Military OneSource Podcast — Online Scams

Episode transcript

Intro voiceover:

Welcome to the Military OneSource Podcast. Military OneSource is an official program of the Defense Department with tools, information and resources to help families navigate all aspects of military life. For more information, visit MilitaryOneSource.Mil.

[Bruce Moody]:

Welcome to the podcast. I'm Bruce Moody. We're welcoming Carol Kando-Pineda back to the podcast today. She is with the Federal Trade Commission in their division of Consumer and Business Education. We're going to talk about the current state of online scams. We had Carol on this podcast about a year ago to talk about online scams, and she's back with us today because technology continues to change. Looking at you, AI, and the cat and mouse game played by scammers continues. So if you think that these scams are just too obvious, the ones that you see in your inbox and you'll never get burned, I really encourage you to stick around and listen to our conversation. Carol, welcome to the podcast.

[Carol Kando-Pineda]:

Thanks so much, Bruce. I'm thrilled to be here.

[Bruce Moody]:

It's great to have you back. This is going to be a really interesting conversation, but first, what is the Federal Trade Commission and what is it that you do?

[Carol Kando-Pineda]:

Well, in a nutshell, the FTC is the Nation's Consumer Protection Agency. So we work to stop fraud, deception and unfair business practices. We do that in a number of ways, mostly through law enforcement cases, but also through education. These kinds of programs where we get out into the community and talk to people and tell them what we've learned in our investigations and what we're learning about fraud as it evolves. And then we also have a very strong network of partners like DOD, like CFPB, but like public libraries and other kinds of organizations like Legal Aid to reach as many people as possible in the community and to leverage how many consumers that we can get to.

[Bruce Moody]:

Okay. So what is the work that you do with the military community?

[Carol Kando-Pineda]:

So we've always had outreach to the military. We've always focused on trying to share with service members and their families and with veterans, all kinds of information about avoiding scams and making wise money decisions, other consumer protection issues. But about 10 years ago, we made it sort of a more formal collaboration through our military consumer initiative. And we developed that very closely with DOD's Office of Financial Readiness and with the CFPB and a variety of other military, federal and state partners.

[Bruce Moody]:

Good, people we all know. Now, the last time that we spoke, you were sharing the scams that the FTC saw trending during Covid. So bring us up to date. What's changed? What are you seeing now? What kind of reports are you getting? How much money has been lost?

[Carol Kando-Pineda]:

So as you know, scams do change over time. They evolve, they respond to the current landscape, whatever's happening in the world. And Covid scams are fading because the public health emergency is over. We're still seeing online shopping scams. Those spiked during Covid and they've never gone back down again. Probably a little bit less, but they're still out there. But last year in 2022, FTC got more than 2.4 million reports from consumers. So quite a bit. But here's the interesting thing. The number of reports actually has gone down from in 2022, but the amount of losses reported is way, way up. It's nearly $9 billion in losses to fraud in 2022. That's $2 billion more than what we saw in 2021. So the fraud numbers are, the losses are up.

[Bruce Moody]:

Okay. So the grab has gotten greater. Now, when we were discussing how to put together this episode, what to bring in, you mentioned the sort of merging of romance scams and investment scams. This is a very interesting blend. So how does the bringing together the romance scams and the investment scams work?

[Carol Kando-Pineda]:

Yeah, it is kind of a strange blend, isn't it? But it makes sense when you hear how it plays out. So just in general, there have been big losses with romance scams. In 2022, consumers reported to us that they lost $1.3 billion in romance scams. So a giant chunk of those overall losses came from romance scams. So the blending with investment scams is kind of a new twist. Your online love interest, and they may approach you not

just on a dating site, but on social media. They may try to slip into the DMs, approach you online somehow. That way they'll claim to be a successful cryptocurrency investor and they want to teach you how it's done. They may be checking out different social media posts that you've done to get a sense of whether you're in the market to date or in a relationship, or whether you're interested in investing or any of those things before they try to cultivate you.

And they'll spend some time trying to get to know you and to gain your trust. And then they'll say, look, if we're going to have a future, we need to start planning for our future together. We're going to get married. This is what we need to do. I'm going to teach you how this is done so that you can make some real money in cryptocurrency. But by that point, you may trust them. You may think that you're in some sort of a friendship or relationship with them. They may actually set up fake dashboards so that you send them a small amount of money and you can log in supposedly to this website and look around and see your money there, and maybe even pull a little bit of it out. And so people feel like, oh, this is legitimate. I can trust this person. And I've actually gotten on the site and I've tried to get my money out. So it's all okay.

But they've set all of that up just to trick you into feeling comfortable because once you actually send them a significant investment, once you send them the 10, 20, $30,000, they disappear. That website comes down, your money is gone, and you have no idea where it went. It's impossible to get back.

[Bruce Moody]:

Amazing. So that is the elaborate long con.

[Carol Kando-Pineda]:

Yeah. Yeah. A romance scam is kind of a long con because they will take the time to try to make you feel like they're getting to know you and to gain your trust.

[Bruce Moody]:

All right, another attempt, another approach would be maybe the simpler short term perhaps, and that would be text messages. So scammers are using text messages as a different way of trying to get your money. What do these texts look like? What are they trying to accomplish?

[Carol Kando-Pineda]:

Yeah, so you're exactly right on that. The appeal of text message scams to scammers is that it's quick. They're counting on the fact that something comes in and it's going to be irresistible. And they're hoping if they can get you excited or frightened or panicked about something, that you'll act on it immediately. And once you click that link, you're going to go to a fake website or you're going to get a phone call from a scammer, and that's when the scam takes off. So the top text message scams that we had seen in the

last few years, there's several of them, but I'm just going to focus on these top two. The one impersonating bank fraud alerts. So it looks like they're trying to warn you that somebody's taken money out of your account or this charge is against your account. Was this yours? Just to get you to click and say, no, this wasn't mine.

I didn't buy that. But if you click, you're going to get a phone call and they're going to pretend to be from the fraud department, but they're fake. And so you're going to probably think, oh, it's okay to share all kinds of information with them so that they can help straighten out your account. But really they're just taking money from whatever account number that you shared. The second text message scam involves fake package deliveries. So they pretend to be from the U.S. Postal Service, from FedEx, from UPS, they say there's a problem with a delivery. They link to a fake website and they tell you, share your credit card number or some other personal information so that you can get this straightened out or let them know that it's not actually yours or where it should be delivered to or whatever the story is. There's just some sort of a problem with the delivery.

And of course, who doesn't expect to get a delivery at some point during their week? Right? We're all doing online shopping and getting deliveries. So it's very likely that they may hit somebody that is expecting to get a package, and they may actually be concerned that there's a problem with it. And so they're going to try to click on that link or enter that information into a website, or they'll get a phone call and try to work things out with somebody. But it's a scammer.

[Bruce Moody]:

So a scammer is looking across the whole landscape of people and saying, somebody getting this text is wondering where their package is, and it's that meeting that person at that emotional moment, and that's what they're looking for.

[Carol Kando-Pineda]:

Right. And texts are very cheap and easy for the scammer to send. So if they send out millions, chances are they'll hit some subset of people that are going to respond to that text and that's where they make their money.

[Bruce Moody]:

So since we last spoke, AI has really jumped into the center of it all. So it's new to us, we're still trying to get our heads around what it all means and what it's going to do for us. Of course, the scammers are already active in this area. What is it that scammers are currently doing with AI?

[Carol Kando-Pineda]:

You're right. I think many of us have been sort of fascinated with developments with AI and watching how things are evolving. And to many of us, it's occurred to us how this

could be used in scams. And we've sort of been trying to see where it's popping up. The first instance that I've seen is involving voice cloning and using that in impersonation scams. So in particular, family emergency scams. So someone may get a phone call, and it may sound like that they have kidnapped a family member, and you need to pay a ransom to get your family member back. And in the background, you hear the voice of your family member and that it may sound very threatening or like they're being hurt or that they're pleading with you for help. And so you can imagine that would cause horrible panic and fear and dread, and that you need to do something immediately to figure out what the situation is and to stop it and to help your family member.

But that's all done through AI voice cloning. So the scammers can take a recording of you on social media, online someplace. They can take recordings of your voice, clone it through AI, and then make it appear that your loved one is saying anything that they want that person to say. So you can imagine the kind of havoc that reeks and how upset people would be and how you're much more willing to send somebody payment if you think it's going to make the problem go away. And so what we have told people is probably the most important thing to do is to get somebody else to help you try to contact that person or put that call on hold and try to contact the person yourself. If you're thinking clearly enough and you're able to do it, because chances are you'll be able to reach them and they'll say, I'm fine.

I'm okay. I'm at school, I'm at home or I'm at a relative's house. Don't worry about me. I'm okay. That's a scam. And then you can hang up on that other phone call. And I know that's asking a lot because if you're in a situation of super high emotion. But that's the whole point of knowing these warning signs, is knowing that if somebody is triggering you with that kind of emotion and they're asking you to pay in these particular ways, you want to take a step back and try to figure it out before you take any action.

[Bruce Moody]:

And that's really it. The trigger is the high emotion. So yes, AI is very sophisticated, but text messages are not. Romance is sophisticated in its own way, but really whether we're talking about the high-tech AI or low-tech text messages, these tactics are not especially high-tech. It's really getting us to make decisions based on our emotions. So talk about what is it that they're trying to achieve and how can somebody guard against this?

[Carol Kando-Pineda]:

You hit the nail on the head, Bruce, that the scammers are, they're very professional, they know what they're doing, they know how to target us, they know how to create those emotions. And some of these more high-tech methods are just ways for them to create those emotions and to create that urgency and to try to play it against you. And as I said, they want to knock you off balance just long enough. They only need you to be in that suspended state just long enough for you to share information with them or make arrangements to pay them. So that's what they're aiming for.

And the most important thing to remember, I think the biggest warning sign because when you're in that sort of a state, you need something like a big, bright red flag, something that you'll remember to help you slow down and stop and to think and get yourself back on balance. Pay attention to how they ask you to pay. So if you're in one of these situations and somebody is threatening you or pretending to help you, but they're asking you in this urgent situation to pay them using gift cards, a wire transfer, a mobile payment app, or cryptocurrency, it's probably a scam. And you definitely should slow down, take a breath, stop, think about it, maybe try to contact somebody to bounce it off of them, and that's probably what's going to help you to say no and avoid that scam.

[Bruce Moody]:

Such an interesting conversation. It never ceases to amaze me, but Carol, as you were discussing what the FTC does, you did mention that people contact the FTC to report having been scammed. So for those who have never done that before, if they find themselves in a situation and they want to report something, how do they do this?

[Carol Kando-Pineda]:

So consumers want to go to ReportFraud.ftc.gov, and that's true whether you've lost money to a scam or whether you've just encountered a scam. If you've seen a scam, we want to hear about it at ReportFraud.ftc.gov. So those complaints, those reports all go into a big database, and it helps us analyze the trends that we see and how scams are evolving and whether the volume of complaints is going up, whether the volume of losses is going up, the way the losses are happening. And it's a really helpful tool for our attorneys and investigators to build cases. We also share those reports with other law enforcement agencies so that they can build cases as well. So that even if FTC can't necessarily bring a particular kind of a case, maybe another enforcement agency is able to do that.

I do want to caution people that not to expect that they're going to get a case number and somebody following up with them. It's not that kind of a system, but it's still really critical for us to hear what people are seeing in the marketplace and to see the kinds of scams that they're seeing. Because that's our way to maybe help somebody else not lose money and to build cases so that we can get some money back to consumers.

[Bruce Moody]:

Carol, as we wrap up the conversation, I just welcome any final thoughts.

[Carol Kando-Pineda]:

So if people only remember one thing from our talk today, I would want it to be always pay attention to how somebody is asking you to pay. If they're asking you, if they're pressuring you, especially if there's an urgent situation and they want you to send them

money through a gift card, wire transfer, a payment app, or cryptocurrency, it's probably a scam.

[Bruce Moody]:

Perfect. We'll leave it at that. Carol Kando-Pineda, thank you for joining us. Carol is with the Federal Trade Commission. Great to have you with us.

[Carol Kando-Pineda]:

Thank you, Bruce.

[Bruce Moody]:

Absolutely. Want to remind everybody that military OneSource is an official resource of the Defense Department. We hope to hear from you. Click on the link in the program notes and send us a comment, a question, maybe a idea for a future episode, and be sure to subscribe to this podcast wherever you listen to your podcasts, because we cover a wide range of topics to help military families navigate military life. I'm Bruce Moody. Thanks so much for listening. Take care. Bye-bye.