18 | PROTECT YOUR PRACTICE & PERSONAL DATA FROM CYBER FRAUD WITH MARK GROSVENOR

Jason O'Dell:

Thank you, David. I get the opportunity today to be here with Mark Grosvenor, and we're going to jump right in to our cyber discussion. And Mark, right now, you obviously can't turn on the news without hearing about another cyber security incident. One major example, right now, we're hearing a lot about as the PPP loans and the scams coming out related to that. Why has this shift been so significant over the last couple of years, and what's fueling the surge?

Mark Grosvenor:

You're absolutely right, Jason. It's kind of, it's amazing. I mean the cyber fraud market, if you look at it globally, is about $6 trillion. It's what they're estimated to be this year, which is about five times the annual revenue of the pharmaceutical industry worldwide. So, I mean, it puts it in perspective from a scale side of things. And with all the information that's available out there, the PPP loans that are going on, obviously the bad guys are getting some of that information. They're taking it and combining it with all the social engineering that they're doing, and they're getting the information and looking at it on an entity by entity basis. And they're being able to sound a lot more credible when they call up. They know who your bank is. They know that you're getting the loan. They can pretend to be either one of those two entities.

We're seeing a lot of the individuals come after companies now with that information combined. And so it's very important from a user's perspective that as they start to get those phone calls, as they get those emails and somebody coming after them from a text messaging perspective, we all know who our bank is. We all know who we got our loans from.

Don't feel like you have to click on the links just because they're in the email. Go type the address into your web browser on your own. From a standpoint of phone calls, you can't trust caller ID anymore. You can buy apps on any of the app stores for under $5 that you can put in whatever you want caller ID to show when you call somebody. So you can say it's Wells Fargo with the right phone number and everything else, but don't be afraid to say, "Hey, I'm going to call you back." Hang up the phone. Get out, go on Google and look up at Wells Fargo phone number, or use the one that you've got on your statements that show you what number you're supposed to call and call them. You'll get back to the right department and go at it from that approach.

But it's certainly something that we see a lot of these days. And we're seeing the bad guys come after organizations in many, many different ways. And because it's so lucrative, it's something that they're going to continue to do for quite a while.

Jason O'Dell:

That makes a lot of sense. And you obviously got to be very leery of anything you're getting in your email these days, and or phone calls that you're receiving. What do you think is driving a lot of this surge over the last several years?

Mark Grosvenor:

I think there's a couple of things that are driving it. I think, number one, I think the amount of information that we have online in the cloud these days is so much larger than it's ever been. The information is out there and you hear the term the dark web a lot, and that dark web is just kind of where all the nefarious activity happens. And what you find out on the dark web is where people start selling information. And they'll sell everything from emails and passwords to financial accounts. And they'll actually sell the balances on the accounts, and different prices go for different balances, et cetera. So it's pretty sophisticated marketplace out there. And then of course all your illicit drugs, and theft of things, those kinds of things also are going in that area.

But it's getting so much easier if you think about it. In the old days, from a security perspective, they used to have those things called dumb terminals. They were a mainframe. They weren't connected to much of anything. And when you left the office, you left it all behind. Now, you don't leave the office behind. In fact, many of us, the office is wherever we go, because we have not only our laptop computers, but our tablets and our cell phones. So the number of devices that we all have and the places that are avenues for the bad guys to get information has significantly increased. So they have a lot more ways to do it.

And then finally, I think it's just the technologies that are out there. From the standpoint of we use so much on our devices these days, as far as communicating and accessing information and doing our business, that it's so easy to quickly get lost in something and click on something we didn't mean to, and before you know it, you've given them access to a PC or to data or to an account that you didn't mean for them to have access to. So it's just the overwhelming place you can do that.

Jason O'Dell:

It seems like there's this unbelievable unfettered access to all business information. As you were just explaining, just the fact that everything sits up in the clouds. There's things on all of our devices that it feels like it's hard to prevent an attack from occurring. So that's interesting. And it seems like there's an extreme ease, if you will, in really getting to this information. What is making it easier these days to do these, or create these attacks or get information or get to our private material?

Mark Grosvenor:

I think number one, I think it's a lot of it's the social media. People think that they're... It's funny, I saw a survey where they were talking about people and over 50% of them said they don't post anything personal on their social media accounts. And I don't think they quite realize what they're posting and how quickly it becomes sensitive or personal. And I was talking to one individual and she was saying, "Well, I don't post things like birthdays and all that kind of stuff on there." And what she meant was she didn't post that her birthday was January 25th of 1972. But when they do things and they go out there and they're like, "hey, I just want to wish my hubby a happy 50th birthday today", well, you've just given away the year and you've given away the date of what exactly your husband's birthday is, or your birthday, et cetera.

So things like that, the bad guys are using a lot. And people just don't even realize they're giving it away. And let's not even talk about how many people use their pets name as their password, and they mentioned their pet 10 times on social media.

But I think the real thing is the bad guys that go out there and identify all these vulnerabilities that exist within our systems, within our phones and on our computers, et cetera, they kind of take a lot of pride in telling everybody, "hey, I found this hole" and they publicize it. So then now everybody has it. So now what was one person knowing how to do it now though, the entire dark web has got the understanding of how to do it. And if you look at the fact that many of these services are almost commoditized these days. So you can go out and buy email address distribution list that you can send it.

You can think even buy the virus that you want to send. So I don't even have to be smart enough to know how to create the virus. I can go buy one on the dark web, and mail it to everybody that I just bought on my email distribution list on the dark web. And the nice thing is I don't even have to collect money for them. When the virus hits and the individuals businesses get locked up with a ransomware, there's a virus as a service where you can sign up for it and they'll actually accept the phone calls and all the payments. They'll trim their portion off the top, and then they use one of those cryptocurrencies and they can't be tracked, to ship the money back to the person that started it. So they've got this whole enterprise that's set up that allows pretty much anybody to be involved from anywhere. And I certainly think that's the biggest ease. The biggest piece of it is just the way they can do it and communicate it with so many ways of hiding their tracks and not being able to be followed.

Jason O'Dell:

I've heard of social engineering attacks and the fact that they've gotten much more sophisticated. What is it? And is that actually the case?

Mark Grosvenor:

It is absolutely the case. I think from a social engineering perspective, so much of our lives are online like we've talked about already. And if you think about it from a standpoint of all the breaches that have happened, so whether it's Home Depot or whether it's some of the big rewards programs that are out there, Target, right? The bad guys are getting information that's above and beyond what most people would know about us. So they know I shop at Home Depot. They probably even know some of the things I bought at Home Depot. So when they call me, they sound so much more credible. Because they're talking about my last purchase at Home Depot, or they know that I'm at Home Depot, and they know that I like to travel. And they'll weave those in together into something that they're trying to offer me that makes it enticing.

And so I think that when you look at those kinds of things and just the fact that they're getting so much more sophisticated, and they're not just an individual anymore, but they're actually organizations that are behind a lot of these cyber attacks, that you can see how they become very convincing and how they're able to use that information.

And I guess if you go on more, I mean, I have children. I'm sure many of you guys have children, right? I mean, people on social media know I'm going on vacation before I know I'm going on vacation. Because they're out there telling everybody, "Hey, we're going here on vacation." And all of a sudden now, my

neighbors all know before I know. Because my wife hasn't told me, "Hey, we decided this is what we're going to do for vacation." So I think that some of that comes into play a lot. And I think that it's important that always when you get phone calls or emails from people on that sort of thing, from a social perspective, if somebody sounds like they know a lot more than they probably should, I would definitely be a little bit careful. Because it's somebody that's probably trying too hard to get you to really click on something or follow through with something.

Jason O'Dell:

I think one of the things that's really, at least it's frustrating for me and I'm sure for a lot of people, is you rarely hear about these bad guys being caught. Why is that?

Mark Grosvenor:

That's a great question. It definitely runs through my mind a lot. And I was fortunate enough to go to a presentation and a meeting with the Secret Service, and they were talking about it. And they were kind of like, well, first of all, in the old days, you used to have to be close to somebody to really commit a crime. I mean, if you go back to 30 years, if you were going to rob him, you had to be right next to him. If you were going to go and do a home invasion, you had to go into the home and do it. That's not the case anymore. The internet has really opened things up and now these bad guys can sit in any corner of the country or even the world for that matter.

And the long arm of the law is just not long enough to reach out and grab them. And then you talk about the ability to hide your tracks. You can bounce around to hide where you're coming from. You can take the payments over crypto. You can get the monies and shuffle it to offshore bank accounts that don't have extradition rights with the United States, and it makes it very difficult for the authorities to go after them and get them.

And there's an individual that they were talking about that was from Russia. And they knew exactly who he was. They knew what he looked like. They knew where he lived. They knew everything about him, but they just, they couldn't touch him. And he was getting about $15 million a month in cyber fraud from the citizens of the United States and around the world. And the only reason they ever caught him was they finally convinced him that his mule that he was using in the United States to kind of shuttle some of the money got cold feet because the government got to him. And then they convinced him to come in through Cuba, come up to Miami, and they were going to hand it all off in Miami. And the moment he stepped foot on the American shores is when they grabbed him. But up until that point, they knew everything about where he was coming from, but it wasn't until he stepped on the land in Miami, that they could actually do anything to take him into custody. So it's tough. And the anonymity associated with this crime is so hard for them to track down.

Jason O'Dell:

Yeah. Crazy. So what do you recommend a company do if they have a cyber incident?

Mark Grosvenor:

I think preparing ahead of time is the most important thing. And I know a lot of small companies out there, a lot of practices think to themselves, "Oh, we're too small, we're not going to be who they're coming after." But the reality is these guys come after everybody. They have no prejudices against anybody in particular. They are happy to take money from anywhere they can get it. And so it's very important to number one, lay out your plan ahead of time. Make sure you have kind of a business continuity disaster recovery type plan in place of "what would we do if all of a sudden we lost access to every single file that we had." And I think in order to answer that question effectively, it's making sure you have a relationship with a good technology company that can help you put that in place ahead of time.

So a lot of small companies want to use, "Hey, I've got my son's friend, who's a computer science major. I'll use him as my technology guy". And there's nothing wrong with their technical capability. They just don't have the experience and the understanding of all the threats that are out there. So getting with a reputable organization that can come in and say, "Hey, we're going to do these five things as far as setting you up. One is making sure that we archive your information off-site, in a secure location every night." So that if you happen to get one of these attacks that completely takes your network over, you're only out the one day of activity. You're not out, three months or six months or anything from that perspective. So I think that's number one.

Number two, knowing you have somebody to call. The moment you realize you've had something happen, having a trusted company that you can call, that's got expertise in identifying what the threat was, where it came from, and what it did, and how to clean everything up to get you back in operation is extremely important to be able to get back on your feet quickly.

Jason O'Dell:

Yeah, that's all great points. And you know, obviously 2020 was a unique year in every single aspect of being unique, if that's even the right word to use anymore. Talk a little bit about some of the things that went on in 2020 related to cyber security.

Mark Grosvenor:

So it was a super interesting year in the cyber world as well. I mean, all of a sudden we went from organizations and employees working within an office with a very confined environment, that very set processes and procedures and in many cases, very good technology controls, to all of a sudden they were working from home on a computer that may or may not have been a business computer. You don't have any idea whether it was up to date on the security patches, whether it had all the antivirus on it. It's probably the same machine their kids were using at some point during the day, no account on what pages and websites those kids were going to. They might be putting things on the machine that were then kind of watching activity, et cetera. And obviously we all know from an impact perspective.

I mean, it was a significant distraction for all of us. So all of a sudden you go from being in an office where you can have a little bit of quiet, not quite as much disruption, to where you're at home. You've got people coming to the door with deliveries. You got kids in school. You're trying to run back and forth and help them from home. Your spouse is running around on their calls, doing what they're doing. The chaos was significant. So employees are distracted. They were trying to get more done in less times so they're clicking on things a lot faster. So we saw a lot of people clicking on phishing emails, a lot of compromises going on from that perspective. Now the bad guys significantly ramped up their activity. So just at NFP alone, we saw a 5 X increase, just between March and April of last year, a 5 X increase in the malicious emails that were coming through our door.

So, that just shows you that the bad guys realized, "Hey, people are off their guard. They're off their game. Let's try to hit them." Even with some we've seen many times before, but they were hoping that the home environments wouldn't have all the same controls in place that they had when they were in the office. And I certainly get it. As an individual, like the rest of you that probably spent some time working at home, those distractions were real and made it real easy just to kind of get off track.

And the second thing we saw was even not from a technical perspective, but because people were out of their element, they stopped following their same processes. So the processes of approvals to do things and making sure that when they used to stand up on the cube and just kind of yelled at the person next to them, "hey, what do you think about X or Y?" That went away. So all of a sudden they were more isolated. They were forced to do things a little bit more independently. And unfortunately that led to some mistakes that also allowed people to wire money to places they shouldn't have without the right approvals. They were used to getting instructions from the boss that was across the hall. And now they didn't get to see the boss. So it seems like a legitimate email from my boss. I'll just go ahead and do it. In reality, it wasn't. So we saw a lot of that and really spike as well.

Jason O'Dell:

Yeah. And so talk a little bit about just ransomware and what it is, how does it work? What is this ransomware stuff?

Mark Grosvenor:

Ransomware is really kind of a favorite now for the bad guys. And it's interesting because what ransomware does is it's a virus or malware that gets somehow into your network. It could be from an email. It could be through a file shared that you download. It could be off of a website that somebody visit. But once it gets on your network, it basically starts to lock files. And it starts on the one machine that it gets on at first. And then it just starts to expand through the network, and to the point that this all takes minutes to a couple of hours. So it's not like it takes forever. And they might be set up on a timer and not start until a Friday evening when people are going home. So they have time to hit the various components of the network. And then each time somebody would log back into the network with their own computer, it would then pass it down to that one. But essentially it locks all your files. And if you want to get them unlocked, it'll pop up a little message and say, "Hey, call this number and we'll unlock your files." But it's going to come with a significant price tag to do so.

Even for our small businesses, we're finding that many of these bad guys will do research and they'll try to figure out what the revenue is. And there'll be looking for 20 to 25% of the annual revenues of a company to unlock their files. So what used to be a couple of thousand dollars has significantly gone up. And we've seen the numbers now, and even the municipalities are getting into the seven figures, over a million dollars to unlock files. And if you don't have a way to recover those from some other source, like we talked about earlier, you're in a world of hurt because all of a sudden you've lost everything you've ever had from a business perspective.

On the good news side. Usually when you pay the ransom, they're getting pretty good at unlocking the files. It's the business to them. Because if they don't, they know you're not... No one's going to pay if they find out that when they do pay, it doesn't happen. But the problem is by the time you realize you're going to have to pay, and you do end up paying, you still may have a regulatory requirement to notify because you can't guarantee they didn't take the files and they already have them, and they're going to release all your client information to the web.

So from a HIPAA perspective, you've got those regulatory requirements. So it gets to be very expensive. They're saying forget the payment to get it unlocked. Just the cost from your side for the forensics, on a small business can be over 125, $150,000. So it's a significantly large dollar amount that comes into play with these guys and they don't mess around.

Jason O'Dell:

And it sounds like it's not just big companies with big budgets anymore.

Mark Grosvenor:

You know, it's really not. Let's say that the attack occurs every 11 seconds. So the number of attacks that are happening in the United States is just crazy. And they say that it'll actually have your company down for about 19 days. So even if you agree right off the bat, you're going to pay, you could be without all your files for 19 days. You don't know when your next appointment is. You don't know who's coming in. You can't access the previous appointments to see what you did, what you prescribed, what you we're working with them for. So it's a huge inconvenience, and it's definitely a business impact that you're seeing. And like I said, just from a dollar amount-wise, we've seen those numbers go up so significantly over the past couple of years that it can almost be to the point that businesses can't recover from it. They can't afford to pay it and they can't afford to recover from it if they do. So it's definitely a significant issue.

Jason O'Dell:

And then it doesn't seem like there's a silver bullet out there that completely protects the company. So give me some thoughts or suggestions on what small medical practices, small businesses out there can do that have the best protection that they can afford. What are some of those ideas?

Mark Grosvenor:

I think if you look at it from a standpoint of, Jason, 95% of the issues are human error, right? And unfortunately that is the weakest link. The systems themselves have gotten pretty good at kind of blocking what it is, but the bad guys prey on the individuals in the company. And they basically with all the locked doors and everything else that they've got around them, or the chain link fence and the barbed wire, they just talk you into opening the door for them. And then all of a sudden they come in and once they're in through the chain link fence and the barbed wire, they have full unfettered access to all the information that's out there.

So number one, I would say that businesses should all know, where is your sensitive information, right? Where do you keep it? Who has access to it? What are the avenues to gain access to it? Can it be done from an off-premise perspective? Are there only certain machines that can do it, certain log-in IDs, et cetera? I think number one.

Number two, you need to make sure that all of your employees are using a password best practice. I can't tell you how many people that we found even within our company, right? That we have to change your password every three months. And so they'll go through and do something along the lines of, "Hey, I'm going to use spring 2021. And I'm going to use summer 2021, fall 2021." And the bad guys know this. They know those same propensities that we, as a human race are lazy when it comes to passwords. And it's hard for us to remember them, so we try to make it easy for ourselves, but we're making it easy for the bad guys too.

So definitely go on the long complex passwords. And require that your employees also don't share those passwords with any other sites. Like we mentioned earlier, we've seen Home Depot and Target, Marriott. Some of these companies that have lost email addresses and passwords to their sites. And if your employees are using the same password across all of their sites, it doesn't take them long to figure out, "okay, well, you were using mgrosvenor@nfp.com as your email address for your Marriott account, let me go try to log into your NFP account with mgrosvenor@nfp and that same password." And all of a sudden, now they have access to that as well. So super important on that front.

MFA, the multi-factor authentication, which is when you try to log into something with your username and your password, the next thing that you have to do is enter your four digit code on your phone or something in order to make it go through. I can't emphasize the importance of that enough. And I would make sure that all of your business systems have MFA in front of them.

Document the process as far as when people should be accessing sensitive information. So that you're sure when they should be achieving it. So the systems can start to be programmed to say, "Hey, this is somebody accessing our sensitive information at 3:00 in the morning", which happens to be perfect business hours in Eastern Europe, but it's not a business hours for you.

Train your employees. Make sure that they know what fishing is, excuse me, and how to stay on top of those things. Cyber training is extremely important. It doesn't take much when you're talking a couple hours a year, but you can keep people very well abreast of the things they should be paying attention to. And I can't emphasize that enough.

And then finally, I would say, making sure you have a good cyber insurance coverage. Being sure that you've tailored it to your business to know what kind of losses can you expect, what kind of information do you have, and work with an individual that's in that space that understands the cyber insurance space that can get you the right coverages to protect your business.

Jason O'Dell:

Great. That's great tips for the business and what they can do. What are some tips you think for personal, for individuals that they can utilize to not be hacked and, or become a victim of any identity fraud?

Mark Grosvenor:

Well, there's... A lot of it's the same. I mean, there's a lot of overlap there. I mean, again MFA, the multi-factor authentication. I tell this from my parents to my coworkers to people I've consulted with is, "Look, if any of your financial institutions, whether that's your bank, your insurance, your medical stuff, if the access to your information doesn't require MFA, or they don't offer that as an option, change." There's so many banks and so many insurance companies out there that do it. You should be making sure you're using those companies that provide that protection for you. So that's the first.

The second is the passwords. The same thing, not sharing passwords. I mean, if your USA Today account and your Wall Street Journal, and maybe your Pinterest account, if you want to have those have the same password because there's not a financial loss issue to keep those easy to remember, that's fine. But your banking accounts, your insurance accounts, your medical accounts, your educational accounts, those should all be unique passwords for that individual thing. And I get the question, "Well, that's awful hard to keep up with all those unique passwords." And so I would strongly recommend using one of the password managers. They're great tools out there that have some really good capabilities to help keep all of your logins secure, whether it's LastPass, 1Password, KeePass, Dashlane. You can Google password managers and you'll see the top 10 top 15 of them pop up. They're cheap. They're anywhere from a couple bucks a month to call it $40 a year. So nothing as far as cost goes, but they do provide a significant amount of protection.

Public wifi, making sure you don't get on the public wifi and do sensitive things on public wifi. You'd never know where that public wifi is really connecting to. So be very careful on that. And then, like I said, minimize the information you put out on social media, because while you may think it's minor, or it's not a big deal, it does give people information about you that you may or may not want them to have.

Jason O'Dell:

Right. About things from a financial perspective that can be done. What can we do from the financial standpoint to be better at not being infiltrated, hacked, or a victim of identity theft?

Mark Grosvenor:

I think there's a lot of things. I think number one is I would, I recommend everybody uses credit cards when buying things, not ATM cards. The ATM card you got tied to a bank account, there's a significant loss possibility there. And usually your banks don't have the same amount of timeframe that they allow you to report a fraudulent charge as a credit card. Credit cards give you 90 days in most cases where your bank's going to give you 30. So if you've missed something, you're busy, you're traveling, just happens to come at the wrong time and you don't notice it right away, it might be too late by the time that you do, you just have a lot more recourse if you use your credit cards.

The second one is you can put a lock on your credit account. If you are in a position where you're not buying cars and buying houses and needing to have somebody go out and open up new credit cards to where you have somebody hitting your credit accounts, you can lock them. You can go to the three credit agencies. You can actually go to one of the credit agencies and tell them you want to lock it. And that would mean no one can open up any new accounts under your social security number without them calling your cell phone and you giving them your password or your pin. So I highly recommend people consider doing that thing. I think it's super important.

And then if you haven't logged into the social security administration website and set up your login ID, you should do it before the bad guys do it. May never be social security payments when we all retire. We don't know, of course, at this point, but at this point it looks good, so I'm hoping they're going to be there, but you should be the one that gets the benefit of them and not the bad guys. But if you don't log into it, the bad guys might try to impersonate you and go do it. So I've seen a lot of people try to hack that and really get that set up to where, when they go to get their social security benefits, somebody has already started claiming them, et cetera. So I think that's important.

And then just the basic shredding your info and making sure that you don't get phished or spoofed by bad emails. Like I said, you know the websites to go to, go out there yourselves. And password-protect your phones. There's more information on those than people ever realized. And lost devices are a huge contributor to financial identity theft just because all the account numbers that are on there, your email accounts go there. They have full access when they get your phone. So if you password-protect it and make it lock in less than a minute. That way you don't have to burn out if you leave it in the cab or set it down on the bathroom sink in a public bathroom, and you walk off the next person coming in doesn't have time, and if they do, it's already locked before they get it. That's more than you wanted, but there's a lot of things in there. I think there's just, there's a lot of good opportunities for people to find ways to really help keep that to a minimum.

Jason O'Dell:

That's fantastic. And again, Mark, I want to just thank you. This has been super educational, and certainly appreciate all of your time. And I was happy that I got to be a guest host, so thank you for your time. I appreciate it.

Mark Grosvenor:

Well, thank you I really enjoyed it. I appreciate the opportunity to be on with you, Jason. Thank you.

Jason O'Dell:

Thanks.