Ralph: Thank you everyone for joining us today. A couple announcements first. We are recording this, if you don't want to be recorded… We'll probably use it for some kind of marketing or on our website at some point in the future. If that's problematic for you, mute your phones and turn off your video. But we won't do anything with it that I don't think anybody would be pleased with.

When COVID started, we had already been using Zoom in meetings quite a bit and so, it was kind of a natural progression for us to move out into doing some Zoom Open Hours, we call them. And we started looking for some ideas of some things that might be of interest to people, and as we got through things, I was in a conversation with Tim Marsh, who is gonna take over here in a minute, about cyber security and as it relates to Zoom and to all kinds of other things. I forget the specific topic, but we decided that it would be really helpful to talk a little bit about what cyber security means in today's world, because it's gonna be super important to everybody.

And not only did I get Tim on, but I got Grayson and Michael Terry to join us. So, we've got LPL's whole team. They're gonna start with kind of an overview of the relationship between LPL and our clients and as it relates to cyber security and what the layers are there. Because our system does allow for uniqueness in that context for protecting your information.

The other thing about the topic we're gonna get into some of the best practices, which, I think that's really the thing that most everybody wants to hear.

If you have a question, there's a couple of ways you can reach out to us. First, you can just interrupt. We want this to be as interactive as possible, so feel free to interrupt and just say, 'hey, what about such and such?' If you have my cell phone, you can send a text, and maybe Mona can shoot it out there for everybody, you can shoot us a text or shoot an email to me or to anybody on my staff and we'll try and respond. I've got my email open as well if you don't want to jump in and interrupt the conversation.

So, that being said, Tim? You want to take the lead on this?

Tim: Yeah, sure thing. And good afternoon, everyone. This is Tim Marsh. I lead LPL's advisor-facing cyber security team, helping Ralph, his peers, and folks like you every day. This is gonna be nothing to do with work, nothing really to do with Ralph's practice, but really excited to have Mike and Grayson from my team here. And we're just gonna talk about keeping yourself safe, your family, your kids, grandchildren… Just keeping safe online, especially as things start to get a little bit crazy and more computer-focused each and every day.

So, I'm gonna go ahead… Now, let's share this here. Can everyone see that okay?

Ralph: It just popped up.

Tim: Great. I'll move this off to the side here. But again, I'm Tim. And I'll hand it off. Grayson, do you hear me loud and clear?

Grayson: I do, thank you, Tim. My name is Grayson Wellington. I've been with LPL Financial about three years now. I've been a lot of different roles in the cyber security team. Right now, my predominant role is focusing on getting Ralph and all of our LPL advisors some really cool cyber security tools that's gonna defend them inside and outside the office.

I'm also joined by Mike. Mike, how are you doing, man?

Mike: Doing well. How are you?

Grayson: Doing good.

Mike: So, how is everybody doing today? My name is Michael Terry. I'm actually another member of Tim's team. So, I've been with LPL for around six years now. I've worked in a couple of different departments. So, I started in service center, transitioned over to compliance, and I'm happy to be on Tim's team this year. So, just looking forward to presenting to everybody and hoping you guys learn something today.

Tim: Great. Thanks, Mike. Like Ralph said, we're gonna talk a little bit about how we make sure Ralph's office is safe, but really, we're gonna focus on you. Making sure you're not getting scammed and your family is feeling safe and secure. Best practices to use, different tips and tricks… And again, all of this will be recorded, and if you need to reach out to Ralph or reach out to anyone on my team, please feel free. We're more than happy to help.

So, we'll dive in a little bit, and we'll talk about what I like to call the pyramid. And you are at the top of the pyramid, right? You're the most important. You're why I'm here, you're why Ralph's in business. You're the most important piece of our world and nothing more is true. We're making sure that you have the right training, the right tools, and understand what's out there, what to be afraid of, what probably doesn't need as much anxiety and stress, and how to help.

Ralph's always a champion for technology and cyber security. He reached out very early discussing with my team, my management, making sure that his office was on the right track. Big receiver of team training. We have a strong relationship doing things like this. And all of the tools that your funds, your college retirement, your savings, whatever it may be, those are in a really great place due to the work that Ralph and his team are doing.

And then finally, at LPL, we help Ralph on the back end. We have a team of about 110 protecting all of your information and all of your financials. 24/7 monitoring of budget, our internal budget of about 40 million dollars per year. Dedicated to keeping you all safe as well as cyber insurance and state of the art facilities. So, a really good team. Some really smart people of varying backgrounds. I'm really excited to share some of that with you all here tonight.

I'll talk a little bit about who's behind these recent cyber-attacks. You might see different things on the news, you know, topics you see in the newspaper, and you might see… You know, you hear the videos, the movies, of a hacker in someone's basement or the mob, organized crime. And then, you know, the national news, you might hear about cyber warfare and criminals and terrorism.

I spent the first couple years of my career in military factories. NASA's spacesuit factory, Blackhawk helicopter factory, and at that time, we were really worried about the folks on the far right of the screen, right? Those are nation-states. China, North Korea, people who have a vested interest in learning about the secrets and the militaries of other countries. That's not something that Ralph and my team have to worry about every day, frankly.

For you, in your personal lives and throughout, we're worried about far left, and that's organized crime and just, hacker kids that are up to no good. But these folks are really smart and they're after your money more than anything else. And we want to make sure these criminals… It is, organized crime, often times a mob of other countries. They're really looking to get your money. That's it. We're gonna try to make sure that you have the right tools to know exactly how to not let that happen.

So, I'm gonna hand it off to Michael a little bit and I'll pause and say please, over the next few slides, if you have any questions for me, Mike, Grayson, jump on in. If you need to text Ralph or if you need to just speak up and interrupt over us, please feel free to do so. I'm gonna hand it off to Mike here and he's just gonna talk a little bit about the four biggest issues that we see, both for Ralph and for you folks as investors, what you're gonna want to be careful of.

Michael: Thanks, Tim. So, as Tim mentioned, I'll kind of discuss and highlight the four major categories of cyber-attacks that we see. So, we have phishing, ransomware, tech support, and client impersonation.

So, phishing. Let's start with phishing attacks. So, phishing attacks are gonna be probably the most common type of cyber-attack that we see. So, these are gonna be the attacks where cyber criminals are gonna submit emails with suspicious links or attachments that are actually gonna… These phishing attacks are built and based to feed off of your emotion and try to get you, to entice you

to click on a link or an attachment. So, once you've clicked on the link or the attachment, the actual cyber criminals will use keyword searches and they'll look for usernames, passwords, or key information within your actual device, or they'll look to spread malicious software on your device.

So, when they spread the malicious software on your device, that's actually called ransomware. And what that is, is that's actually a type of malicious software that's encountered when you're actually the victim of a phishing attack where, in the background, your files and your pictures and your data, all your information is actually gonna be locked down, and the cyber criminals are gonna request a ransom in exchange. So, they're gonna request a monetary payment in exchange for actually providing you your data back or giving you access back to your data.

We're also gonna touch on tech support scams. These are gonna be the pop-ups that you may see on your computer that are gonna imitate reputable companies. These are gonna be like your Windows or your Googles, and they're gonna try to get you to click on the link and infiltrate your system.

And then we'll also briefly discuss client impersonation. So, this is actually going to be very applicable to everyone here. We're all consumers in some sort of fashion, and so, let's talk about kind of what client impersonation is and what to do when it occurs.

So, let's dive into phishing and really just talk about what phishing is and how to kind of identify phishing emails. So, as we stated before, phishing emails are gonna imitate reputable companies. So, if you look at the screen here, you'll see Amazon, Netflix, Starbucks, FedEx, etcetera. Some ways to identify these phishing emails are gonna be, they're gonna come from senders that you don't know or that you don't recognize. These are gonna be random individuals that are gonna be emailing you, and often times, these emails are gonna have generic greetings in it. 'hi, sir, hello, ma'am, hi, dear.' So, if you receive an email from somebody that you don't know with a very generic email, it's immediate red flag that you may be receiving some sort of phishing email.

As I stated before, these emails will also have suspicious links and attachments in them, and that's really the clickbait. So, that's what the scammer wants you to do. They want you to click on the link or attachment so they can try to infiltrate your system. And often times, these---

Ralph: Hey, Michael? Hey, Michael?

Michael: Sure. Yes?

Ralph: So, I'm looking at… And I'm speaking for, I think, a lot of people here. I see Amazon. 'Boy, that looks like their logo!' I see Netflix. 'That looks like their…' They look like legitimate emails.

Michael: Yeah.

Ralph: I've identified a few fishy things in the past, and for me, the key is, I'll highlight the reply address from that email, and by clicking on that reply address, I'll say, well, this is not… It does not say Amazon.com. It says something, so, this big, long thing. Is there a better way to do it than that?

Michael: So, that's actually a great technique to actually identify the phishing email. So, if you look at the actual reply email from the sender… If it doesn't make sense, if it's an email that you don't recognize, that's a tell-tale sign that this is an actual phishing attempt.

Another way to know that's a phishing attempt is, you may see spelling or grammatical errors. So, often times, these emails, you're gonna see that they'll have some sort of spelling or grammatical errors. I'll make fun of myself and tell a story here.

A couple of years ago, me and my family were coming back from a vacation in Atlanta. And I was coming back and received an email from Wells Fargo, I bank with Wells Fargo, and it was requesting me to verify some information. Verify some transactions. So, that makes sense, right? Coming back from Atlanta, this isn't my normal spending patterns… So, I went into the email, clicked the email, entered my actual login, my username and password into the phishing email so I could actually go in and verify this information, and when I hit Submit, nothing happened. So, I thought, huh, that's strange. So, I re-entered my information, did this a couple of times, and hit Submit. Still nothing happened.

So, then I started to kinda get concerned. I'm thinking, you know, what's going on? At that point in time, I went and tried to log into my Wells Fargo account, and I didn't have access to my account! So, my password had actually been changed that quickly to my Wells Fargo account.

So, these phishing attempts, as Ralph said, they happen to everybody, right? And I think, as I stated before, that these criminals are really trying to entice and get you to make an emotional reaction. They'll put a well-known logo on the email, some place that, you know, you may work with, and it's easy to mistake it for an actual, a real email and make that mistake, so…

That's what happened to me. I'm not sure if it's happened to anybody else, but if it does happen, we have a couple of tips as well for you.

So, we want you to immediately change your passwords. So, if you fall victim to this, as with my case, I tried to change my password, but I was kinda locked out. I couldn't change my password. So, my next step was to immediately alert Wells Fargo or that company, right? At that point, after I alerted them to a potential fraud, I had to actually go into a Wells Fargo location the next couple of days to provide them with my ID and to kind of verify who I was.

Cyber criminals are very smart, and they make it very, very realistic. And if you don't pay attention, you can easily fall victim to this.

But the phishing emails is just one aspect of it, and that's just one of the actual major attacks. So, let's talk about ransomware a little bit as well. So, ransomware can actually be a result of the phishing email. So, if you actually click on a suspicious link or an attachment on a phishing email, you may have ransomware that actually runs in the background.

So, I kind of discussed what it was earlier, so let's discuss what happens if you're a victim of ransomware and kind of how you should proceed forward, alright?

So, if you are a victim of ransomware, we ask that you never, ever pay the ransom. So, the reason why we don't want you to pay is, one, the FBI recommends that you don't pay, and two, you're dealing with criminals. So, the fact that you're dealing with criminals, even if you pay a criminal, there's no guarantee that they won't just request additional payment or they they'll provide you with the key to actually unlock your files.

So, some best practices to avoid a ransomware travesty would be to regularly backup all your data using cloud storage services. So, we recommend cloud storage services as a backup for your data and, you know, if you are in an unfortunate circumstance where you are a victim of ransomware, you can simply just clean the malware from your device and restore your backup files from the cloud, and that way you won't have to pay the ransom and you still have access to your data.

Tim: And if you're not super comfortable with cloud, what I've set up for my mother and my grandmother is they have one of those hard-drives from Walmart. And every Friday, my mother goes in and plugs her hard-drive into her computer, saves all the pictures, anything important that she needs… Maybe if she's working on a refinance of her mortgage, whatever you can save. And then just unplug it and leave it on the desk. So, if there was an emergency or some sort of problem with your computer, all of it is living somewhere else on the side and then you can get back to normal once any of this got cleaned up.

Michael: Thanks, Tim. That's a great example I didn't think about as well, the external hard-drive.

Male Speaker: You have to disconnect it though, correct? Because otherwise, it would be infected upon the…

Tim: You're a hundred percent correct. Yep. So, save what you need to save, unplug it…right? So, it's physically separated. Unplug it, put it somewhere else on your desk, so if there was a computer problem, you still have that completely separate copy hanging out about five feet away.

And that works. And this type of scam will take everything. It will take your pictures, it will take your documents, it will take important, memorable things. Anything you can think of can go on that external hard-drive, and you buy one at Walmart or on Amazon. It can save you quite a bit of headache. Forget a cyber criminal – even if your computer dies and it's been acting slow and it's getting old, I like to do the same thing and keep it off on the side just in case.

Rose: A quick question on that one. Would you also recommend scanning your computer before plugging in that external hard-drive, just to verify that there's nothing already on the computer? Because otherwise, you're just backing up the same corrupted files, right?

Tim: Yeah. Your logic is right. If there's something already bad on the computer, and copying it onto the hard-drive, it would copy the bad stuff. Certainly, no harm in scanning, right? But unless you're really suspicious something's on there, not necessarily a requirement. More than happy to scan something and send it over. Unless you think something's suspicious, then yeah, I would certainly do a scan or investigate it before copying anything elsewhere.

Ralph: And what about if most of your stuff is on mobile devices? You're not dealing with a PC or a Mac. I know some of the people on the call are probably using iPads as their primary device. Show of hands, is that the common? Yeah, iPads is a common device. So, now your pictures, your stuff, probably a lot of it is already in the cloud. But how does that change the dynamics of what you guys are talking about?

Tim: Yeah. It makes your life a lot easier, right? So, cloud is great for your laptops, your desktops, but you have that alternative. You don't really have an alternative for your iPad, right? It comes with the iCloud. I think you've all seen it when you go to set it up. It's all waiting there for you. So, if your iPad was to become infected, which is exceptionally, exceptionally unlikely, it's all living at Apple out in Cupertino and if you needed to go back and get it, it's waiting for you there.

Your pictures, your text messages, your email. It's all sitting in Apple's cloud for you.

Ralph: Would the same be said for Android?

Tim: Android, you have to sign up for a service, right? So, if it's Google or Microsoft cloud. Apple's a little easier because they force you to turn it on. For Android, you'll have to go out of your way and sign up for a cloud service, but Google and Microsoft would be your two most popular there.

I think of a Google Drive or a Microsoft One Drive, which is different lingo but the same type of tool as an Apple iCloud.

Mark: Yeah, I use Amazon for my backup…

Tim: Yeah. Yeah. Great solution as well.

So, we're talking a little bit about these large tech companies and how to protect yourself. I'll tell a little bit of a story before Mike gets in. I purchased my grandmother an iPad. Was very happy, I don't get to see her very often, she lives in Connecticut, I'm in South Carolina. And about two days into having her iPad, she calls me all worried. Someone from Apple called her and said her iPad was broken and she needed to pay to get it fixed.

Obviously not the case, but it made me really, really upset. So, I know Mike's got a little bit more about that, some of his stories and what he sees as well. It's real and it happens all the time, so we'll be mindful of it.

Michael: Yeah, definitely. Thanks for that, Tim. That's a great example as far as of a tech support scam. So, as Tim mentioned, these are gonna be the pop-ups that you receive on your computer. They're gonna reputate these companies. So, you're gonna have like Apple Google, Windows, and they'll pop up and they may impersonate like a computer technician, and they're gonna say that they've located an issue on your actual computer and they may need to do a diagnostics test or do some sort of troubleshooting to ensure that your computer is okay.

At that point in time if you give access to your computer. So, if they remote into your computer at that point in time, they'll gain access to your files and even your personal information, potentially, within your computer.

So, I'll give another example. As I stated, I previously worked in compliance, and I was working on an investigation where there was an elderly gentleman who had recently purchased a computer, I would say roughly within the past two years, and he received a pop-up that he thought was from Apple on his computer saying that there was an issue with his computer and that he needed to have a diagnostics test done. So, he allowed this fraudster to actually remote into his

computer, and roughly 15 to 20 minutes later, his name and his social security number appeared in the box on the computer from the fraudster because they had actually located his information within the computer.

So, these tech support scams are serious and they're actually very, very dangerous as far as getting your information exposed.

Let's talk about the last type of scam, and that's gonna be client impersonation. And this may be something that Ralph sees a lot, right? So, as I stated, we're all consumers, and if it's a situation where your personal email is compromised, fraudsters will actually reach out to individuals that you previously contacted, that you do business with, in an attempt to actually get money transferred to a newly created account that they've established.

So, the way to combat this is to validate, validate, validate. So, as Tim mentioned, Ralph has annual training that he takes every year. He knows that if he receives a request that seems suspicious via email, he knows that he has to call the client to actually confirm verbally that it's a legitimate transaction to ensure that there's not any fraud that occurs with that money movement.

Ralph: Yeah, and that's actually one of the advantages of working with somebody like the independent financial channel, is that we get to know you pretty well and, for example, everybody that's on this call, I recognize your voice when I talk to you. And Mona and Mark and Rose also are likely to recognize your voice. If we don't, and if it's somebody that we haven't talked to in a long time or we have somebody new, we have some background stuff that we check to verify the identities and that sort of thing.

That's also another reason why we're very particular about your beneficiaries and getting their information on the front end of the conversation as well, so we have a way to verify, in an event that…I mean, we're all gonna pass at some point. But so that the right people get the money, and we want to get to know them as well.

So, more about that to follow. But just, it's a structural thing that I think transcends the threat of the internet impersonation, if you will.

Tim: Yeah. And my wife and I have an LPL advisor up here, Ralph, here in South Carolina. And I like to think I'm techy and I know how to use the tools, but she's adamant that we visit. She knows our voices, she knows our background, and it's part of getting to know you, right? What are our goals, what are our dreams. And that also helps my advisor protect us, right? If someone is trying to call and scam or open a new account or transfer money, she has that background, she has our

voice, she has our story to understand what's real and what's probably worthy of a follow-up.

Michael: That's a great point.

Fem. Speaker: Can I interrupt? May I?

Michael: Sure. Yes, ma'am.

Fem. Speaker: Okay. Two questions. I just opened a new account with Fidelity that my advisor set up for me and I got a link from Fidelity that said, you know, click here to verify your account information. And this was just two days ago. And I clicked on it and I put in the information and a message came back that they couldn't find me.

So, I panicked a little, emailed my advisor, who is in Pennsylvania because I moved from Pennsylvania to Washington, and they said that they were having technical issues, and no one has gotten back to me and it's been two days. Do you guys know anything about Fidelity going through issues?

Tim: Yeah, I can give a little bit of guidance on that. And that's actually something that LPL has been proud of, of not having issues. Given the market volatility, people trying to get in, people trying to get out, the volume has been so drastically larger, sometimes the computer systems can't handle it. Fidelity is one. Robin Hood, which is the mobile app for trading…you see kids trading Tesla and Amazon. That's been crashing as well.

Just from your story, I'm not sure anything is out of the ordinary. It sounds like you knowingly wanted to sign up for Fidelity and---

Fem. Speaker: Yeah.

Tim: ---there was just a mishap. So, I wouldn't say there's anything fraudulent or any cyber issues going on. But, yeah, there have been some issues at some of those more commercial brands, just because they haven't been able to keep up with the demand of rising tech and a lot of, frankly, 18 and 19-year-old kids starting to get involved in investing and opening accounts. They've been overwhelmingly busy, so it's not necessarily out of the ordinary for that to happen.

Fem. Speaker: And this was through my LPL advisor. A second question. I have Morton LifeLock on my laptop, and it keeps passwords for me. Am I being stupid, or am I okay with that?

Tim: No, not stupid at all. It's something we'll talk about in a couple slides. But the idea is great. I think Grayson is gonna talk about his personal experience with another tool, a tool that we like to share. I don't want to say, so far as to endorse

as a company, but maybe the three of us on the line do. But great idea, and we'll talk a little bit more about that I think in the next slide here. Or two or so. Go ahead, Grayson.

Fem. Speaker: Thank you.

Grayson: Yeah, thanks. So, we can all agree that the world has changed drastically in the previous six months. Lots of things going on between COVID to Census to everybody jumping on Zoom calls to talk with family and friends. And just like us utilizing technology as an opportunity, so are cyber criminals.

We've seen an increased amount across the board when it comes to these types of scams, and they all harness their own little characteristics and their own opportunities within them.

So, COVID scams. A lot of times, cyber criminals will pretend to be government organizations, pretend to be harnessing a new kit or a new testing facility and they just want to try to get some data off of you.

Some Census scams. So, Census hasn't come out just yet, but it's coming out and maybe they'll try to formulate ways to steal your family name or where your address is, just so they can use that against you in the long run.

Or even Zoom, like what we're talking about right now where, if passwords or meeting IDs were not put on the Zoom meeting, any individual across the globe can join in on those meetings and potentially cause some damage.

And so, just sort of a couple of best practices and some tips along any of these types of scams would be just like we talked about with phishing and with those scams that we talked about earlier. So, don't click on any links or attachments from sources that you don't know. So, I heard the audience members talk about how he was calling out the email address and never saw it. That's a great red flag, that's a great way to instantly call a cyber criminal out in their tracks.

Only visit trusted websites. So, make sure that you're typing in the correct URL. When you're going into that link at the top in that white bar, make sure that's all spelled right. A lot of times, cyber criminals will try to misspell it on purpose because they know that a lot of people are misspelling it and will trick you into thinking it's that the real website.

The urgent demands and emergency requests. I know Ralph does a really good job of this, but making sure that if you ever get some crazy gift card for $500 or $1,000 or you get this opportunity that sounds like it's a little too good to be true, it probably is for your sake.

And then, add passwords to virtual meetings for additional security. So, this is particular in Zoom. I know Ralph does a great job with this, but even if you're talking to your friends and family, maybe consider adding a password to your virtual call. Just make sure that it's safe and secure.

And last but not least is just protecting your information. So, I'll go in the next few slides to how you can do just that.

So, the number one way is protecting with a password. Those are the keys to your kingdom. I call it the safety net when all else fails. So, where should you start by setting these passwords. There's four main platforms that I like to see my passwords on my accounts. That is email, because of the phishing scams – we heard that phishing scams are really popular. Social media, because social media is tied to your personal brand, it's tied to that personal identity, so you want to make sure that it's locked and secure. Your financing apps – so, Wells Fargo, Bank of America… Maybe Ralph has an app. Just making sure you have passwords on those apps as well because it has our financial information attached to it. And last but not least is eCommerce. So, Amazon, eBay… If a cyber criminal were to get access to that account, they could instantly start draining the bank account of all of the money that's in that bank account by just purchasing anything that they wanted.

And so, we had a really good question asked earlier: So should I write down passwords, or are password managers a good option?

And the first answer to this would be, I strongly encourage to never write down passwords. As technology becomes more advanced, we've got a lot of great alternatives to this. And if your house or your office were to ever get broken into, they have that journal full of passwords. My brother left a notepad in his car overnight that had his whole list of passwords, and a laptop, and the next thing you know, the next morning he came in and the window was smashed and the password journal was gone. So, he had about a 48-hour headache where he had to go and change every password that he could remember of his entire life.

And that could all be erased with these great tools called password managers. So, just like the one that I mentioned earlier, there's a lot of great options. I like using this tool called LastPass because it's super intuitive and it's super easy to use, even for the people who think they're not too tech savvy. It automatically creates all the passwords for you and stores them using some very advanced cyber security algorithms, and stuff that's almost too smart for me. It encrypts everything and it makes sure that it's locked away so you can sleep peacefully at night.

LastPass is a great option for it but there's also other great options such as Norton or even KeePass. And you'll never have to remember your passwords ever again. You'll never have to remember, oh, did I put one or two? Or did I put one exclamation point… You'll never have to remember that because the computer application already has it designed so all you have to do is just click that button and it automatically puts in your username and your password.

If you do decide to go to that or creating your own passwords, I want to keep it simple and sweet with you. And let's start with a phrase that you know. So, start with 'I love California.' You want to make sure that it's not just one word such as like pineapple or soccer. The simple words like pineapple or soccer are often very easy to crack for cyber criminals, and that goes even further when they don't have numbers or symbols or like exclamation points attached to them.

So, as I stated, this is a good starting point. Then you want to start with adding those unique characters. So, maybe capitalize. Make it numbers, make it symbols, make it lowercase… Just make it more complex and unique.

And then what you want to do after that is just making sure that you're not using the password across multiple websites. I know I'm guilty of this before I started using LastPass, and then this is where LastPass or other password managers really come into play here, is they never use the same password across multiple websites. That's because you've got to remember, let's say your password for Facebook got hacked and you used the password for Facebook, LinkedIn, Twitter, Google Chrome…everything. And so, if they have that one password, then they have the password to all those separate accounts.

And cyber criminals, a lot of them are dumb, some of them are smart enough to realize that, hey, I can just use this password and try it somewhere else and I guarantee you it will work.

And then change the passwords frequently. So, we ask our advisors here at LPL Financial to change their passwords on a regular cadence. Once about every three months. And we encourage the clients to do the same. We know it's tough to keep remembering those passwords, and especially when we don't want you to write them down, and that's where password manager also come into play, so that it will save those new updated passwords for you. In addition, those passwords managers, you also just click a button and it will change all the passwords in one go so you never have to do anything with it.

And then don't use repetitive keys. So, again, I'm guilty of doing this as well before my password manager transfer. But sequences like AAA or 1234 or QWVRTY40 or even just PASSWORD, I mean, those are super simple and easy to

break and often times the most at risk when it comes to getting your password broken.

The next thing that I want to talk about is multifactor authentication.

Mark: Sorry, I've got a question about passwords.

Grayson: Yep, sure. Go ahead.

Mark: So, I know someone who does keep a password journal, but in the journal, it has basically the last eighth of a password, so they only remember the first eight, and the first eight is the same on every single password. Have you heard of that before? How secure is that, actually, compared to…

Grayson: So, it would be under my assumption that he or she is using that password across multiple websites. Which is fine. It could be a little bit better, but it's certainly not as bad as just having all your passwords in one journal like my brother did, and had his car broken into.

So, what I would encourage with that kind of circumstance or that kind of use case would be to have that journal locked away when it's not in use. Don't leave it out in a public setting such as like your office or even your desk or even at home. If you're not using it, just put it in like a locked file cabinet or even in a safe at home.

Ralph: Grayson, what are your thoughts about having your browser store your passwords? You know, we use the…I'm sure many people use Chrome, but all the browsers now have the ability, when you go on a website, they'll store the passwords. What's advice on that?

Grayson: So, personally speaking, I'm not a big fan of keeping all of my eggs in one basket. I like to have my information in different places. So, we talked about ransomware. You don't want to have all your information stored in one location because if that device were to get hacked… So, I'll be honest, while it is very rare that I can assume that Google or Apple would be hacked, if they do get hacked, then they have all your passwords.

So, that's why I like using a tool such as LastPass or even KeePass where their sole responsibility is just making sure that passwords are protected, secured, and well managed. Whereas Google has to worry about the search engine and then keeping your passwords and making sure that your credit card information is safe… While those companies are super good at maintaining a lot of items, I put my trust in LastPass or a service where that is their sole initiative, is just making sure that their password is safe and secure.

Tim: Yeah. And if I can add onto that too… This is Tim. In your personal life, it's probably not that big of a deal, right? It can store your credit cards, it can store your passwords, it's convenient… I wouldn't do it in your business, though, to be honest.

Because there's just generally larger sets of information, right? If you have a small business or you work in an office with other people's information, I would stick to a tool like LastPass other than letting Google or Apple auto-populate it. But, look, we're not gonna split hairs. It's probably gonna be just fine in your personal life.

The benefit of, like Grayson said, LastPass is they're focused on just that. And it's a very similar experience. Once you sign up for LastPass, just like if you had to type in your username or password and Google is gonna fill it for you, LastPass fills it for you as well. You just click on the little…the Ellipsis, the little three dots in the logo, and it's gonna auto-populate it, just like Google or Amazon or Apple would, but in a little bit more for a secure manner, especially for the workplace.

Ralph: Cool.

Grayson: So, now we're moving onto MFA, or multifactor authentication. And I know that sounds very complicated but it's super easy after we break it down.

So, what happens is, you have your laptop and you're logged into an account. When you log into that account, you also have already sent it to your phone where it would text your phone, hey, this passcode is 678980. And you say, okay, I can put this passcode into the computer, and I'd get full access.

And what that does is that prevents hackers from only stealing the account information from taking the account. This really helps mitigate the risk of overseas hacking. So, a lot of the times you'll hear on the news, you know, Russian hackers, North Korean hackers just stealing accounts. And none of the accounts have MFA on it, because if it did have MFA on it, they would also have to have that phone or that second token in order to access that account. So, I really do encourage multifactor authentication. It's super simple. I can share a resource that shows how to turn on MFA across multiple websites, but at the core, it's always gonna be in your security settings or your privacy settings or on Facebook, Amazon, Wells Fargo… Any of those four platforms that I talked about earlier is where I also use MFA.

Ralph: So how big of a headache is it if you have to change your phone number?

Grayson: [Laughs.] I have not had that incident yet. Luckily, I have had the same number for about 10 years, in theory, if I'm thinking into it right now, I think it's pretty

easy because all you have to do is recalibrate your security settings to set it to that new number.

Mark: With the rise of multifactor authentication, have we seen any rise in what's called…I think it's called sims swapping?

Tim: Yeah, I'll take that one. Multifactor authentication is almost entirely NOA. If the NFA or a different country was trying to get you, they would get you. But almost impossible to track. If you sign up for Apple or you sign up for Facebook and you turn on that setting where they're gonna send you a code to your phone, you could be anywhere in the world, only you're gonna be able to get into that with that phone.

Yes, at times in very…I'll say very rare occasions. I wouldn't want any on the line here to be concerned about it. People will swap out the guts of a phone or a malicious Verizon employee will swap out the back end of your cell phone and try to switch the number. But, especially for this group, it's not something I would be overly concerned about. The return on this is much better than any other concern or worry you may have.

And it's worked for me before. My iPad about three weeks ago said: are you in Shanghai? Promise you, I wasn't. So, what do I know from that, right? Somebody had my account name and my password, no matter how strong I thought it was. It wasn't necessarily my fault that someone gathered that information, but they did, and they tried to log in. And that one-time code got sent to my cell phone, not to whoever the bad person was. So, I can just reject and say, no, I'm not in Shanghai. And I think Mike mentioned it earlier – that's a cue that I need to go change my password to something very different, but it saved me quite a bit of headache than if they were instead just to log in and start poking around my personal area.

Grayson: So, one of the final things I want to talk about as well is social media. It's your identity in cyberspace. I have multiple platforms for social media, I know Tim does as well. And as more and more social media platforms come up such as LinkedIn or even Snapchat that you want to start using for business or even for your personal life, we want to make sure that you're safe and secure on them as well.

So, I broke it down into five simple steps to social media. One is that there's no delete button on the internet. And what I mean by that is, often times individuals think, hey, I can post this and if I don't agree with it later or, or if I get in trouble, I can just delete it in an hour. And while that is true that you can delete it, often times, people will take screenshots or snapshots of the post and

just share it somewhere else. So, just make sure that you're being safe and curious and think ahead before posting what you want to post.

Don't broadcast your location. So, a lot of times, this is very popular with Facebook that they'll say, 'hey, are you going to Target? Post your location going to Target.' I encourage you to not do that because that only gives the cyber criminals more data and information to run with. So, they say, 'oh, Tim went to Target? I can now break into his house because I already know his address and I know he's gonna be gone for the next two to three hours.' So, just be sure that you're turning off those locations or you're not sharing them when you're…

Tim: And I'll--- If I can order up you there, Grayson, I've actually had that one in real life. My dear mother shared that we were going on a cruise for a week. It was a great cruise. We came back and the side window on the house had been smashed in. So, someone locally, unfortunately, had saw that post, assumed we were all out of town, showed up that night, and they were right. So, just be mindful of what you're sharing, particularly when you're gonna be out for an extended period of time.

Grayson: Thank you, Tim.

Ralph: I've had a rule of thumb on social media for years that… Because when it first came out, I was a big proponent of social media. But my wife reminded me that when I posted that I was in such and such location and she was home, I was announcing to the world that she was home alone. And so, the rule of thumb in the Bender household has been for years now that you take your pictures and then you post them after you get home.

Grayson: That's a very good rule of thumb. I agree and back you up completely with that.

The third step I will talk about now is connecting only with people that you trust. So, a lot of times cyber criminals will pretend to come up with fake aliases and fake names, and they'll even put up a fake profile picture and some fake posts and try to friend individuals and to gain their data information. Make sure that you only friend or accept friend requests or follow individuals that you know and have met in real life.

And then flip your account settings to private. This is super easy. Often times, it comes with like a little lock next to your name, or just carrying on some checklists in Facebook. But making sure that you're setting your settings to private so not any wandering pair of eyes can come by and just view your profile and see your pictures or where you're going on vacation.

And then last but not least is turn on MFA. So, like I just talked about before, MFA is a great way to keep everything locked down. Just go into your security settings and it should be a quick toggle that you turn on.

And then we talked a little bit earlier, I know a question got hit on this with mobile device tips. So, iPads, cell phones, tablets, anything in between, they've become super popular. In fact, I think I've run into more mobile devices than I do laptops and desktops nowadays. And with that, we want to make sure that we're just as safe on our mobile devices as we are with our computers and our laptops.

So, I've broken it down into four steps. One is, just like laptops and desktops, let's make sure that we use strong passwords. I know there's a lot of different orders that you can do for like an Apple password. You can do six-digit to four-digit. I would stick to six-digit just to make sure that it's safe and secure.

Keep software up to date. So, a lot of times you'll see the IOS or even the Android pop up with a window saying, hey, it's time to update to IOS 13, 14, 15… And I'm guilty of this too, often times I'll just set it to the side. I'm like, hey, I want to use my phone, I won't let it download right now, and it's too cumbersome. But often times, those software updates are via security updates as well. So, they provide your phone in tip top shape with everything you need to stay safe and secure.

And then, know your apps. So, this is both for Apple and the Google Play Store. I encourage you to only download apps that have high ratings and are downloaded frequently. A lot of times, I see where apps have low ratings and they look like they've been on the store for two days, and those are often times the ones that have bugs and they have some nasty ransomware and some viruses in there that go on unsuspecting devices.

And then this thing with Bluetooth and public wi-fi. So, a lot of times when we're out and about going to McDonald's or going to like Starbucks, you might connect to the public wi-fi just to search Facebook or search LinkedIn. Public wi-fi, if you don't use the VPN or any other security controls, can be very dangerous, and I encourage you to stick away from that if you can. LTE, or your data, is a great alternative to this, but public wi-fi and public Bluetooth can harness some nasty, nasty enemies in the shadows if you're not careful.

I will now hand it off to Mike to take over protecting your children with cyber security.

Michael: Thanks, Grayson. So, we'll kind of conclude the presentation and talk about cyber security as it relates to children.

So, I'm a father. I have three children and two stepchildren, so this is something that's near and dear to my heart. A lot of these are piggy backing off of kind of what Grayson mentioned earlier as far as with, you know, general cyber security and internet practices, but we'll kind of dive into some do's and don'ts specific to children.

So, you're gonna hear me probably say this a few times on this live, but I'm a big proponent of keeping an open line of communication and definitely educating your children, right? So, you want to educate them as far as, they should never give out their personal information, right? Like, you should educate them as far as how important it is to keep their personal information and kind of educate them as far as with what consequences could occur if their personal information is exposed on the internet.

You also want to block websites, right? So, there's a lot of unsuitable content on the internet for young children, so you want to make sure that you kind of block that and you want to have control over what content that they'll actually have access to. And you'll also want to try to set time limits as well so that they're not on the internet for extended periods of time.

You also want to discuss the impacts of cyber bullying as well, so, on both sides of it. So, you want to keep that open line of communication with them so if they are being cyber bullied, if they're a victim of cyber bullying, they feel comfortable enough to have that conversation with you. And this shouldn't just be, you know, your children. This could be nieces, nephews, grandchildren as well, right? So, any young person in your family that you have a bond with, you want to kind of make sure you have that conversation with them so that they're comfortable, so if something happens to them, that they can go ahead and, you know, relay that information.

On the other side, right, you want to discuss with them the negative impacts that occur from cyber bullying. I'm not sure if you guys have seen it, if everyone's seen it, but in the past couple of years, you know, there have been too many stories that I've seen that have kind of posted as far as news headlines where you see young adolescents and young teens who have lost their life far too early just because as a result of the impacts of cyber bullying, and they really couldn't kind of take the stress and the pressure of everything that was kind of occurring. And that's a direct result of social media.

So, let's talk about some things that you don't want them to do, right? So, you definitely don't want to create any accounts for your children with unlimited access. This kind of piggy backs off of what I was saying before. There's a lot of

content that's unsuitable on the internet for young children or adolescents and you want to make sure they don't have access for that.

You also never want any photos to be posted without your permission. So, let's follow what Ralph says, right? Let's wait for photos to be posted after you get back. Just make sure that you have permission to post these photos as well.

You want to make sure that the friend requests that they receive are from people that they know. You don't want your children associating with people that they don't know at a young age. You want to keep the network of people that you know. And also, I know it's not the coolest thing to do, but you want to be a friend of your children or your grandchildren or your nieces or your nephews as well so that you can kind of be a fly on the wall sometimes, to kind of monitor the content that they're posting or what they're kind of getting into as well.

And last but not least, you never want to share passwords as well, right? It would be a terrible situation where, you know, a child in your family, something posts on their account from somebody else who had access to their account that didn't represent…you know, is not representative of what you want your child or family member to actually post.

So, those are kind of the do's and the don'ts at a high level as far as with children, and this is gonna conclude our presentation. And we thank everybody for joining and we'll open it up for any additional questions anyone might have at this point in time.

Mona: I have a question. I have a question regarding home computer security. So, you'll see all sorts of different anti-spam software that you could purchase and there's also some that's for free. Is there an advantage to one or the other?

Tim: Yeah, I'll take that. This is Tim. There's really no advantage from brand to brand as long as you pay for it, right? In this world, you really get what you pay for. I mentioned LPL's $40 million budget, right? That's not practical. But those free versions, they come with a catch. They're collecting your information and they're sharing it with others.

I don't want to bash brand to brand, but Kaspersky was tied back to the Russian government, right? So, if you have Norton or one of the other local tools, you might be a little bit safer. You just don't want to get a free version.

More than happy to repeat if we need to, as well.

Mona: Okay. Thank you. And then can I ask one more question?

Tim: Sure!

Mona: So, robo-calls, spam calls, those… Is there anything that we can do to protect ourselves there? I mean, I hang up. We get them all the time, you know, it's… I get them at home, I get them on my cell phone, and I get, you know, at least something spam alert, potential scam. But is there anything that we can do about that?

Tim: Yeah, my wife is a victim of those. She gets quite a few. I'm not sure how her number got on those.

My tip would be, when you answer the phone, don't say anything, right? One, don't answer it. I have a bad…well, a good habit, but I do not answer it unless I know who it is. Let it ring. If you choose to answer it or if there's some sort of message… A message is easier. A voicemail because you know it's garbage. If for some reason you need to pick it up or you choose to pick it up, don't say anything. And I'll share with you why.

A lot of credit monitoring tools, they ask you to register your voice. I don't know if any of you have ever signed up for credit monitoring, but they know your voice. So, we've seen criminals trying to get you to say, 'Hello? Hello? Hello?' And they're gonna take that voice and use it against you.

If you need to pick up the phone, pick it up, let them try to say something, and the second you're not feeling comfortable, just hang up. They're cyber criminals. In this case, they're criminals. Don't need to hurt their feelings, it's fine. We'll hang up.

Mona: Thank you.

Ralph: On that point, I found an app recommended by the Wall Street Journal a couple years ago called Nomorobo, which is an app for my iPhone. It scans the calls and when I get a call comes in, if it's a known robo-caller, it pops it up with a big red mark on it. It says, you know, this is a robo-caller. And I just let it go to voicemail.

Normally, I… It's frustrating for people trying to reach me, but I normally let my cell phone go to voicemail anyway for some of the reasons you just said, not the least of which, frequently, I just don't hear it, but… [Laughs.]

Male Speaker: I've got a… One other thing. Are there differences in different cell carriers? I've used, and it seems to really… I use Consumer Cellular, but I hardly get any type of spam. Other people that I know have other services and they get it all the time. Is there a different level of protection that some carriers provide than others?

Tim: Not necessarily, and I certainly don't want to say protection. Often times, it's just a phone number that gets wrapped up in a breach or an exposure, right? I have

Verizon, we don't get too many. My wife gets a ton. I'm not sure why. Maybe online shopping, who knows.

So, no. Brand to brand, pretty consistent. And that speaks to what Grayson said about not using public wi-fi. If you can use your cell signal, if you're out and about and need to shop on something, they're all gonna be pretty consistent. Certainly, better than going to a Starbucks internet, for example.

Mark: Question about robo-calls. Do they ever use a legitimate number or are they always spoof phone numbers they're calling from? Because I've got callbacks from people I've never called who seemed like a legitimate person wondering why I called them. It's like, I didn't. So…

Tim: Yeah, that's a great question. My boss is our chief information security officer at LPL. He spent about 20 years in a large German conglomerate as well and he demo'd it live for an audience the other day, where there's an app… You know, go online and in 30 seconds, you can make any cell phone number in the world look like another cell phone number.

Now, are they gonna attack you with that every day? No. But I think, Mark, you've seen it firsthand, it's very easy to make it look like other people are calling, or make it look like you're calling other people. So, unfortunately, that's more of an after-the-fact, right? We'll make sure, 'hey, if you're hearing anything suspicious, it's not me!' Or if you suspect that it's not the right voice on the other line, go ahead and hang up and call back the person that you know could be the right person.

Are there any other questions?

Ralph: I was just getting there. Okay, so, if it's been helpful, hands up. I want to see if it's been… Thumbs up. This has been good? Good. Okay. Mark, take a screenshot of everybody with their thumbs up.

Fem. Speaker: [Laughs.]

Ralph: Print screen.

Fem. Speaker: [Crosstalk] Yeah, this was incredibly helpful.

Ralph: Yeah, that's good. So---

Tim: I appreciate it. Also, more than happy to answer anything else you guys have. If it comes up tonight, in the middle of the night, you wake up and you remember something, please reach out to Ralph and he'll get ahold of me, and we'll answer any---

Ralph: Reach out to me in the morning! Not in the middle of the night!

But, yeah, absolutely. Absolutely. If you've got any other ideas or any other thoughts. I'm glad that this was helpful. I just want to let everybody know that we've got these going every couple of weeks now. In two weeks, we're gonna have another runner, which, thanks to John Hancock, we have Jared Ward who placed sixth in the Olympic Marathon down in Rio de Janeiro four years ago. So, that's the same time.

And then we have two events scheduled for August. I don't remember the dates, but both dealing with long-term care issues and different concepts of… You know, What Happens If You Live Too Long is one of the titles. But I think they're useful where you need help. And the other one is having to do with using 529 plans in a creative way to help fund long-term care issues down the road. Actually, for me, this is a continuing ed type thing that I didn't even know existed until our friends from Columbia Threadneedle pointed it out to us.

So, we've got a constant flow of these things going on, so pay attention to the emails and feel free to share them if it's been useful. We're trying to make them as useful as possible. So, help us out by sharing them with your family and friends as well.

If there's no other questions, we'll just say thanks for joining us. Thank you Tim and Grayson and Michael.

Mona: Saying goodbye to my notebook tonight! [Laughs.]

Ralph: [Laughs.]

Mona: Thank you. It's been amazing. Great, great information.

Male Speaker: Thank you.

Tim: Thank you all. Appreciate it. Have a great day.

Mona: Thanks, everybody, for joining. Thank you.

Ralph: Bye bye, now.