Please note: This is an AI generated transcription - there may be slight grammatical errors, spelling errors and/or misinterpretation of words.

Protecting Your Family and Wealth From New Cybercrime Tactics (Webinar Recording)

Intro: Hello everyone, and welcome to today's webinar, Cybercrime Is Changing: Is Your Approach to Protecting Your Wealth Changing With It? I would now like to introduce Eddie Welsh, Managing Director and Head of Wealth Management at CAPTRUST. Eddie?

Eddie Welch: Thank you, Kara, and welcome everyone to our wealth webinar.

Today we're going to talk about cybersecurity, and I think we found a topic that everyone is interested in. This has been a well-registered webinar. I really think it's gonna be a very informative hour for you and our audience. I welcome today Mark Hurley. Mark is a longtime industry friend.

He won't say this, but he has been really a leading voice in our industry, the wealth management industry for Mark, at least two decades. I know maybe a little bit more. And his latest endeavor is digital privacy and protection. It's a cybersecurity protection agency that that CAPTRUST has partnered with, I guess maybe three or four years ago now.

And Mark is very informed in this area. A lot of interesting things I think we'll discuss. Looking forward to the questions at the the end of Mark's comments. And so yeah, Mark welcome my friend.

Mark Hurley: Thank you very much, Eddie. It's been great. I... You and I have known each other for forever.

I'm joined today also when we get to the question and answer session by my partner Carmen Chicalese. Carmen is one of the people who helped us design our service and set up our company. He's a senior partner. In earlier life, he ran the Army Cyber Warfare Strategy and ran the team that was responsible for using the internet to hunt down some of the worst people on the planet so the military could deal with them.

But he'll be around for this call. At the end he'll if we have any really technical questions that I can't handle, I'm sure I'll get him to step up and do that for us instead.

Eddie Welch: Outstanding. We're gonna talk about a lot of things today, and some of them are gonna be a little scary, quite frankly.

But we're g- we're gonna start at the end here, right Mark? R- really to say i- is it that hard to protect yourself when you're online, right?

Mark Hurley: Yeah, look, I know that when people think about this, it's, it can be scary and there's all kinds of various people out peddling stuff, et cetera, but it really isn't complicated to operate safely online.

You gotta do four things. Number one, if you have an account that matters it's gotta have a really good password, really long, really sophisticated, absolutely unique. Number two, all the consumer technology that you get today comes with a bunch of features that are not turned on that make it much safer to use, and you turn it on by putting on a bunch of settings.

They're on your devices, they're on your search engines, your browsers, and your apps. You turn these things on you geometrically lower your risk. And the only catch of course is you have to regularly update them 'cause they do change. The third thing everybody needs to do is they probably need some inexpensive, widely available cyber technology.

We'll talk some more about this later, but it's not hard to get. It doesn't cost very much. But the fourth thing that everybody needs to do is, and it's probably the most important thing in my view, is you gotta keep getting educated about this. I think this class provides a phenomenal baseline so you can think about this.

But if you look at this class today and the one we were doing a year ago, it's almost completely different because the bad guys are constantly innovating. The good guys create new ways to protect people, and the bad guys come up with ways to get around it. And the only way you stay, be able to protect yourself is to stay informed and know what's actually going on So we at CAPTRUST work really hard to protect our clients' assets protect our institution.

Eddie Welch: I actually just heard a presentation by John Meyer, our chief technology officer, to a group just last week actually. It was really impressive. We're doing a lot of things. And, perhaps if there's interest we'll have put together another webinar to talk about some of those things.

But, multi-factor, multi-factor authentication we do really a rigorous job On our vendors to be sure that they are coming in a protected mode. So a lot of really good stuff happening at the institutional level. John Meyer and Nick Brzezinski work really hard on this.

They have a, a, a significantly significant number of people that that, that work on that team. More on that maybe somewhere down the road. We wanna talk about today our audience and specifically how they can protect themselves. You've talked about cybersecurity but you've also said, Mark, cyber privacy is really important, and we're all probably going to get breached at some point in time, right?

Mark Hurley: Yeah, that's absolutely right, K- Eddie. Everybody thinks about being safe online. They focus on the stuff they see online about, various either technologies or passwords and things like that, and those are all important, but the reality is it's a bit more complicated problem. It's a two-dimensional problem.

You have to worry about both your cybersecurity and your cyber privacy, and if you don't protect your cyber privacy, you will not have cybersecurity. Now, when we talk about cyber privacy, we're not talking about your Social Security number, your birthday, your email or address. All that stuff's online. The government lost a bunch of records.

One of the big credit bureaus lost a bunch of records. What you're worried about here is that modern consumer technology is set up in a way so that the companies that provided the technology can collect your information on an ongoing basis. And unless you take a bunch of steps that we'll talk about today you're literally broadcasting what you're doing second by second to tech companies, and really bad guys have found ways to get to that information.

And what they do is they design attacks that get around your protections on your cybersecurity. In fact, where we've seen substantial amounts of money stolen, that's what they've done. Y- you have to think of this as you either have both cybersecurity and cyber privacy, or you're not gonna have either.

The other thing to keep in mind is that if you are connected to the internet, at some point you will get breached. Everybody gets breached the FBI, DOD, CIA. The, the objective of cybersecurity is to minimize how often that happens, but more importantly, make it so that even if they do breach you, it's still really hard for them to steal something from them.

And keep in mind, these, these criminals, they have ... they're businesses, criminal enterprises, but th- they have limited resources, and so they hit most people with automated attacks two, three times. They don't get what they want to, they gotta make a decision whether they wanna invest a lot of time and resources to go after you, and for most people, it's just not worth their time.

It's just a negative expected value to do that a- and particularly 'cause most other people don't do anything. So if you just do the basics and take care of it very hard for the bad guys to get to you.

Eddie Welch: We wanna protect everything that we do online, right? Chief among that is our assets, our money.

W- where are the members of this audience probably most at risk?

Mark Hurley: Yeah, we... Our, our company has never had a client get breached, lose money in five years that we've been doing this. Always say touch wood. The But we help as a rule, we'll help anybody who's breached pro bono. We've helped many CAPTRUST families who've actually come to us looking for help after they've been attacked.

And the thing that all they're all stunned to learn is that if somebody gets into their bank account or their custodial account, it's really unlikely that they're gonna get the money back. And we're not trying to scare anybody here, 'cause let's understand, the banks and the custodians, they spend a king's ransom on cybersecurity.

But they lose lots of money every year because most people are acting like it's 1990 as opposed to 2026 on a personal basis when they're online. And I know someone will say, "Wait, my bank has Federal Deposit Insurance." Understand that is there only in case the bank fails. It's not if someone gets into your account.

It's your online account agreement. And your online account agreements for both banks and custodians protect banks and custodians. Example, we had a very prominent physician show up on our doorstep last summer who lost 400,000 out of a Bank of America account 'cause he didn't protect his password, and BOA told him to go pound sand.

We had a family that lost 375,000 out of a Chase account, exact same thing. They came to us saying, "What do I do?" You're not getting the money back. Look it's important to understand that you have some real risk here, and that it's

really important when you take the steps that we're gonna talk about today, because if this money gets stolen, you're probably not gonna get it back.

Eddie Welch: So I know we're gonna talk about some really sophisticated tactics that cyber criminals are using these days. But f- just from a really basic cybersecurity standpoint, what are maybe a couple of examples of how people have made it easy to get breached?

Mark Hurley: Yeah. It's just really important.

People, we as a country are self-unaware when it ... of some of the stuff we're doing and why it's got a lot of risk. That's why some people when we do this class get frightened, 'cause they realize they're doing foolish things. For example, public Wi-Fi i- if anyone on this call has ever done much in technology, they would tell you that they could, if they're on a network, they can go and look inside anyone else's device that's on the same network.

And it's not that complicated. And so there are people who sit all day on public networks at public Wi-Fi at hotels, coffee shops, and they look like they're banging away on the computer, sipping coffee, and what they're doing is they're copying passwords and selling them. There's actually a multi-billion dollar business doing this.

Now, the way you prevent this is they're, A, don't do something that you would care about a third party seeing, or B, you get a piece of software, it's called a virtual private network, or VPN we'll talk more about this later and it encrypts your online traffic. But i- with what they say just 'cause you're paranoid doesn't mean they're not out to get you.

Honest to goodness, there's somebody watching when you're online. The other thing to keep in mind is that public charging stations are really convenient. When I travel a fair amount, you take your device and I'm not talking about the regular p- power cord, the one that goes into the side of the device, the USB, USC charger.

They're in rental cars, they're in back of an airline seat. You'll see some of these in hotel ala- rooms they'll have these. If you plug your device into one of those things and you don't protect yourself, there's a really high likelihood two bad things are gonna happen. Number one, your information will get downloaded, and criminals know how to grab that and sell it, but even worse, you'll probably get infected with a computer virus.

The FBI has an alert out about this. The Army Cyber Command has an alert out about this. Forbes even did a story where they showed where someone could take an entire one of these giant public charging stations, and for seven bucks rig it so they would infect every device and download all the information from it, from every, any device that's connected to it.

All right. That's the bad news. The good news, it's not hard to protect yourself. There's a thing called a USB or a USC blocker. It's about this big. You can buy them at Amazon, Target, Walmart. They cost three bucks. We don't recommend using the Chinese versions because there's been a whole series of counterfeits made by Chinese

Eddie Welch: gangs.

Good point.

Mark Hurley: You wanna use the one out of Britain, which is called the PortaPow. P-O-R-T-A-P-O-W. That's the one I use. I carry a bag of 10 of these wherever I travel, and you put this in, you put your cord in the back, and the only thing that comes in is electricity. Now, understand though, if you do it just one time without this, it's a really high likelihood you're gonna get infected.

You ... Again, this is one of those things where you've gotta be very self-aware of what you're doing so you don't make it easy for the bad guys. Yeah, Mark, I, I travel a lot as well, and I've, I see people plugging them into the back of- the seat on the airplanes in the airports, there's, there's power stations and they're plugging directly in.

Eddie Welch: It makes me crazy. I wanna run up to them and say, "Please don't do that." But yes, absolutely happens all the time. And who knew, right? I didn't realize this until, we started working together- Yeah ... two or three years ago. By the way, I didn't say at the top that I'm, I am a client of Digital Privacy and Protection as well, and have been for about three years or so.

All right, so we've established cyber privacy is in many ways more important than cybersecurity. Why are so many people at risk of-

Mark Hurley: Yeah. Great, great- ... of cyber crime? Great question. Look, tech companies have figured out much more money collecting user information than there is in selling technology.

So even if they sell you the technology, a big part of what they've done is set it up so that you on a, a default basis are broadcasting tons of info. Like for example, Amazon, they make more money selling customer info than they do selling customers products. Meta, which I'm sure you're familiar with, Facebook, Instagram that, that company makes 60 billion a year collecting and selling info.

So all these guys have set up the technology so you're just pumping information out second by second, literally what you're doing minute by minute. The bad news is criminals have figured out how to access that information, and it isn't just guys offshore anymore. These are local guys with guns. Now, these companies don't want to get sued, so they give you the ability to opt out, but they make it a bit challenging.

They make you turn on a bunch of settings that are on your devices, your search engines, your browsers, and your apps. The- most families, it's about 900 settings in total that we find. And and then the companies, they make so much money, they don't like it when you turn these on, so they change them.

So you have to learn these settings, get very familiar with them, and about every four months go back in and update them but if you don't do this, the risk, particularly in the last 18 months we've seen, have gone from being just somebody offshore trying to steal money from you to really local bad guys.

Couple examples. There's a report out from the beginning of this year that said there were about 900,000 burglaries nationally, and they estimated that 80% of the time, that's eight zero percent of the time, the burglars were using the improperly protected social media accounts of their targets. 'Cause you have social media, there's location tracking software built into it. And if you know what you're doing, you can figure out where the person is if the person hasn't protected it. The one that the FBI will talk to you about, the really dark, scary one, is the predators. There are some horribly bad people that go into parents' and grandparents' online accounts.

They collect a lot of information about kids, and then they, and they profile them, and then they connect with the kid in one of these anonymous online chat rooms, and the kid thinks they've met their soulmate 'cause this person just seems to know what's going on in their life and how they feel, and they get the kid to trust them, and you can imagine what happens.

This is the really scary side, and what we deal with every day in our business. This is much more than just protecting your money. This is also, quite candidly- Yeah ... protecting your family's safety.

Eddie Welch: Yeah, absolutely. So artificial intelligence I'm betting a few people have heard of that recently.

It's it's everywhere, and it is, as the slide said it has changed everything, including how bad guys are using it to target families. Talk about- Yeah ... some of that.

Mark Hurley: Yeah, every single at- We're helping three to four families a day who aren't clients, but are coming to us looking for help.

And I would say in every single attack we have seen in the last year, it's, AI's been used in some form. One example is that involves passwords. For example, if, every time there's a corporate data breach, many of you may remember that AT&T had a really big one last year. Uber has a lot of these. The bad guys have set their computers up with AI, and they go in and grab all the compromised information: names, user IDs, passwords any personal information they can. They throw them into very sophisticated computer algorithms, and they create thousands of variants of passwords, and then they try to guess passwords.

And they are successful a million times a week. And they want to get into your financial accounts, but if they can get into your cell phone account or your telecom account or into your email account, they can get around the protections on your financial accounts. And quite candidly, if you were ever gonna be a cyber criminal, this is the time to do it.

Because as I said, our country's back at 1990, particularly when it comes to passwords. Now, this is a report done, a chart taken from a report done by a company called Hive. They're a big-time consulting firm in the cyberspace, and they do simulations where they try to figure out how quickly they can guess a password using a computer.

And for the first time ever, about three years ago, they decided to try AI. And what they found was that they could now correctly guess any eight-digit alphanumeric password, that's uppercase, lowercase, numbers, and symbols, in less than one second. And now processing power has sped up, so it's probably a 10-digit one.

Look, if you're just gonna use eight, nine, 10 digits, just use password. The bad guys are gonna waltz in. The way you protect yourself is you have to use a password that's much more sophisticated. It's gotta be really long, about 20 to 25 digits. Gotta be randomly generated, it's gotta be alphanumeric, and it has to be completely unique.

It can't be similar to any other password. Otherwise, as I say, just use password because they're gonna waltz right in. They do it every day.

Eddie Welch: And audience, we're gonna talk a lot about how to circumvent a lot of this a- as we get in. As I said, we're maybe gonna share some things that are a little unsettling, but but there's a, there's an answer.

Not fo- nothing's foolproof, right? But there is an answer and a way to help mitigate a lot of these risks. So s- seeing, hearing a lot about cyber criminals using AI to clone images and voices that one is really particularly unsettling to me. Talk about that a little bit.

Mark Hurley: Yeah. About 18 months ago, this would've been kind of a novel new technology, now it's generic.

What the bad guys do is they ta- download a video from somebody. With AI software, it's really easy for them to clone their voice and their image. There's even a YouTube video that will show you to create one for a Zoom call, and I would challenge you to tell you that your mother could not tell the difference between that avatar and you.

That's how accurate- Wow ... these things are. This is for $4.95 you can clone somebody's voice and it'll defeat voice recognition software. We were approached by a couple families who got attacked this way. One involved a a family that was using voice recognition on their custodial account, and they didn't protect their cyber privacy.

Someone cloned their voice, bye-bye $2 million. We had another lady whose daughter, and she's an older woman with a grown daughter, who didn't protect her cyber privacy, and this allowed the bad guys to use the location tracking software to figure out where she was and couldn't be reached, as well as to clone her voice.

And as we'll talk about in a minute, she didn't protect her cell phone either. So what the bad guys did is they went in, diverted her cell phone, and they cloned

her voice. They then texted the mother and said, "We've got your daughter. We're about to take her to Mexico unless you wire us 200,000 in crypto."

The mother obviously freaked out, picked the phone up, tried to call her daughter. The cell signal was diverted. Bad guys picked up and they had a cloned voice of the daughter calling for help. So with the criminals on the line, she went to the bank. The bank refused to wire the money. They sent her to another branch, and then they wired the money, okay?

This is not theoretical. It's not hypothetical. This is every single day in the world that we operate in right now. You really, quite candidly, you don't know who's on the other end of the phone or even on the other end of a Zoom call anymore.

Eddie Welch: Yeah, that that's not fun to think about at all. So spinning up websites is pretty easy now and you could do that easily with AI.

What are some of the ramifications of that?

Mark Hurley: Yeah. What the bad guys have figured out is ways to create fake websites and put them in front of legitimate websites, and the reason they wanna do this is they'll also put an app up on the site hoping you'll download it, and the app is packed full of computer viruses.

Really common with crypto sites. We're starting to see it with other sites. Okay? Look, a blanket rule for you, you never download an app except from the Apple Store or the Google Play site.

Eddie Welch: Sure.

Mark Hurley: Candidly, you just don't know what else you're looking at when you're doing this

Eddie Welch: So you, you've mentioned profiling potential victims.

Maybe a little more specifically how that works. Yeah. This is the one area that really has caught our attention, okay? And these are very sophisticated criminals 'cause they study cognitive psychology. For those of you who don't have any experience in that area cognitive psychology is looks at how the brain actually makes decisions, and if anyone's ever studied that, we have a bunch of shortcuts that help us make quicker decisions.

Mark Hurley: They're hardwired into our brain. They come back from when we were cavemen so the lion wouldn't eat us. We could make a quicker decision. And one of those is that we actually don't take information in on an arm's length basis, analyze it. The reality, if someone approaches you with new information, you're gonna take that information and compare it with reference points that you've accumulated over many years.

And the criminals have figured out that if the information you get is consistent with those reference points- ... you're almost hardwired to believe all the other information. And so the most common attacks that we're seeing where they steal lots of money, they've actually profiled the client, and what they've figured out is what these assumptions are, so the client, or the victim, quite candidly, has a very hard time not believing what they're telling is true.

Eddie Welch: And I know you have some real-life examples of this as well, right?

Mark Hurley: Yeah. One involved one of the most sophisticated women you'd ever meet. So this isn't just some little old lady who's over her head on the internet. Very active politically, very successful, did not protect her cyber privacy- and this allowed the bad guys to profile her. And as part of that, they ... and she was a Democrat, very active in the last election cycle doing a bunch of stuff. So they were able to target her and send her a calendar invite for a political event that sh- they knew she might be interested in. She clicked on it.

She got a piece of malware on her device called a RAT, which we'll talk more about, but it allowed the bad guys to read her emails, her text messages in real time, and they could see everything she was discussing, what she was worried about, what she was thinking about- ... and they were able to profile her very effectively.

And so they waited until right after the election, and right after that, they contact her, and they posed as a Treasury official and an FTC official, and they had the right name, the right email, the right phone number. It was the right position. It was like if these were the people who would be contacting you.

And they said to her, "Look, we're really concerned because we've been alerted by the Secret Service that some of your accounts, unknowing to you, have been used for money laundering, and that while we know you're not a crook, we're very concerned that the next administration, out of spite, will put you in jail."

Now, all this is baloney, but this comported with her assumptions, and they knew she was all terrified about a bunch of stuff like this. And so they said, "But don't worry, we're gonna help protect you, and we will get with you and take steps that will protect you." And then over an attack that took- About three months.

They proceeded to convince her to give access to her certain accounts to the government, and they stole $6 million. That's- And these were guys offshore. They met with her on the Cape, and they met with her in Breckenridge. Okay? Now, let's understand, this is a very sophisticated woman. This is not someone who could be easily fooled.

And and when the attack was over, and that's when we get asked to help, she came to us and she said to me, "How did y- how did I ever fall for this?" And I explained cognitive psychology and, how they know the brain works, and she said, "It's funny you say that. Throughout the entire time this was going on, I kept saying to myself, something doesn't seem right here, but it was like I had to believe that it was true."

And that's what they're taking advantage of, okay? You've gotta be careful. If you don't protect your cyber privacy, it makes it easy for them to create an attack like this and come after you.

Eddie Welch: That's a chilling example. A lot of these attacks are getting more personal and aggressive and- As you've told me it's really no longer just, and as you said a moment ago, just people offshore.

These are, this is happening locally. Local criminals are using cyber tactics, right? And getting super aggressive around this.

Mark Hurley: Yeah.

Eddie Welch: Talk about that. Yeah,

Mark Hurley: we've talked about, there used to be the famous Nigerian prince. "Send me $5,000 and we'll give you a million dollars when I get my inheritance."

Okay. All right, th- this has gone way away from that. The bad guys are much more aggressive. I don't have a slide on this, but one of the things I wanna warn everybody listening here, if you do crypto, never tell anybody about it o- about

it online, okay? And the reason is that there's been a wave of home invasions both in Europe and the United States because crypto is a fungible asset.

And so if you have a wallet, a crypto wallet, with say 25,000 in it, that's like having $25,000 in $100 bills inside your house. And there's been a whole series of attacks where people have gone into people's houses, put a gun to their head, made them wire the money out, and it is utterly untraceable. But on top of that, we're seeing now that the bad guys know that because the technology you get is set up to export your info, a byproduct of that is every device when you first get it is set up to automatically record all of your user IDs and passwords in multiple places.

Now, you can prevent this by turning on these settings that we talked about, but if you don't and somebody gets onto the device, like with a virus, they got everything. They're off to the races. More commonly we're seeing now, and there's an FBI alert out on this, there are people who work bars and restaurants.

They're called shoulder surfing gangs. There was a gang that was recently arrested, it was stealing over 50 grand an hour, and what they do is they wait for you to open your device, so they look over your shoulder while you're doing it and see you put the passcode in, and then they distract you and get the device, and they have your communications ability and they have all your passwords.

And we've seen people have their accounts cleaned out in 30 minutes. An advisor on the West Coast had a client who came out of a restaurant, opened up their device, and someone mugged them, stole $300,000. Now, if that isn't enough cheery news for everybody here, and this is why these settings are so important, if you don't turn the settings on, there's another group of people that take advantage of this, and I call them the the dark side of the Force, which is Google, Facebook, and Apple.

They actually collect all your passwords, and they had a big data breach last summer. You can look this up. It was in Wired, it's in Forbes, Cybernews. And what happened is a bunch of their vendors got breached, and they now estimate there's approximately 16 to 19 billion user IDs and passwords sitting online.

So if you haven't turned these settings on and you haven't changed your passwords in a while, you probably wanna do that. But a quick example of where all this has been used in the attacks we've seen involved a lady who came to us who lost $400,000. And what happened was is the bad guys went in there, they grabbed her email password, they went into her email account, they

changed the settings so that any notifications from the bank or the custodian were automatically forwarded away.

They then went to her cellphone account, clicked on the forgot password link, changed the password, and then, and with that, then they could divert her cell signal. They then went to her custodial account, they clicked on the forgot password link, reset the password. They then put the new password in, and when the code, the multi-factor code came back- they went into the cellphone, they intercepted it. Bye-bye $400,000. This isn't theoretical. This is every day. That's why when we talk about settings I can't overstate how important it is to do this.

Eddie Welch: Wow. So a new term I learned vishing. Not phishing, but vishing with a V. This was new for me.

Talk about how this works.

Mark Hurley: Yeah. Vishing is a term. It was ... It's called voice phishing. And what's ... that's gonna happen is someone will call you. They're gonna pose as your bank, your custodian. We've even seen this pose as an advisor with a cloned voice and a spoofed caller ID. In other words, it's not hard for me to send you a call, make a call you, and have someone else's number show up on your phone.

And we've seen them pose as Microsoft, Apple, increasingly Google IT help. And what they're gonna do is try to convince you that one of your bank accounts or one of your custodian accounts is at risk, and you've gotta take steps immediately to protect yourself. Now, if they're ... If you get this call and you open the account, the money is gone.

Bye-bye. We saw a family recently lose 3 million in one of these attacks, okay? What ... How do you protect yourself here? What you start with is you have to understand there is not a bank or custodian on the planet that's ever gonna call you. Google, Facebook, Apple, those guys don't care about you.

Who are we kidding? Microsoft, they're never gonna call you. All right? And the, it's a scam. Y- it's always a scam. So the hard and fast rule is you never ever open a financial account when somebody calls you. If you have any doubts about this and you really think there's a risk, get your advisor.

Your advisor will call us. We're happy to take a look at it. But never open the account, 'cause the money will be gone. This business is a $40 billion theft

business every year, and these attacks are growing 400% a year. So someone on this call is gonna get one of these attacks. It's almost certain that's gonna occur.

Eddie Welch: Yeah. A- again, super unsettling. So communications is the next section we're gonna talk about. And, I think we almost communicate digitally now more than we communicate verbally with one another, certainly with our financial institutions. We're we're wiring money back and forth.

And there are, yeah, I- I did it this morning. I look at my bank account, I get sent a code on my phone, I enter that code. Yeah. Criminals are learning, unfortunately learning how to get in the middle of this communication from what I understand from you. Talk about this, how they do it- Yeah

and we should be thinking about it.

Mark Hurley: This has gotten, this has really exploded because you think about when we protect money. First there's passwords, then there's information, and then it's communications. And so the criminals are now targeting communications. The most common way we've seen involves diverting cell phones.

If you don't protect your cell phone account, they will go in and actually s- change where the signal is sent, as I mentioned in that kidnapping attempt. Additionally, when Comcast got breached last year, we had a bunch of people come to us who'd been breached, and what we figured out was is that the criminals had not just stolen information from Comcast, they actually had a list of people whose cell phones they wanted to divert.

So the way you protect yourself here is use a really good password, but also put a pin on your cell phone account. The other way we're seeing is there's been this new type of computer virus that is geometrically more sophisticated than we saw just a year ago. It's called a RAT, remote access technology malware.

If they get one of these onto your device, they can take real time information off your device. They can listen to your conversations, they can turn on your camera, they can read your emails, your text messages. And the only thing that's changed from this, which we saw a wave of these, is just in the last 10 weeks we've seen in a wave of attacks another way of doing the same thing involving legitimate apps.

If anybody works for a company that has remote workers, they're gonna have a some sort of app they put on your device so that the IT department can come in

and do the work they have to do for the technology. What the criminals are doing is they're getting these legitimate apps and planting them on people's devices in really sneaky places like browser extensions and things like that.

I would say about 75% of the attacks we've seen in the last, oh 10 weeks, we found one of these things sitting on there. And again, if you get one of these things on your device, y- it's as if they have the device. We were helping someone remediate a breach, and they actually took control of the device in the middle of the appointment, so they had to turn it off so we could go get it wiped and get the thing off the device so we could actually stop the, to help remediate the breach in the first place.

That's how powerful this stuff is.

Eddie Welch: So what, what does this all, all this mean, Mark? How are we-

Mark Hurley: Yeah ...

Eddie Welch: what does this mean for protecting money?

Mark Hurley: If you take anything away from this class today, what I would encourage you to think is that nobody knows who they're talking to. I can clone your voice, I can spoof a caller ID, I can intercept your communications.

And if you're ever gonna move a material amount of money, my advice would be, a- and CAPTRUST didn't tell me to say this, is have your advisor put it in your bank account. They got an ACH. It's an automatic direct link. It ain't getting breached. And then go get hand-delivered wiring instructions, and go to the bank and wire the money yourself.

Anything else, you're throwing the dice, okay? And this is a daily event, when someone comes to us who's tried to move money, and hundreds of thousands, millions of dollars have been stolen 'cause they didn't do this

Eddie Welch: other maybe recent examples of this, yeah ... to drive this point home, 'cause it, this is a really important point, and it's something we're taking very seriously as well.

Mark Hurley: Yeah. Involved a family was buying a vacation home. Unfortunately, two years earlier they had been breached. They clicked on a calendar invite that shouldn't have, had a virus in it. They got malware onto their device. They, the bad guys got into their email account. When they got

into the email account, they also sent more emails that they got the person to click on, and by the time the, they got attacked, there were 42 pieces of malware on their device.

In other words, they had been breached for two years, their device was massively infected, they had no idea at all, 'cause you, really hard to detect this unless you know what you're doing. And so what the bad guys did is they set up their computers to read their emails, and they just sat and waited, and this is very common.

Most people, we see they're breached, are breached for at least two months, oftentimes for years before anyone steals anything. And they saw that this home purchase was coming up, so they sat back and they waited, and they watched the whole discussions on where the money was gonna move and how was it gonna move, and then they got n- they could see in the emails that the title company was gonna send the wiring instructions to the family so they could wire the money.

And what they did is they went into the email account and forwarded away the title instructions, away from the family to themselves, and then immediately changed them and sent them back. And so the victim had no idea that was going on. It looked like it came from the title company, but the wiring instructions were bogus.

They took the wiring instructions, wired the money, and they effectively wired it offshore. And I always get asked at this point why didn't they call?" W- we figured also they were on their phones, so they probably would've just- ... intercepted the call. This is why you can't trust anything electronic anymore.

Nobody knows who they're communicating with anymore.

Eddie Welch: Yeah. I've heard dozens of those stories as well. We're working hard to come up with new ways to protect ourselves. The cyber criminals are coming up with new ways to get around it. I, I know you had a couple of examples ar- around that as well.

Mark Hurley: Yeah. Understand, too, that it isn't just, this gives you a sense how fast the whole game is changing and why it's so important to all the things we talk about here. A really common attack now is they're finding ways to manipulate asset values to steal money without actually having to move money.

And we've seen about nine of these attacks that have come to us looking for help. The first one involved a, a lady in Chicago. She got a text message what looked like it came from Fidelity. Very, they spoofed the caller ID, looked like any other text message. She clicked on it. Unfortunately, it had a virus on it, a RAT.

And with the RAT, and she had not turned her settings on her devices. So with the RAT, they went into her Chrome browser and they stole 19 passwords, including her password for her Fidelity account. Now but before going into the Fidelity account, they went offshore and they bought up a bunch of penny stocks.

Now anybody who's seen The Wolf of Wall Street, you know these things are very illiquid. You buy a little, the price goes up. Sell a little, the price goes down. And they loaded the boat with these stocks, mostly biotech stocks. And then what they did is they went into her account and they used the password to get into the account and then the RAT to intercept the multi-factor code, and they took every dollar they could find in the account, including the trust linked to it, and bought up the same penny stocks.

And then a second later, they dumped them in the offshore account. In other words, at the moment that the victim was being notified something was going on in her account, they were gone. The money is gone. Okay? Guy- they're watching us. They're studying this. This is why I talk about education. You gotta understand.

You gotta take the steps we're talking about, and a really critical one is to stay current on this, 'cause they're very clever. They're finding ways to get around all our protections

Eddie Welch: I often wonder if these people would just use all this ingenuity to do good where the world might be. But, Yeah, yes

that's a contradiction. All right, let's get really specific about the how people can can protect themselves. Give us, give us-

Mark Hurley: yeah. And we've already talked about it. It's really easy to do. All the steps that we talk about combined or the people in this profession call basic cyber hygiene.

These are table stakes. You want to operate safely online, you gotta take all of these steps. You can't skip any of them, 'cause it's like building a fort and

forgetting one of the walls. But if you take them, extremely hard for the bad guys to get to you. As I've said, we worked with families for five years, we've never had a client get breached and lose money.

What are they? All right, number one, if you're gonna have an account that matters or home Wi-Fi or something connected to the home Wi-Fi, you gotta use a good password. Gotta be 20, 25 digits, it's gotta be randomly generated, it's gotta be alphanumeric. There's really not- All right.

Eddie Welch: So let me inter- interject in there.

You're talking about like a Wi-Fi password as well?

Mark Hurley: Yes.

Eddie Welch: Okay.

Mark Hurley: Yes. I've seen many dr- breaches where they came in through the home Wi-Fi where they had the pet's name on the Wi-Fi and- No ... nobody will ever know that. Yes, they will. I assure you they will. The other thing is, we talked about devices.

Look, I just taught a 16-year-old how to drive, which I can assure everybody is a religious experience. ... Before she could drive, she had to do a bunch of classroom training, and she had to learn, all the settings on the car, the windshield wipers, all, all this kind of stuff. Okay. Being on the internet is as dangerous as driving a car.

There are about 60 settings on an Apple device. There's about 120 settings on a Windows or Android device you have to learn, turn on, and then regularly update or it's not safe to use. Now, the hard part about this hard process are apps. Okay? Everybody likes to use lots and lots of apps. This is insanity if you think about it.

This device here, this connects to everyone I love and my entire net worth. You better believe I am really careful about what I put on this device, and we've gotta get to that mentality that we don't wanna use apps unless we absolutely know what they are and really need them, and we only get them, as I said, from the Apple Store or the Google Play site.

But they all come with settings, and you have to go through and learn the settings. The problem is the stuff that's really great has lots and lots of settings.

TikTok has a ad out right now about the new safe TikTok, 50 settings, 50 safety settings. It means if you don't turn all 50 settings on, it is not safe to use.

Okay? And remember, they change these settings regularly. Now, to do all this, as I mentioned before, you'll need some widely available and inexpensive cyber technology. One is a password manager. Look, if anybody here can remember 60 or 70 25-digit alphanumeric passwords, call me, we'll go to Vegas.

We'll make some money. But for the rest of us, you need software. We recommend a company called Keeper. We use it for all of our clients. We just set up a 96-year-old. These things are really easy to use. You get all your accounts in there, you alphabetize them, you put in all the links. Y- Once you get one of these things, you never not wanna have it.

You need a piece of software to encrypt your online traffic if you're ever gonna do something on a public Wi-Fi that you're worried about somebody seeing. We recommend a company called Surfshark. It's military grade. Again, don't have it on unless you really need it. And then lastly, you gotta have a pay-for email that's used just for one purpose, and it's called account recovery.

We talked about that lady who lost the $400,000. The way they're, reason they were able to change her passwords was they got into her regular email account. And the way you prevent that is all of your critical accounts will allow you to put in a different email for what's called account recovery.

That's what you use this email for. You don't wanna use a free one 'cause they can find it with AI, and you set it up so the only way to get to it is through the password manager. Now, keep in mind, everything we're talking about here, though, is not a solution. This is a process. You get new devices, you get new apps, you might lose a device, and your settings are changing, so every four months you gotta sit down and go back and update your pr- protection.

But look, think about this. You have an automobile. If you don't change the oil, I can assure you, your engine at some point is going to blow up. Okay? We just have to realize this is the world we're in now, and these are the steps that we need to take to protect ourselves

Eddie Welch: All right we're gonna go to questions in just a moment here, and we have well over 100 already.

There's no way we'll get to all of it, but we'll talk about that in just a moment. Any sort of last thoughts, other other things people might wanna do to consider protecting themselves?

Mark Hurley: Yeah, look, there are these services that monitor the dark web. You don't care about your, as I said, any personal info.

What you wanna worry about is someone selling a password. There's an aftermarket that you can look for. It's a backup alert. Y- we get to that point, you probably lost money. Title fraud is something that we help clients with. It's really important that everybody can do themselves. Criminals have figured out that counties they don't have the staff to closely scrutinize filings.

So what criminals will do is they'll make a bogus filing claiming they bought somebody's house, and if the documents look in order, the, the assessor will just change the ti- the deed, and then the criminal will borrow money against it, rent it out, or even sell it. We've seen this happen 12,000 times a year nationally.

The way you stop that is you go in and sign up for a notification if someone makes a filing, and you call them right away and say, "Stop." And most counties will do this for you. And then lastly, look, if you're breached, you've been breached for a long time. These guys are organized, systematic. If you think you got a problem, get with your advisor, get ahold of us.

I'll... We get, we'll get someone on that day onto your device, okay? We don't charge for this. We do it pro bono. But understand that the people who wait are the ones who really lose most of the money

Eddie Welch: Wow, that was a lot. So one takeaway I have is there's some simple tools you can put in place that, can really mitigate a lot of this.

And then secondly, be smart, be vigilant and consistently Change your oil, a- as you said.

Mark Hurley: Yeah.

Eddie Welch: Good stuff. Hey, we've got about s- 20 minutes maybe left, and I know there are literally 150 questions or more.

Mark Hurley: A- and we'll, we will give written responses to any that we do not get time to get to today, as well as the ones that were submitted in advance.

Just

Eddie Welch: so- Yeah, so just for the audience that we had plenty of, many questions submitted in advance. We'll pro- as Mark said, we'll try to, we'll provide written responses to those. The ones that have come in, we'll Mark and team will answer those as well and we'll get those back out.

This is, one question that was asked is this is being recorded. It is. I think Kara mentioned that at the outset. All right. So do identity protection services work?

Mark Hurley: Yeah. If anybody is on this call and uses identity protection services, don't waste your money. Okay? Look, identity protection services...

First, identity theft is not a material threat to your wealth. If someone steals your identity, it's useless to your credit. And by federal statute, the lender is on the hook, not you. And what I dislike about identity protection services is they are pregnancy tests when everybody, when it comes to cyber, needs birth control.

By the time any of something's happened, it's too late. Additionally, they actually collect and sell your information, and they make your cyber privacy worse, so you're a much better target for the bad guys. But the reason I really dislike them is they come with this phony insurance that s- makes so you can sleep at night.

And if you actually looked at the policy very closely, it's effectively uncollectable. It typically has an out for what's called simple negligence. And what that is, if anyone's an attorney, they will tell you it means that you made a mistake anywhere along the way, you're not getting your money back.

But also, they're not first loss policies, they're umbrella policies. So let's say you lose a couple million dollars, you can't go make a claim with them and get collected. Instead, you first have to sue anyone and everyone who could have been one tenth of 1% liable, and you have to do that like your bank, your custodian, even your advisor.

And that takes years and millions of dollars of your own money. And then after you get through that, then you can take them to arbitration. And if you lose the arbitration, you're likely to have to pay their legal fees. Now, look, LifeLock, for example, was set up by a con man while the con man was in prison.

LifeLock got bought by Norton, and Norton got caught recently using their customers' devices without their knowledge or permission to mine for Bitcoin.

Okay? Again don't waste your money on identity protection services. That's my advice.

Eddie Welch: I'm gonna peruse through some of these real quickly, but while I'm doing that, we've had several questions Mark, around what the, the names of the password protection group Yeah

the, the device that you the, you know, the- Sure ... USB blocker that you talked about. You wanna go back through those and then-

Mark Hurley: Real quick, back to the technology real quickly, what you need, okay? And I one is you need a password manager. That's software that's an encrypted online vault.

Never use Google, never use Apple. Those things, they're really easy for bad guys to get into, okay? What you wanna use when it comes to a password manager is one of the online vaults. We recommend Keeper. We find it's really easy to use once it's set up. I joke, my, my girlfriend's a partner in a big accounting firm, and, once you get one of these things, you're never not wanna have it.

She actually told a friend of ours that she wasn't sure she was keeping me, but she's never getting rid of the password manager. That's actually a true story. You need for the virtual private network, we recommend Surfshark. And then for the device for protecting yourself in for using public charging, it's from a company called PortaPow, P-O-R-T-A-P-O-W.

It's about this big. There's also smaller ones for the USC chargers. A- and again, you can buy them online, Amazon, Target, Walmart. They all sell them. But, bring them with you when you travel. Put them in your bag

Eddie Welch: great. So But the, it's almost dizzy in how many questions there are.

Y- your specific service, Mark who is this for? There was a question that said, "Who's this not for?" Who's, who what, who's-

Mark Hurley: Great question ...

Eddie Welch: service?

Mark Hurley: Yeah. First off, we're very privileged to have a partnership with CAPTRUST, and we work with many CAPTRUST clients, many advisors you personally.

Thank you very much. Look, our business is to help protect people, and what we do is we provide a service that costs $35 a month. It covers up to three devices. If the client has more than three devices, for an extra $5 we'll throw in three more. The only upcharge would be if a couple wants to be set up completely separately and so if you want, we'll double the service for an extra 25 bucks a month.

And we come in using Zoom. We can't see or access or copy passwords. We record every appointment. We have two groups review 'em internally for quality assurance. And we're gonna do, come in and take all the steps to protect you. It'll take two to three two-hour appointments to get you set up, and after that we come in every four months to update your protections.

As part of this we look for viruses, we look for all kinds of stuff that shouldn't be there. And then we come in and we'll, we... it's all-inclusive. We give you this technology, training, set-up, 24/7 support. We'll provide you the password manager. We'll set it up for you, put all your accounts in there, reset your passwords for you.

We'll help you get your home network secure. We turn all these settings on and then we come back every four months and update this thing. And then we have a second layer of protection where we will monitor the dark web to see if someone's trying to sell one of your passwords. We'll also monitor to see if someone's trying to steal your home title.

W- we tell our clients w- we're always here. We're here 24/7. Please don't do surgery on yourself. Just call us. We're always available. We got this football team of guys who are the greatest technerds you've ever met, and most of them built their first home computer when they were, like, in elementary school.

They know this stuff better. What would take a client an hour to figure out will take them two seconds. Now if you're interested in getting more information, we have a landing page we put on our website. And I have a, a document that I think you guys will be sending out later that has this landing page also and, step-by-step thing.

But you go to this landing page and you click on the link, and a form will pop up. Now, we do not sell direct to consumer. You can only get this through

CAPTRUST. And the form will have you tell us who your advisor is so we know you're working with CAPTRUST. But also we'll get your contact information, and we'll email you and text you a calendar link, and you can schedule a meeting.

And it can be as short as 10 or 15 minutes, it can be as long as an hour, whatever you need. We're gonna spend the time. We'll explain what we do. Now, we only work with families. We don't work with companies. But we work with thousands of families across the US and Canada- including many, as I said, from CAPTRUST.

So if you're interested in getting more information, I'll put this back up 'cause people wanna see it. It'll live there for a minute or two. This... You go to this link, click on it, fill out the form, and then we'll have to have someone get on a call with you at your convenient time for you.

Eddie Welch: Yeah, and just full disclosure for our audience, CAPTRUST does not...

We're a separate company. D- Digital Privacy and Protection is a separate company. They're just a strategic partner. We do not participate in any revenue or anything like that, that, so just wanna be sure that's totally clear. I'm gonna g- go back and get technical c- for again, if I may, Mark 'cause I was curious- about this as well. How do how do the cyber criminals install RAT on your device, and-

Mark Hurley: Yeah, great question. Great question. W- this is why it's so important you have the classes, 'cause you've gotta figure out how they're getting around, getting you to do stuff you probably shouldn't do. The single most common attack we're seeing right now is you'll be sent a calendar invite from a friend, and the way email is set up is the cyber part of protecting email protects the email, it doesn't protect the calendar.

So what they'll do is they'll hack into somebody's email account, oftentimes where they figured out their birthday's coming up, and then they'll go into the contact list and they'll send out invites to everybody. So you get this invite from a friend of yours for a birthday party or something else like that, and of course you're gonna open it up and look at it.

If you click on anything inside there, you're getting infected, okay? With certainty. And look, if you get a, a calendar invite from somebody, call them before you open it up, period. Never take something... i'm, we're at the point

now here that even if I get an email from a family member and it wants something to click on I'm calling the family member first because the criminals have figured out that they know who you're talking to online.

They're watching, and they'll find a way to plant something like this on your device. If you're gonna go overseas to, say, certain Asian countries, I'd recommend bringing a burner device. I wouldn't bring your regular device. There are gangs there that actually work to plant stuff on your device, and if you are gonna go overseas and you've not turned your device settings on, you gotta do that before you go.

All over the world, people have figured out... Like I was talking to a advisor on the West Coast who had a client down in Chile on vacation, and he was walking down the street. He pulled out his cellphone, his iPhone, put the passcode in, a guy on a motorcycle came up and grabbed it, and 30 minutes later, his accounts were all cleaned out 'cause his passwords were just sitting there, okay?

This is why we, understand, they're, they know where the vulnerable points are, and you have to be- make it so that even if they get onto your device, they can't get anything of value

Eddie Welch: So this is an interesting question. An audience participant says, "I have a dedicated laptop to access my financial accounts and never access the internet with it except for accessing those financial accounts only those financial accounts.

Is that an effective way to protect my assets?"

Mark Hurley: It's an incremental measure that's fine if you've done the other stuff. Okay? So here's what I mean by that. If your home network's not secure, it doesn't matter using a dedicated laptop. They're just gonna go in and get you. Similarly it, the, if you're only using it for doing- And we work with many billionaire families they oftentimes you have tremendous amount of liquidity, we recommend you get a dedicated device.

But candidly, you never wanna connect it to Wi-Fi ever. You wanna connect just using cellular. When you're on Wi-Fi it's like being in a hot tub on a cruise ship, okay? You don't know who might get there, all right? There have been reports where people have been on networks and another device is connected to the network and they've got infected.

So what you really wanna do is either have a separate home network just for that, or with that devi- and never get on public Wi-Fi like that, or find a way to communicate using either a hotspot off your phone or something else. Don't use Wi-Fi to get into that. The other thing to keep in mind is if your passwords aren't re- really robust like we talked about it doesn't matter what you're doing, they're just gonna walk right into the accounts.

And keep in mind that when you're going into your accounts, you're being sent multi-factor codes that are coming back to your cell phone, and if your cell phone isn't secure, guess what? They're getting into the accounts. So you've gotta think of this like an ecosystem. You gotta decide, all right, I'm gonna do, look at all the basic pieces, get all the passwords good, get all the settings turned on, make sure that I've got my home network set up securely, and then that's an incremental measure that you can do.

Eddie Welch: How about biometric identification? Yeah, we like it for certain things, particularly if you're gonna open a password manager up in a restaurant or a bar, you- we'd prefer you use that than putting the code in, 'cause it's easier for someone to look over your shoulder as you put the code in. Yeah

Mark Hurley: At some point, will that get compromised? Yeah. Everything gets compromised. I may be back a year from now telling you guys biometric, you better do this, and this also," because the bad guys have figured out how to do that. Think of this as like a daily arms race. The good guys come up with ways to protect stuff.

The bad guys find ways around it, and it's just literally every day. A good example would be, many of you remember that a while there, they were gonna require everybody to get an authenticator app. It's like a random number generator that you have on your device, and so whenever you went to an account, you put that number in.

And the reason they're not mandatory is because about a month after they came out with the authenticator apps, the criminals came out with new computer viruses that breach the authenticator apps. Of course. Okay? It's just back and forth.

Eddie Welch: One-time passwords?

Mark Hurley: Sorry, please?

Eddie Welch: One-time passwords,

Mark Hurley: Yeah, a lot of people like to have a family password or something like that. Just understand, you use it once, and then you can never use it again. All right? I used to work in nuke weapons in the Army, and we'd do a code, and then we'd tear the code up. One time, just one time.

It example would be, like I have a family safe word. You do realize if they've somehow gotten on, on, onto somebody's device, they could be listening, and so you use the safe word once, and then they have it. That's why you can only use it once.

Eddie Welch: Okay. This is a good one, because this is something we probably many of us are using regularly.

Venmo, PayPal- Yeah ...

as well.

Mark Hurley: How about that? No, V- Venmo and PayPal are very good apps. You just have to realize that if you've not s- set up the whole system securely, they're a vector into your other accounts. Okay? Typically, for example, when these gangs are working bars and restaurants and somebody hasn't done all the stuff they need to do to make sure their device is secure, the first place they go to is Venmo or PayPal to get into either the bank or the custodial account.

So they're fine to use if you take all the necessary steps to make sure they're secure. If they're not secure, then what you need to do is not use those things, right? Just in general, they'll get to you regardless, okay?

Eddie Welch: Okay. We have just a couple minutes left, Mark. Th- so many great questions. We will try to respond in writing to to everyone.

This has been great. Final thoughts this has been in some cases a little chilling, some of these stories were certainly. Leave this on a happy note here somehow. Yeah.

Mark Hurley: All right. G- everybody I do these classes, people say to me, "Oh my God, you're trying to scare me." No, I'm not.

Honest to goodness. If I was teaching driving instruction and then showed you a bunch of car wrecks, you probably wouldn't wanna go driving. The problem is that the internet, as I said, is as dangerous as driving a car. But we as a country are so far behind where the criminals are. I honestly believe in 20 years when a,

when one of my kids has a kid and gives that child a device, they're gonna say, "Show me the settings.

Okay, let me see what your passwords look like." Instead, we're operating like it's 1990. And what, anybody can protect themselves. This is not brain surgery, okay? It just takes an investment of time, it takes some self-awareness, and some education. But you have to make a decision, okay? 'Cause you're either gonna do this, or as I, we like to say, before or after.

You're either gonna do this before you get breached, or you're gonna do this after you get breached. Everybody's gonna get breached, and the only question is what happens after you're breached? How much money are you gonna lose? And it's not hard to protect yourself. It really isn't complicated.

We'd be delighted to talk to you about this. And please, if you ever have a breach, get us right away. We'll do it for free. We'll help you stop the bleeding. Okay? You can't get the money back you may have lost, but we'll help you stop the bleeding. We do this every day for families. That's our purpose.

That's our vocation. That's why our company exists. Yes, we have a great business, but our job is to help protect the most vulnerable from really bad guys online.

Eddie Welch: Yeah, and we do have numerous examples of that, and we really appreciate the help. I get copied on one of those emails so I see that, so thank you for that.

Okay we're at 5:00. We're gonna wrap it up here. Mark, this has been great. Always informative. Audience, I hope this has been helpful for you as well. If you're interested in digital privacy and protection, reach out to your advisor so he can certainly point you in the right direction.

And you can click on the link that, that Mark provided as well. Really good stuff, Mark. Always good to be with you. Audience, thank you. We look forward to to our next webinar probably in the next couple months or so. There'll be, there will be a survey that pops up. If you have a moment and can complete that, that would be great.

Mark, thank you my friend. Audience, thank you, and have a great evening everyone.

Mark Hurley: Thank you very much.

“CAPTRUST” or “CAPTRUST Financial Advisors”) is an Investment Adviser registered under the Investment Advisers Act of 1940. However, CAPTRUST video presentations are designed to be educational and do not include individual investment advice. Opinions expressed in this video are subject to change without notice. Statistics and data have come from sources believed to be reliable but are not guaranteed to be accurate or complete. This is not a solicitation to invest in any legal, medical, tax or accounting advice. If you require such advice, you should contact the appropriate legal, accounting, or tax advisor. All publication rights reserved. None of the material in this publication may be reproduced in any form without the express written permission of CAPTRUST: 919.870.6822 © 2026 CAPTRUST Financial Advisors