[music]

**Rihonna Scoggins:** Hello and welcome to *Fraud Talk*, the ACFE's monthly podcast. I'm Rihonna Scoggins, the community manager for the ACFE. Today, we're joined by Jenny Radcliffe, aka "The People Hacker". An ethical social engineer and burglar for hire, she helps companies test their security through simulated criminal attacks using her social engineering skills. Jenny, thank you so much for joining me today.

**Jenny Radcliffe:** It's my pleasure. Happy to be here.

**Rihonna:** I'm really looking forward to our conversation today. Your experience is really interesting, to say the least. Now you're at this point where you've spoken at many events, and for different companies, and some of our own members may even recognize your voice from our anti-fraud leadership summit that we had last year. Can you tell us a bit about your unconventional experience that led you to where you are now, giving talks, authoring books, and helping companies?

**Jenny:** Sure. Within the security industry, social engineering is not such an unusual job. Although a lot of the time people will do the same job to me use technology. Social engineering is all about hacking a company at their request. At least when you do it actively like I do, at their request. It's a cross between a fire drill and *Oceans 11*, but we're not that good-looking.

We put together a team, I put together a team, sometimes I work on my own, in order to test the human side of a business' security. That would be everything from whether people follow the rules, or whether we let people tailgate through gates and reception, whether we give our details away or information away through phishing e-mail or phone calls.

Also, what I do that's not as well known is we actually break into buildings. We actually do our best to bypass security, to get into a site, and work our way around that site to find out, sometimes we have a target from the client but sometimes it's just generally, are there any things that I might see that I think could be a security risk. Then it's an education piece, we report back to the client, and we help them fix those issues so that the real criminals can't do it for real.

I guess this is a job that I've done in the open for maybe 15 years, but all my life really, and that's because nobody really spoke about this until cyber became a thing and the internet became a thing, and you realize that there was more people than just me who did this. I started just as a kid where I grew up in the UK. It was not such a great neighborhood.

A couple of things happened when I was younger that were a bit dangerous. My parents basically asked my family, my older cousins who were much older than me, much more streetwise than me to teach me a few things and to look after me. I ended up following them getting into empty buildings, derelict buildings, just out of curiosity. Gradually, we've got into occupied buildings, but that was at the request of

the owners just as a little job. Then I gradually grew the business into what it is today.

**Rihonna:** It's so interesting how you paved your way into this career. Can you tell us about your first ethical social engineering job? Did the company come to you? How were you recruited for that? Were you like, "Hey. I know I can get info from your employees that you wouldn't like. Do you want to pay me for it"? [chuckles]

**Jenny:** It depends what we say. It depends what you say. Those first jobs that we did after we did it as a hobby, and somebody had said, we have soccer players live near where I'm from, and they have big houses, and a lot of robberies were happening in the neighborhoods at the time. They asked us, "Well, if you can get into buildings, is there a way that you can get into our house, and show us what's vulnerable, and help us fix it?"

They paid us for that, me and my cousins, but I was very young at the time. I was involved because being a woman, I was less threatening to the families, the wives, and things than the boys were. Really, those are the first real paid jobs. Then I was paid to look at a government building in Liverpool where I'm from by someone who was a friend of a friend. He knew people in my family. I honestly don't really know where he got my name from, but I guess he's done a few of these jobs in and around Liverpool. It was unusual. The boys were just about on the right side of the law, but they were security guys in bars and things. Slightly less, I suppose, visible than I was at that age. Also, I did all the reports, so there was me.

I actually got a call at home that asked me to go into this government building and steal a diary from a desk just because as a security test. Can it be done? Is the security adequate? Would the guards stop you? I didn't ask enough questions, and even though I now know that the reasons behind that, and that it was justified and legitimate in a way, it wasn't as legitimate as we do it now. In other words, I'm not sure that the guy who actually owned the diary knew, but everyone else around him knew, so the company, and everything knew, and the security guards because he turned out not be a very good person.

**Rihonna:** Got you.

**Jenny:** That was the first time I ever worked on my own. When I got the call, I said, "Well, I'll ring the boys and I'll see if they're free." The client said, "Well, do you have to do that? Do you need them?" It just occurred to me that I probably didn't.

[laughter]

**Jenny:** I called them anyway. They said, "No, no. Go for it. Make some money." After that, it just built and built. I think because it's an unusual job, the way I approached it was very unusual because, Rihonna, I had no tech skills. I had no money. It was all about outthinking the building, the security team, and the target. That's what makes my job and the way I do it more unusual, I guess.

**Rihonna:** Definitely. Like you said earlier and just then, you don't use any special technology or tools for your work. You're really just armed with your words, which is a little bit scarier, I have to say.

[laughter]

**Rihonna:** You don't need all these tools to do your job and do it well.

**Jenny:** They help.

**Rihonna:** Okay. [laughs]

**Jenny:** I've got colleagues, some people in my network who are brilliant hackers and who can bypass security in lots of different ways. That's wonderful, and I wish I had those skills, I don't. It's not too late to learn, but I don't have the time. I think it was more a case of what makes it so compelling to security teams is that we can throw millions at security, of fences, on alarms, on doors, anti-malware, and the tech's very good. It does a lot of the heavy lifting when it comes to keeping our businesses and ourselves safe.

I think what's compelling is that because of humans in control of that technology, a human can be bypassed. For us, our USP really are niche. My niche was that look, without, in the absence of that, can we do it in a more human way, a more elegant way, a more simple way because those are the ones that get passed? The tech can be hacked, everyone knows that that can happen, but it's very, very good.

Is there a simple thing that could be done that makes exposes us in the same way? I use skills like negotiation techniques, influence persuasion, reason, nonverbal communications, deception work. There's lots of things that we use to just make people do what we want them to do, which is very often open a door or share information.

**Rihonna:** Right. You mentioned these different tactics that you use. In your opinion, what are some of the most effective techniques or tactics for social engineering? Maybe, how can people or companies protect themselves from being manipulated by social engineers? In just the simplest way. I know there's so much more than can be said in a podcast.

**Jenny:** Yes. It depends on what you mean. What people need to-- if we take the first part of that question, which is what techniques and tactics, the technique that is the most effective still is phishing e-mails. Even though we put lots of protection in, and we have lots of tests, and the jury is out in the security community of whether those phishing tests are really effective because we can write things to make sure that people follow them or fall for them.

The e-mail is the way to get people to interact with a hacker. What's happening with social engineering is that it's a blended attack. It's the human alongside technology. You need a human to write a convincing script and then the technology to access the

system if they click on the link or open the attachment, right? What social engineering will also try and do is try and get people off technology as soon as we can, get them off the site, off the network, because criminals know that that's protected and detection is likely, but a phone call or a social media interaction leaves less of a footprint, is harder to trace.

The techniques are everything from those text messages to vishing calls, scam phone calls, all the way up to in-person "chance meetings" and social media interactions. For example, something like romance fraud might start with social media, but the target might be where you work. It might be that they look you up on, say, LinkedIn, find out where you work, and then research you a little bit and then try and get to know you as access to the company. People often think that they're not rich enough or important enough to be hacked, but everyone's worth hacking. The techniques will always be whatever way humans communicate can be manipulated by a criminal.

Now, how do they do it? Well, from a tactics point of view, and I spoke about this when I spoke for the conference in New York, there are red flags, and there's lots of different ones, but really, I essentially boil it down to four things. They're going to make people feel emotional in some way. Is it the sob story on a romance fraud that they've had an accident, they need medical bills, they've been caught up in some natural disaster and they need the airfare?

There'll be some emotional elements of these stories often, as in those two examples, mixed with urgency. Then money is going to come into the equation, and so is a call to action. The four things are emotional content, some time, urgency, and then money, usually, as well as a call to action. Now, it's difficult with money because obviously, we all deal with money and we all deal, for that matter, with e-mails, links, and attachments all the time, so it's difficult, but that's really how they're going to try and get you with social engineering.

In terms of the buildings and stuff, it's similar things. It depends on the client, what story, what script will work, but they will fit it to something around those things. That's really what's happening. Social engineering attacks, attacks that involve human error or manipulation, are a very high percentage of cyber attacks because they enable cyber attacks, they enable hackers. They need to weigh in, and that's usually humans that give them that, but I think the numbers are-- some think tanks give it as much as 95% more.

It's a huge amount because someone somewhere has to give access, ultimately. That's that side of it. Now, you asked me, Rihonna, about what we can do to prevent it as companies. There is a lot of things. You have to have technology these days to try and block some of the malware and things that come through on e-mail. We have to pay for good security in terms of on networks and our teams. It's expensive, and people do still see it as a cost center, but it is so much better to do it than be hacked, right? Or conned, or defrauded.

It's no longer just a cost center that we will negotiate whether or not we need, you have to have security in your business regardless of the size. Then we have human things that are free or almost free. For example, security awareness training for your team. You can spend millions and millions depending on the size of the organization, but the truth is, as long as the team are talking about security, there's a lot of free resources out there that you can find with basic awareness advice. Lots of videos, podcasts like this with people like myself can all help your team be aware.

What needs to happen is, that team needs to know what social engineering is and these stuff that goes along with it from a cyber point of view, but the thing is, the stuff I specialize in is much more compelling than cyber a lot of the time. A lot of people want to hear about someone breaking into a building as opposed to another virus.

It's just true, but it's available. People need to know it. They need to talk about it in their weekly meetings, in their line management meetings every week. Did anybody get phished this week? Did anyone see an e-mail that looked dodgy? Why do you think it looked dodgy? Has anyone seen a movie with fraud in? Has anyone seen an article in the news about hacking?

It just has to become part of the conversation in the same way the health and safety did. That you just have to have your team talking about this amongst themselves. It cannot be that you have a security person or throw money at some security tools and it fixes it. It just doesn't. It has to become part of culture. There's all of that stuff. Then it has to be the people feel comfortable reporting when they've made a mistake or when they think they've been conned. That's a cultural thing within organizations. If we blame people for falling for this, no one will ever say when they think they've fallen for it.

All of that is part of it, but then there's basic, what we call cyber hygiene. There's basic things that can stop you being conned and defrauded as a company, and partly is keep your tech up to date. If you look at something like WannaCry, which was a big attack a couple of years ago, a big cyber attack, that took out a lot of the UK healthcare system for a couple of days, but there was a patch available. People just hadn't updated their apps, hadn't updated their software.

People still reuse passwords, they still share passwords amongst teams and things for certain things. All of that stuff that we all know or at least have been told, it only works if we do it. Then it's just making yourself a harder target. Don't put everything about you out online. That goes with the business as well as personal. Control your audience. Control what's in the post in the picture, put that attack ahead on and see things from an of mindset.

If I meant this company ill, how could I use this information? Then we have to carry on with our lives and our businesses, but it's a big answer. It's a long answer to a short question, but it's important because I will talk about this endlessly if it helps people protect themselves.

**Rihonna:** No, definitely. Thank you so much for all of that info. I knew it would be a lot, but I think like you said, it's incredibly important. My favorite nugget of knowledge from that is that it's not any one person's job to protect a company. It's every employee's. We all have to be careful and safe, and like you said, we have to get rid of this stigma around being a victim of a phishing attack or any sort of fraud. That way we can talk about it and learn from it, so thank you for that.

**Jenny:** My pleasure.

**Rihonna:** With the career that you have, is there a conventional route into getting into it, is there any training or education or experience you may recommend to a CFE or someone who's looking into having a career as an ethical social engineer?

**Jenny:** There really isn't, and there isn't even, really. There's a huge gap in the market for me to do training on this right, but there really isn't anything that I would out and out recommend in terms of purely what I do. Now, if we look at the cyberspace, there's lots and lots of courses that are technical in nature, and some of them have a social engineering element, but for example, I had a friend of mine went on a very popular course that was built as social engineering.

It cost thousands of pounds. It was done virtually on a global basis. She came to me at the end, she said, it's not social engineering. She said, there's an element of influence from Robert Cialdini's work. There's some element body language from Paul Ekman's work, but really, it's not really what you do. This is the problem. It's not really pure social engineering, and that's for a couple of reasons.

It's because technical skills are so useful and harder to be certified-- well, easy to be certified in, but harder to-- Social engineering's hard to isolate, right? People want some technical skills as well. Social engineering in and of itself is something that's quite hard to learn because what it really relies on is an interest in people and in human behavior. It takes in lots of different routes. It takes in psychology, even anthropology, some linguistics elements there to analyze scripts and to help persuade and influence people.

There isn't really a conventional route into it. What I say to people is if you really are interested in social engineering, then I've listed already a lot of areas that you should look into, but you should also start to follow some of the security community because there's something called the Security BSides and you can look it up on YouTube or online, and those are community conferences not for profit and they're held all over the world. The first one was in Las Vegas. There's lots and lots in America. I think Vegas is the biggest, then London is the second biggest.

That involves people from the community, non-paid speakers going in and speaking at these things and talking about their career, their research. Within that there's lots and lots. It's a mine of information for anyone who's interested in these things. I think what it does is it shows people, oh, look there's lots of routes and lots of jobs in security. I don't have to be purely technical, but these are the technical skills that help. I think what happens is people with some technical skills and an interest in

social engineering tend to get jobs then with firms that do pen testing which is what we're talking about, penetration tests.

There's no conventional routes into it but if you are good with people and you've got an interest in security, you'll find a way. If you're good with people with an interest in security and a couple of technical skills, then you're likely to get a job at a technical level to start with and then be deployed on jobs that involve social engineering. Again, a long answer but there isn't a simple one, I'm afraid, for a lot of this.

**Rihonna:** [chuckle] You said that you will sometimes work with a team, sometimes work by yourself. This team of people that you work with and that you have, is that their background as well? Is that their route or is it a hodgepodge of different experience?

**Jenny:** I love that word. It's a hodgepodge. I don't have a permanent crew so I recruit the crew depending on the job and the client, right? I would use a different crew if we were looking at a hotel than I would maybe a private residence or a hospital. They have different skills and different backgrounds and it's a contract basis for me. Now, other security firms do have permanent employees but for me, that means that we say, oh, someone's asked for social engineering so we'll put our social engineers on the job, as opposed to someone's asked for social engineering, who do we need?

Do we need former military people who are big and tough and angry and can pull doors off their hinges? Do we need hackers with a particular expertise in certain type of cyber attack? Do we need people who can climb high buildings? Do we need role players who will fit in with the culture and the aesthetic of the company? We fit. That's how I work. I fit the team to the job and I recruit from my network. I have some people I always work with, but I recruit from the network.

That's really the way that I do it. All of those people who've worked with me in the past are very welcome to come out and say they've worked with me, but I'm fairly sure they won't, and that's just because I always recruited people who were more interested in the job than the spotlight. I think certainly in the last year or two, it was starting to become clear that because I was so focused on bringing this message to the wider public and to speak in and doing whatever work I could to spread the words, then I would be the one that would probably do that.

Now if they come out and do it that's fine, but it's just that I have a feeling that probably most of them won't. Some of them are just still in a normal regular job. They just help me out now and again. Just think about everyone who's listening. You could be doing whatever job you do all the time and then take a few days off one week and come and work with me. That's what we're saying. [chuckles]

**Rihonna:** This is all just a recruitment message. [chuckles]

**Jenny:** Just a recruitment drive. Absolutely.

**Rihonna:** I want to go back a little bit. You mentioned one job that you did where you were getting that diary. A big part of your role is the fact that you're doing all of this for the right reasons, right? You're doing it ethically. What are some of the ethical considerations that come into play when you're engaging in the work the way that you do? How do you ensure that you're not crossing any legal or moral batteries when you're running these simulated attacks?

**Jenny:** Well, these days we have a contract [laughs] that says this is what you are allowed to do. This is the boundary. The same goes to the client. This is what we're going to do, and they agree and that's all fine and dandy in terms of legal. Ethically, I make very sure apart from the obvious things like we don't steal anything or break anything without permission. By which I mean if we steal anything, we bag it up and give it back. If we break anything, it's within the contract that we're allowed.

Sometimes we'll say by destructive/non-destructive means, right? The client can say-- sometimes they'll say it's okay to use destruction safely to the tune of, say, $3,000 or something. What that means is we could break a window or a door or a lock or an alarm, maybe a small one on one door. Very often I will say we'll do it non-destructively, right? We're not going to actually blow the doors off. Some people know what that's from. I avoided case in there.

Ethically is slightly different because, obviously, we are bamboozling people even though it's with good heart and with the best of intentions. From an ethical point of view, we have meetings with the client, we do talk to them upfront and say nobody can be fired as a result of falling for what we're about to do because we are professional con artists and therefore they will be conned, right? Sooner or later want someone will fall for it. I also go and meet with the people that we've directly face-to-face conned or over e-mail and I do speak to them one-to-one and talk to them about why they shouldn't feel bad about this.

To spin it in as much as and the spin on this is you've learned a big lesson. You're not stupid for falling for this, you were just targeted and that can happen to anyone, it could happen to me. Now you're an ambassador for this, right? Now you know how it works. Now you can see that anyone can be fooled. What we ask you to do is don't beat yourself up or talk to people and tell them how this was done. I think ethically that that's the main thing, is that cause. First, do no harm. Do not hurt people on our quest for security, if you like. We only take that as far as it needs to go and we do everything we can to try and make sure that those people don't feel bad.

Then on the job, we don't reveal who the clients are. I've written my book, the book is 300 pages. You can't tell who the clients are. You might have a good guess and certainly some of the UK references have had journalists already say, well, was it this person? I just will never confirm or deny who they are. The clients are protected through redaction. Basically, we redacted and changed some details which I made very clear. We never named them.

Although the book gives a lot of tactics that we've used and lots of examples. Unfortunately, the book's not in America yet. It won't be. We're still negotiating the US contracts, actually, but it will be hopefully this year. Although I've given some away, that's nothing that you couldn't find out if you were determined to do so online.

I feel okay about that as well, although I always worry. Then the other thing is that we don't steal or do anything that we don't need to do to get the job done, right? There's no showboating. I always say there's no parrots, we don't talk. There's no peacocks, we don't show off. There's no magpies. In other words, we're not distracted by the shiny things. We don't take the shiny things. That's really the ethical consideration. Legally, it's not such a big deal, that's sorted out with the lawyers, but ethically, we have to cover ourselves for sure.

**Rihonna:** Definitely. You guys get to have these conversations about what you can and can't do. The reality is is that criminals don't care. They're not like, "Hey, can we do this or that?" When you are in these situations, do you say, "Hey, we could have done this if we wanted to. That wasn't really the goal of this attack, but we could have gone this route and even gotten more"? How do you disseminate that information to the clients of maybe just how vulnerable they are?

**Jenny:** Well, there's a couple of ways. Sometimes we just explain, so obviously, if I had malintent this would've gone this way. There are fun ways that we can demonstrate it. For example, there was a point when I was outside the door of a secure room which controlled let's just say something incredibly dangerous. I can't really say what it was, but something so dangerous that it's really bad that I even managed to get to that door. The next task was to get through the door.

A guy stopped in front of me and I gave him the script and used a few bits of persuasion. He had his lunch with him, so his hands were full and he was fiddling with his pass. As he went to do it, he had the pass in his hands and his lunch in the hands, a colleague came and she said, "Wait, wait, wait, you don't know who she is. We haven't seen proper ID. It could be anyone."

To her credit, that stopped us, but what I did was I stuck a sticker. I got a sticker that I had in my hand, and the sticker just said "Yes" written on it. Just a big sticker with the word "Yes," and I just stuck it on his stomach. Then he's like, "What are you doing?" I said, "Because I could have had a knife or a gun, basically." We've just shown that, like in that situation, if I'd have been a criminal, then it wouldn't have been a sticker, it would've been a gun or a knife and we'd have been in. That's the demo.

It's a non-lethal, almost funny-- Sometimes we'd right "Tickle" on it. Sometimes it's just a picture of a banana or something, just something silly to diffuse it a little bit but just to show that we had physical contact with that person. The other thing we do is take a water pistol in the back, and we take the water pistol and sometimes we put some-- Oh, this is giving things away, but we'll put-- or a toy gun. Basically, a toy gun and we'll put that in the back or I'll put it in the back of my pants or it'll be somewhere

on me hidden in my clothes. Then I did one job where again, I got right to the top guy in this huge important place, and I really should not have been able to get in, and just took it out and just went," Bang."

It's clearly a toy gun. Just let me say, this is UK. This is bright blue. Let's just say for arguments sake, it's got Mickey Mouse on it or something. It's really obviously I'm not going to hit anyone, but we'll slip in, and we have actually squirted people with-- we filled them up with soda and stuff as well, and got them with the soda, so it stains, which is terrible, isn't it, but just so it's not just water. I just can't, "Oops, bang, bang." It's also just to show without people being frightened that we got that close. I think there is no lesson like a demonstration to show that.

We are always very conscious, so I wouldn't get a replica firearm because someone might be genuinely frightened. Obviously, we're the good guys, so we're not going to do that, [laughter] but it does show the points. We've done it. Again, we'd use like-- I don't know bananas **[unintelligible 00:33:49]** but we'd use bananas as well just to show we tap someone with a banana. You could take a banana in any way, so it doesn't make the same point as a toy gun, for example, it just shows that the bag wasn't searched. Because they are usually plastic, we actually fill them with metal, but I won't say how we do that.

**Rihonna:** Crazy interesting. Thank you for sharing that.

**Jenny:** That's okay.

[laughter]

**Rihonna:** When you were talking earlier about all the different type of people you've worked with and you mentioned big, strong military guys, but you're not a big, strong military guy. How have you seen your gender come into play, and how has it helped your work and when you're doing these simulated attacks?

**Jenny:** I'm asked this a lot, and the answer I always give is just that I just don't look dangerous. Those of you who saw me in New York, you knew I didn't look dangerous. Nobody pays me a second glance until they do. I think that's very helpful. It will be less easy to do that or to walk around or to make conversation with a receptionist or someone just if I was a guy, just because no matter how well dressed you are, there's always that element of someone's physically bigger or could be hitting on- if it's a woman or whatever, could be hitting on you.

I don't have those disadvantages. I have privilege and advantage because I am- and this is such a paradox, because I'm basically someone who doesn't stand out. I'm a middle-aged woman. I don't particularly stand out. I can be charismatic on stage, I guess. Otherwise, people wouldn't want me to speak on stage. It's very much something that can be switched off. I think that's really helped.

I just think a guy would struggle a bit more with that anonymity in terms of what security you're looking for. Our prejudices are that men are criminals, that men can

be dangerous and that women are not. That's not necessarily true, a criminal doesn't always look like what we think a criminal looks like. A hacker doesn't look what we think a hacker looks like from TV and films. I should be wearing a hoodie and all the rest of it, and that's just not how it really works.

I think those things have been useful. I think as well, people open up to women. Sometimes women particularly might open up more to another woman than maybe a guy. I don't know that's always the case, but I just think sometimes it's the case. I think that's been helpful as well. There's that empathy and the women who are listening to this will know what I mean, there's that empathy and that shared experience that's helped. Whereas I think with men, that might be something that might be harder to draw out of someone. Not all the time, but just, I think occasionally that might be the case.

**Rihonna:** Definitely. As a woman in this seemingly male-dominated field of helping companies test their security measures, have you ever faced any challenges or biases in your work? Have you ever felt like, oh, this person doesn't think I can do this because I'm a woman, or because I look so--

**Jenny:** I'm letting you struggle. Innocence?

**Rihonna:** [laughs] Yes. Innocence. Yes.

**Jenny:** Harmless?

**Rihonna:** [laughs]

**Jenny:** Yes, I guess, I mean, yes. Women, I think most women would tell you that there's been times in their lives when they've been perhaps taken advantage of or underestimated in some way. I would say I was constantly underestimated by people who very much regret that now. Constantly because of where I came from, I mean, I still now get the most ridiculous comments because I have a regional accent, I'm from Liverpool in the UK, it's a regional accent.

People might think I've not got a good education or that I actually am a criminal. Which is just so tone-deaf these days to think those things. Or that I was asked an awful lot in the beginning of my career, "Who's looking after the family if you're away?" As if I was going to go, "Oh my goodness, I need to make a phone call. Everybody stop everything. I've forgotten about my children, or whatever."

Even now the books come out in February in the UK, it's been already very successful. I've done a lot of media and interviews about it, which is I'm very grateful for. I've been asked an awful lot, "What does your husband think about your job?" It just makes me wonder whether anyone would ask a man in the same position, "Well, what does your wife think about your job?" When was the last time you ever heard that? What's that got to do with anything anyway? I find that I observe it now. I suppose it doesn't bother me now because I'm too long in the tooth, I think, and just too grumpy to really worry about it. These days I'm grumpy with that kind of attitude.

**Rihonna:** Definitely.

**Jenny:** I think certainly from a security point of view, the amount of people who's jaw has hit the floor when I've said it was me, or that we did the job. Who knows whether that was gender-based? I think it probably was a lot of the time. I've certainly been mansplained [laughter] even now. I mean, I had someone read the book and say, "Oh, you could have done this this way."

**Rihonna:** Oh goodness.

**Jenny:** You're like you don't want to flex, but you could say, "Do you know what? I am probably one of the best people in the world right now at three or four things that I do, you know? You've never done it, and you're telling me how to do this, right? I'm top of my game, son." People don't like to hear me say that even now. It's like, who are you to try and explain this to me?

I think we think mansplaining is something that just was meant to women, but I think it's people to people, actually. There's certain times when we just think that we've got the right to give someone an opinion. I just would caution all of us, men or women, just be very careful what you assume about a person.

I'll just give you another example. I did a a gig. I can't say much about it because it will totally give it away because it was all over the media. I did a gig and there was this young guy who was lovely in every way. It was a speaking engagement and there was probably 200 people there, something like that. Bear in mind, I do over a hundred speaking engagements a year all over the world. Some of them are virtual with tens of thousands of people.

Some of them are very scary because there's six people but they'll all be hugely important directors of some massive brand. The vast majority of them are at least 200 to 400 people in a room all the time. I've done that job, keynote speaking again at the top of the category for where that Abby put for easily 20 years, off and on. This little chap says to me, "Oh, there's 200 people tonight." I said, "Oh yes," and he says, "Oh, are you nervous?" [laughs] You just go, "I know you mean well, but think about what you're saying before you say that to me. I'm a paid-for keynote here."

I'm often asked, do you get nervous? That's different than what he was saying. He was saying, I suppose that you are nervous because you're speaking in front of people. I said, "I'm not really nervous now." He said, "Oh, do you do many of these?" I suppose it's that whole thing of I don't expect them to know that, but I think people should be very careful about how they phrase things. I'm sure there's people who are on stage all the time who still get nervous. I'm not saying that it's a good thing or a bad thing, but the assumption that I would be because maybe I didn't speak in public, it was just a bit blind. I was saying it's just tone-deaf, really.

**Rihonna:** Definitely.

**Jenny:** Just to add, he didn't ask my colleague who was also speaking whether he was nervous.

**Rihonna:** Of course.

**Jenny:** Why would he be, right? It's well-meant, but it's also targeted, right? Am I nervous, but not my colleague who looks very senior, very executive level, which he is, but so am I. I'm CEO, right? It's that whole thing and I always wonder, don't be grumpy. Don't make an assumption that's what someone means. Try to educate as opposed to get grumpy. Most days I would go, I suppose you didn't mean to sound rude, but I do lots of these so no, I'm not, or even just not, but just answer nicely. I did just let him off because he meant well.

I do think that sometimes it's a teachable moment, [laughs] because for me, it doesn't bother me. It glances off me because I'm in a position now where I'm fortunate I can pick what jobs I do and who I speak to, but you've got to send the elevator down and it would say that that might really knock someone's confidence. If it was, let's say for example, a woman who was going to speak and she saw that she was asked these questions, but her male colleague was not, that might make someone feel less confident. I think it's important that we build everyone up and that we really try and be careful in what we say. That's most particularly on social media because there is a casualness about cruelty that really hurts people's feelings.

Again, some of us are more robust than others. I've had some, absolutely. I've done some social media stuff that has had millions of views, right? Not because of me, just because the platform. Some of the comments are just trolling about the way someone looks or that I should be in jail because of where I'm from and my job without-- They've never listened. These are people who don't obviously have the concentration to listen to the whole interview. [laughs] They just see [crosstalk]-

**Rihonna:** Oh my gosh.

**Jenny:** -burglar. It doesn't bother me one bit. In fact, I wouldn't even see them except that some of them are quite funny. They're unintentionally quite funny. My kids have showed me a few of them. Like one, I won't say, but stuff about my weight or whatever. One of them said-- See, this makes me laugh. Now, there might be people, obviously, you might wonder why I laugh at this, but I thought this was hysterical and it said, "She probably robs cake shops." I thought, oh, [laughs], do you know what I mean? Because I'm not slim or whatever but chubby. My son knew I'd laugh when he'd tell me, but I think there's a casualness to this.

**Rihonna:** Wow.

**Jenny:** I think that's, to me, it glances off me, I'm not that bothered. I've got colleagues, again, some of whom are authors as well, who it turns much darker. Much quicker. I'd guess it's about respect. As a woman and as someone who's got something of a platform, I sometimes choose to be grumpy about it. I wonder if I get

a clap back from a lot of the people listening to this that there's times when, actually, teachable moment.

**Rihonna:** Definitely. Thank you for going into that. People are far too comfortable on the internet. [laughs] I think that's the least I can say about that. I want to go back to it. Your new book, which is *People Hacker*, *Confessions of a Burglar for Hire*, is currently available for pre-order or is it out now?

**Jenny:** As I'm speaking to you, it was released just about a week ago in the UK and parts of Europe. I did not do those negotiations myself, obviously. I got representation and the publisher who are currently negotiating with more worldwide routes. The way it works in publishing, apparently, and some of you may know this, I didn't, is that you do home territory first. I think if I'd have been a known author, they might have gone global. Anyway, it's released in the UK. Before I was released, we went to number one in the chart on Amazon in several categories.

**Rihonna:** Wow.

**Jenny:** Actually, the highest I got, I think, in the Amazon top 100 was number, I think, I want to say 47, but it could have been 49, but I'm going to say 47.

**Rihonna:** Wow.

**Jenny:** Now, of course, it didn't stay there. It hovered in the foot in the top 100 for a couple of days, and now I'm still in the top 1,000. We did top categories. That was before we released. Then on the day of release, it got a little bit higher in most categories as well. On Audible, which I read myself, which I can tell you is a nightmare, just a horrible read in your own words, in your own voice for having to do all the intonations and things. I'm not an actor, so that was quite the thing.

The producer just saying, "Say that again." I'd say something like, "Walking down the staircase and go down the staircase, walking down the staircase and again, down the staircase." Just, oh my God, how actors do it, it's just, it drove me crazy. They're available now in the UK. What I'm hoping is that we'll quickly wrap up this negotiation state side so that we can get it out to America, because I have lots of people I've worked with. Hi, everyone, lots of people I've met. Hi, ACFE, who I know have messaged me and asked for, how do we get hold of this book? How do we get signed copies? We're hoping to get that done.

Essentially, it's a memoir. It starts in my childhood with some things that happened to me that were light-bulb moments in terms of my future career. I wanted to make it really easy to read. A lot of the reviews, a lot of the people who have contacted me are saying, I read it in a weekend. It's easy. It's something that I can race through. It's not boring about childhood. It's done in a series of episodes of different things that happened to me. Go and write off to almost the present day.

I basically chose about 15 different either incidents in childhood which were more or less social engineering break-ins, let's face it, all the way up to showing a range of

the jobs I do, everything from those that were very dangerous and that were at a very high level involving international criminals and things, which, of course, I can't name, to some of the capers that we did, which I know the ACFE members enjoyed a lot when I spoke about it in New York. Times when the jobs have gone wrong and there's been cats turning up on a job or I've fallen off the roof or we've met people.

Those are the stories. I thought that I picked some of the jobs I've done that make good stories. Then incorporated into that is a lot of descriptions and advice about security generally, about social engineering in particular, and the security industry, and also some of my thoughts on things like diversity in the security industry and what we can do to really change our thinking as technology progresses. I've tried to pack a lot into it so that you get good bang for your book, and let's hope that that's what happens.

I just want to say thanks a lot for having me on the show, and also, just to do a big wave in the show to all the lovely ACFE people that I met in New York. You guys were so friendly to me, made me so welcome. It's so nice to come back on and do the podcast for you today.

**Rihonna:** Well, thank you again, Jenny, for joining us today. I really appreciate you taking the time out of your day to chat with us.

**Jenny:** Thank you. That's such a kind thing to say. It's been my pleasure.

[music]

**Rihonna:** Thank you for listening. You can find this podcast along with all other episodes of *Fraud Talk* on acfe.com, Spotify, iTunes, or wherever you listen to your podcasts. This has been Rihonna Scoggins signing off.

[music]

**[00:51:50] [END OF AUDIO]**