ON-SCREEN TEXT: Protecting against COVID-19 related scams; Gary Owen, Head of Information Security, Wells Fargo, June 1, 2020

ON-SCREEN TEXT: Why is fraud protection particularly important now?

>> Owen: Yeah, fraud protection today is critically important. The criminals are under stress just like we are. So they're always looking for a way in. And that way in may be a weakness we have, a heartstring being pulled, or being in financial stress. So, always think about what the criminals' job is, which is to take money out of your and my wallet. In a crisis, things that are too good to be true are probably too good to be true.

ON-SCREEN TEXT: How can I be sure communication about my stimulus check is authentic?

>> Owen: With regard to stimulus checks, the government rarely, or I would say almost never communicates through email and never, that I've seen, through text message. If you ever get a message that feels a little awkward, or that are asking, or that they, the government, is asking you to authenticate, go back to the source. Go to a browser, www dot, and find your way to the legitimate source and validate there. The government doesn't urgently communicate with us. They don't do it through email, they don't do it through text message. So, if in doubt, go back to the source.

ON-SCREEN TEXT: What are some popular schemes right now?

>> Owen: Funny thing with the criminal element, the schemes don't really change. It picks the topic where people feel comfortable or want to provide either help in some way. So the Payment Protection Program is a big one, pandemic based charities is a big one, shipping scams. Anything that's too good to be true. And today, with so many people working from home, think about the online shopping experience that maybe many people haven't done before. Go to places you know. If there are $10 sunglasses that should be $200, it's probably too good to be true.

ON-SCREEN TEXT: What are some signs that an email is fraudulent?

>> Owen: There are a few ways to check if an email is fraudulent or real. Unfortunately, there's no rule of thumb. So, first and foremost, spelling, grammar. The companies you deal with, they're pretty good. They've got talented people writing these emails and writing information. Another thing to think about is really, use the five-second rule. Just take five seconds and look at the email and think to yourself does this make sense? Is it accurate? Is there personal information in it that only my company that I deal with would know. And as I said before, go to the source. Never trust that something is urgent and must be done today. Take five seconds, open a browser, type in the company you know and check.

ON-SCREEN TEXT: What are some signs of a text scam?

>> Owen: Yeah, so text is a newer communication medium for most companies. But always be wary of all caps, criticality in the text message, a link that you can't read. Rarely does your company communicate with you through text other than to notify you of something. It's really not meant to be that transactional. They're so short in terms of number of characters. So just be suspect and my two cents is always go back to the source and validate. Rarely is it urgent.

ON-SCREEN TEXT: I've seen social media posts with special loan offers. Can I trust them?

>> Owen: Criminals go to where the eyeballs are. So if there's a lot of people on social media, that's where some of the scams will come from. Don't trust what you see on social media and don't trust the news you hear about on one edge of the internet or another. Just always have your guard up. Always be a little suspect of what you're hearing. If it's too good to be true, it likely is too good to be true. And if there's some sense of urgency, there's probably a reason why they want you to respond quickly, and it's not to help you. Go back to the source.

ON-SCREEN TEXT: What about communications that say they're from the IRS or from my bank?

>> Owen: I suggest to people the five second rule. Take a look at that message, take a look at the context that it came to you in. Is it personalized? Is it really for you? Does that, the IRS, or any government agency communicate with you on a regular basis? And if not, think about it a little bit. Does it make sense? The IRS usually communicates by mail, not by text message or email. Always be suspect, and the same five second rule that says check the source.

ON-SCREEN TEXT: I run a small business. How can I protect it from fraud?

>> Owen: So for small businesses, you should really think about the adversary, the criminal trying to break their way into your bank, or into you within your account. Don't be cheap. Pay for antivirus. Sign up for all the pre-alerts, the two-step authentication. Reconcile your statements and transactions. Do it daily. If you're moving a decent amount of money around, you should be thoughtful about it. It's your money. Make sure that any transaction that occurs is legitimate.

ON-SCREEN TEXT: What should I do if I identify a fraudulent email, text, or other communication?

>> Owen: Yeah, if you identify an email or a text that's fraudulent, or even you think is fraudulent, forward that to the company that you believe it should have come from so that they can tell other clients about it and act against it. Often they have a website, report phish or report a text message, a way to forward these messages to them. And if you can't find that, the best thing you can do is just delete the message. Delete it and forget about it. It doesn't do you any good in your inbox and it doesn't do you any good in your text message phone, so just get rid of it.