then share some practical steps, not just the risks. Make sure your teen leaves the conversation feeling prepared, not helpless or frightened. Discuss the importance of privacy settings.

Time and time again, we say this. And ignoring those messages that pop up sometimes from unknown users. And you think, oh, do I know that person? And you think you might, but then you're down a rabbit hole. So, knowing who to talk to, if they ever feel threatened again, is really important. Come to you or someone they trust so you can start to help them feel safe.

Intro: Now for some top tips.

Sue: Weekly quick tips, extortion prevention for the whole family. Here's my quick tip this week, I hope it helps, set up private accounts, encourage teens and tweens to make social media accounts private. This allows them to control who follows them and it reduces the chances of being approached by strangers.

Angee, what's your tip for this week on that?

Angeline: I actually think that we've gone through basically everything. I mean, my tip is,

Sue: Yeah, I hope so.

Angeline: This is the kind of thing that scammers will always get more creative and think new ways to kind of trick us. So, it's really all about having the conversations trusting that no matter what happens, it's not the end of the world. Maybe that could be my quick tip, remind your team back to what it was like a team and all the little things like the end of the world and that's there's not a little thing. So, yeah, maybe that's my quick tip. Just you know, remind your team. It's not the end of the world and that you together can get through anything.

Sue: Yeah, and remember to block and report rule as well if there's any sort of, any doubt. So, that leads me on to script of the week. You know, my quick scripts to start important conversations. I've got a whole book about this, but each week now in this new season, I like to give you a quick tip. Just gives you something to sort of start the conversation with that's, you know, open and not judgmental.

So, here's a starter for tenors, they say. So, you could start by saying, I've been learning more about online safety, especially around some of the risks that young people face online, like sextortion. Have you ever heard of it? So, then they respond with whatever they say, yes or no. And then you say, it's when someone online, often someone pretending to be a friend, tries to get personal images or information and then threatens to share it unless you do what they say.

And that is a really scary thought. But I want to make sure that you know what to look out for. So, then your child might start to ask you some questions and share their experiences. So, you started the conversation and then you say, well, remember, you know, if it starts to feel a bit weird, or if someone ever makes you feel uncomfortable online, you can always come to me no matter what, I'll be here to help you sort it out. Because this is the script, I think, that helps you introduce the topic in a way that doesn't overwhelm everybody, but then also invites them to share their own thoughts and their own experiences and then you've popped in that you are there no matter what to support them.

So, Angee what are you working on at the moment?

Angeline: I'm working on a global online safety conference where we have a lot of interesting topics and speakers. Also, you, Sue, I'm looking forward to bringing some of Navigating the Digital Jungle there too. And other than that, I'm just kind of expanding on Data Girl and Friends. We've joined Pinterest now, so you can find us there.

And, you know, just trying to increase awareness, especially about AI, because I'm really passionate about everything that's happening in AI. So, you can find it at data-girl-and-friends.com slashes, between all the words.

Sue: Brilliant. I call them hyphens, but hey, I'm British.

Angeline: That's probably the right word, actually.

Sue: Well, I'm working on some school power hours that I've been delivering to schools. It's an hour, it's a power hour, it's like a Zoom webinar, if you want to call it that, where I talk about five top challenges for parents and how to solve them for parents in school. So, I go online with the school and I deliver my power hour around these five top challenges with practical tips like the podcast really.

But if you want to go a bit deeper onto online safety, be sure to check out my guides and blogs for parents and teachers. All are downloadable resources. They include detailed strategies for managing privacy settings across all sorts of popular apps. There's additional conversation starters there for those difficult online conversations.

There's step by step instructions on reporting and blocking. There's loads of content on Navigating the Digital Jungle under Resources or under Blogs, and you can go and meet the team there as well, actually, to find out more about Angeline and what she does.

Intro: Navigating the Digital Jungle with Sue Atkins and Friends.

Sue: Thank you for joining us today on this episode of Navigating the Digital Jungle. Sextortion is a real and rising threat, but by staying informed, practicing open communication, and taking some simple precautions, we can protect our families from falling victim to this harmful exploitation. Stay safe, stay connected, and remember, digital awareness is the best defense against digital dangers.

Remember you can subscribe, leave us a review, tell all your friends about us. It's a free resource you can put into your school newsletters. Send in your questions, we love hearing from you. Until next time, take care.

Intro: Yeah, It's a jungle out there.

Sue: I'd like to tell you a bit about this episode's sponsor, Mobicip. Are you worried about your child's online safety? Well, Mobicip's here to help. This all-in-one parental control app keeps your child away from risky apps and inappropriate content across all devices. Plus, you can manage screen time, track location, and foster healthy digital habits.

Join more than 2 million parents and get peace of mind with Mobicip. And start your free 7-day trial today at mobicip.com That's Mobicip (M-O-B-I-C-I-P) mobicip.com