Cyber Security Insights: Safeguarding Your Assets in a Digital World

0:06 Megan

Financial wellness includes the ability to manage money in a way that gives you peace of mind and empowerment to make your own choices. At Golden 1, we're here to help with unbiased financial guidance. As a not- for- profit member owned credit union, our main goal is to help you reach financial well-being. Join us as we discuss why financial knowledge matters and how to apply it to your financial journey. Together, we can be golden!

Hello and welcome to the Golden 1 Financial Wellness Podcast. I'm Megan and joining me today is Multimedia Producer, Dominic, and Director of Fraud Services, Ken. Thank you so much for joining us today.

0:49 Dominic

Hi.

0:49 Ken

Hi. Thank you.

0:50 Megan

All right, great to have you all here.

I know in our modern, highly connected digital world, cyber security is kind of the name of the game. And it's all about protecting our computers, networks, and digital stuff from sneaky folks who kind of want to get in, cause some trouble, or swipe our data. But one of the big headaches in this world of cyber fraud, where those bad actors use all sorts of tricks to kind of scam individuals or organizations or systems for money or other shady reasons.

So, in honor of International Fraud Awareness Week, which runs from November 12th to November 18th and International Computer Security Day on November 30th, I've asked Dominic and Ken here to help us discuss strategies and some ways to kind of spot those intruders. So that way we can all stay safe in the face of all these new and tricky threats.

So, Ken, can you share with us some of the latest trends we should be aware of?

01:59 Ken

Yes, absolutely. So, you know, there's probably too many to name in this podcast, but obviously, we want to touch on the ones that are in heightened awareness right now. So, you know, one of the biggest ones we're seeing is account takeover, which is a form of I.D. theft. And that's really where a fraudster or bad actor steals your personal information, such as your login credentials and then tries to make changes to your account and essentially lock you out and and drain your account. So that's one we're definitely seeing a rise in. We're also seeing a lot of elder and dependent abuse. This target population is really on the rise because of the funds available to them. They have a lot of wealth in in the industry and so they're they're a target for social engineering. And then one of the biggest ones we're seeing and it's been on the rise for the last few years, are scams. You'll see anything from romance, lottery, job scams, puppy scams, and even traditional computer virus scams. And, you know, that's partly on the rise, too, because of A.I. and chat about it. Things look more real now than ever before. So, you know, in the past you had poor grammar to kind of alert you to. This email doesn't look good, but, you know, it's it looks really professionally done now. So those are ones we're really on the lookout for.

03:33 Dominic

Thank you, Ken. So, one thing I also wanted to touch on are vulnerable populations. So I've previously worked within the IDD community, the intellectual developmentally disabled community, and I've noticed that there are a lot of individuals, folks there that have been affected by these cybersecurity issues because sometimes they may not realize or they'll have a conservator kind of make these decisions for them, and then when they receive something that may be, fraud related, they might not be able to recognize the signs. And I also recognize that elderly population, like you mentioned earlier, are also kind of like a prime target for for fraud. Are there any other populations that, you know, off the top of your head that vulnerable to these types of fraudulent practices?

04:20 Ken

Yeah, interesting enough, it's our younger population. You know, they've grown up from the beginning of their lives with technology and and there's a certain comfort level. They have almost, you know, to the point of being targets for it, where they click on, you know, the the newest app or the text message that they get. So there's a lot that our younger population needs to to learn how to protect themselves because they become a target as as they've grown in size and as they're starting to enter into the age where they have more funds available, making them an even bigger target.

05:01 Megan

Now, in terms of understanding these fraud scams, what kinds of fraud and scams are out there?

05:08 Ken

They take various forms. But, really what what fraudsters try to do is they they use psychology to really manipulate the victims and into tricking them to make security mistakes or giving up their personal information. And they do this in two primary ways. They either create trust with the victim or fear. And both of those ways are very effective because they're they're preying on, you know, the emotions of the victim to take that advantage. So, for example, you know, those become very easy, especially with social media, where people start building up these relationships and the fraudsters are very patient and they'll build up this, you know, relationship for you and then, you know, come at you and say, I need money for a surgery and victims at that point, they're so emotionally involved, they're willing to do that and become victims very easy.

And then fear again is a very emotional aspect to, you know, be taken advantage of. So I think a lot of us have always heard, but it's still predominant within the industry is you get the pop ups and you have a virus on your computer and, you know, next thing you know, you think you're talking to Microsoft Help and you know, they're going to put the software in to get rid of that virus and instead they put malware on your device and get all of your information and they start access in your account that way.

So, it's really, how they prey on your emotions and how they take that advantage over you.

06:44 Megan

Yeah, I know that there is, or rather can be, some really serious consequences to kind of falling victim to some of these scams. I mean, if you're responding to phishing emails, well, you risk giving away personal info or money. And you're right, people might try to trick you into downloading malware that can kind of mess up your device. And then answering those, you know, smishing texts, those text messages that we get, they can lead to financial scams or unexpected charges on your phone bill. And that also might invite some viruses onto your phone. And then, of course, all those phone call scam, we know there's a multitude of them out there right now, and they can really trick you into giving away your credit card info or those personal details leading to a kind of financial fraud or even identity theft.

And you're right, a lot of times they're also they're trying to intimidate you into kind of complying with their demands. But we also, on top of all of that, we now have this. I wouldn't say new, but a rise in QR code scams, too. And that can really affect our devices and they can use them to kind of steal our personal info and potentially, you know, lead to more financial loss.

So, Dominic, maybe you can expand on this a little bit too, but with all of these scams, we really need to increase our vigilance. So, what are some of the ways that we can identify these attempts of fraud and scams and kind of stay ahead of them?

08:19 Dominic

Yeah. Just from my personal experience and kind of teaching the bare basics of cybersecurity, I've noticed that when we run into situations of social engineering, we're kind of the best advice has been to always slow down, try to bring yourself to kind of like an emotionally neutral position and if possible, kind of verify who's who's trying to kind of, you know, get the information from you.

I've heard kind of like from financial institutions, especially like Golden 1, right? There are specific pieces of information that the companies don't ask of you. So can you give give us some examples of what information a legitimate company, business or financial institution wouldn't ask of you.

09:02 Dominic

Yeah. I think you, you know, nailed it on the head there that you know there's so much more sophisticated now when they use the examples that Megan just said about be it phishing or smishing that they they look so much more like a legitimate financial institution. But but really if you have any doubt, if it looks suspicious and you haven't done anything, then don't click on that. Right. Pick up the phone, go to, you know, log in yourself directly and avoid clicking those links. I mean, that that's really one of the safest ways. This is not, you know, going straight to that that instant click and moving on. And I know in today's world we all want that faster response to it. But at the same time when when we're sending you something legit, it's in response to something that you've done. So, for example, if you, you know, have just done a transaction and you receive an alert, that's going to be more legit. But if you're sitting at home and just received a text saying, you need to click this link and log in to this site and you haven't done anything recently, be suspicious of it. It's all about the timing of of these things. And so as Megan said it, and it can take any form of that. It could even be those phone calls where the bad actors have really been well coached and and get you to do that. But if even on a phone call, if you just feel that in your gut and at the end of the day, that's the best thing to trust, go ahead and disconnect that call and pick up and dial the financial institution directly and verify yourself.

10:51 Dominic

Yeah. And I'd also like to kind of add in here. There are there are also examples in situations, actually an unfortunate one I, I personally know of is a relative of mine got a phone call from someone claiming that they've kidnaped their their loved one and that if we didn't comply with “x” demands, you know, they would, you know, do something awful to that. That person in these situations, what would you recommend for that person to do just because it is such a an emotionally heightened moment? Right. That kind of comes out of nowhere. What what would you recommend? You know, if someone, one of our listeners, was put in a similar situation, how should they respond to that?

11:33 Ken

Well, you know, especially if it's a you feel it's a threat against a family member. Again, immediately disconnect that and either reach out to you know that in that case that family member or law enforcement and benefits of financial aspect of the threat contact again the financial institution directly. And I know it's easier to say when you're in that emotional moment, but the fact is that's what they're trying to take advantage of. It's even getting further away from a person making that threat. They're starting to use A.I. to mimic some of those threatening phone calls. I think there's been a few press articles where they sound very legit and I get that. But at the same time, make sure that your people are safe. You're safe, and do those checks

first. And again, engage law enforcement in the financial institution as quickly as possible. That's your best bet to potentially stop and and or even catch those bad actors.

12:38 Megan

Yeah, I know that, you know, this social engineering, it's really just a mind game that scammers are playing and they're using tricks to manipulate our trust and our emotions for their shady purposes. And it's all about us really getting to spill the beans, if you will, or do things that we shouldn't do. But it's also important that we're aware of different techniques and prevention to help protect ourselves. Now I know Golden 1 Credit Union, we pride ourselves on security and providing for our members. What are some of the things that Golden 1 is actively doing to keep our members secure?

13:16 Ken

Yeah, that's that's a great point, because at the end of the day, it's a joint effort. We're doing what we can to keep everybody educated, such as this podcast. We want to make sure that people are aware of the trends and aware of the latest trends because again, they're taking, you know, trying to get those emotional responses from you. So, you know, it's all about recognizing, hey, I've heard this on a podcast or I've read this on the Golden 1 site, so, you know, some specific things we do. We're we're constantly monitoring the accounts and and we will in a legitimate way that you've set up either through an alert or for a phone call of contacting you. If we detect unusual activity. And with that, we can verify it. But we also have and we've updated our Member Security Resource Center, where we give tips and examples of current trends for you to to reference yourself and see what's going on in there. And then finally, we've also provided opportunities where you can go into your account and self-service your activity, because again, monitoring your own activity is the best way to see if something has happened. And if you see a transaction that doesn't look legitimate, we have the ability on your debit, credit, or ATM transactions to to file that claim right. Then and there. And then we can take action before other fraudulent activity takes place. So we really want to make sure that you have those immediate tools at your disposal on there. But, it's really keeping yourself current on your account and and knowing these type of trends that go on.

15:08 Megan

And, you know, even with all of these measures in place and even with us being diligent about monitoring our accounts, there's always a possibility that we do fall victim. So, if you've been scammed and there were financial transactions involved, the first step, as you mentioned, Ken, is really just to get in touch with your financial institution, report that incident to them immediately. That way they can help you freeze or close the compromised account, investigate that fraudulent activity, and potentially reverse any of those unauthorized transactions. And of course, in case of scams that involve theft, fraud, cyber crimes, that's where you really might want to step in and file a police report. So, make sure you contact your local law enforcement agency and provide them with all of the details of the scam, because that report can be valuable for any potential legal actions and can help authorities track down scammers.

16:12 Ken

Absolutely. And and even before that, you know, we offer a lot of tools that you can, you know, use yourself to help prevent a lot of fraudulent activity even if someone tries to scam you. So, you know, for example, use a biometric based authentication tool, you know, on on Apple, it's a face ID or Android, it's your fingerprint. And that's a great way of using those log in opportunities to prevent fraudsters from jumping in. Or you can set up two factor authentication and where you receive a code, either a call or attacks to log in.

So again, if your information is compromised and a fraudster tries to use those credentials, they'll be blocked by that. And then, you know, another great thing is setting up alerts. You can we have the opportunity for you to set up account alerts which would talk about your balances on there if if you start to see any activity there or overall security alerts. So if there's a password, email or security questions, if those have been changed, which is typical of fraudsters trying to take over your account, you'll get an alert for that. When those changes are being made so you can stop before activity happens. And even card transactions, you can put up alerts where, you know, different transaction types will will send you those alerts and you can be prepared to contact the financial institution before hand, before more transactions take place. But but, at the end of the day, the importance of of doing all of those activities is to not only protect yourself, but, you know, the more we all work together, the harder it is on these bad actors to take these opportunities. And that's really where we win together by by making sure we partner on this.

18:07 Megan

Absolutely. And all those security factors, all those alerts, all of that is so important and key to helping us keep on top of these attempts at fraud. I just want to add another way to protect yourself is to protect your credit and prevent scammers from opening new accounts in your name. To do that, you might want to consider freezing your credit report with major credit bureaus like that of Equifax, Experian and TransUnion. You can also add fraud alerts to your credit reports as well. And once again, it's just another layer. It just makes it harder for scammers to use your information to get new credit. And you can do that simply by contacting each one of those credit bureaus and putting those alerts and freezes on your credit reports.

It's also important to just keep a close eye on your financial accounts for suspicious activity. Make sure you're reviewing your bank statements, your credit card statements, all of your financial records regularly, and take advantage of your free annual credit report available at annualcreditreport.com. Once again, that's annual credit report dot com, because this will allow you to check your credit history for any unusual or unauthorized activities. And if you spot anything suspicious, make sure you report it to those respected financial institutions as well as your credit bureau.

19:34 Dominic

And one thing I did also want to add on there, Megan, is all of this talk about frauds. And, you know, if you've gone if you become a victim of them, I think it's important to emphasize that it's there's no shame in that that this kind of thing can happen to anyone. And as Ken has

mentioned several times, the complexity and ability to spot these these frauds are getting more and more complex every year. So I just kind of wanted to wrap up and talk a little bit about some proactive or preemptive things our listeners can do to kind of help, you know, prepare them for for these for these frauds.And I wanted to really quickly talk about strong, unique passwords. With with passwords. I know there's kind of a like unsaid joke that people will pick like one one password and use it for everything. And because it can be difficult to hold multiple different passwords with different mentally. Ken, do you have any suggestions for people that may want to still stay secure and stay safe? But also may struggle with, you know, maintaining all of these logins for different accounts.

20:46 Ken

You know, with strong passwords and unique, you can you can make those really where they are things that resonate with you, but they are unique. And I know that gets challenging when there's, you know, 50 different applications and things that people have to log into and in this day and age. But it really is important that you think about the importance of this being your your money. And that's that really requires that attention. So, you know, it's one of those that pick something that's not easily forgettable and but more importantly is unique to you and and modified in such a way that can be in reverse engineered at some way.

21:34 Dominic

Got it. And another thing I also know we we briefly talked about was being careful with links and opening attachments. I want it to reflect really quickly. I, I actually got a fraud related text message for Golden 1 a few months ago where I was given a link shortener and if I hovered over the link I could see in the URL that it was clearly not a golden one website. Are there other other tips or tricks that you can provide for for people to be cautious about links and attachments?

22:06 Ken

Yeah. What you did is perfect. I mean, in an ideal world and I do that my, the same way but again I think we're a little closer to it. It's easier for us to say but but again, if it just doesn't feel right to you, then don't click it. Login directly to your account. I've done that before when I've received links and it's again, trying to, you know, tug on your emotions that something's wrong with your account. Don't don't click the link, go directly to your mobile application or go to the website and log in directly or, you know, even call if you have to. Either way, you know, if it just take that extra moment to really think about what it is asking you to do and and you know, why would it be, you know, coming to you that way if if you're not doing anything, essentially its an unsolicited type text. So, so it it's again, taking that extra moment, take a step back and slow down and really, you know, think before you click.

23:18 Dominic

Got it. And my last thing was more of the lines of browsing securely. I know public internet and public Wi-Fi is a really common kind of service that a lot of businesses provide. Do you have any best practices for how to make sure you're keeping how we're keeping our financial information secure while maybe perhaps using the web in public areas you know, a member goes to the library use a public device, do you have any kind of best practices for making sure your information is still secure?

23:49 Ken

Yeah. Again, make sure that you know as much as possible. Try to use your known devices and that you are keeping them up to date with either updates or that you have third party security on there if possible. But if you are in situations where you know it's a public website or public wi-fi, where you know, you're not quite sure, I mean, think about using your phone as a hotspot if possible. If not, maybe wait until you're to a wi-fi that is more known and secure on there. So again, it's it's one of those you you really want to know as much as possible. The method you're going through. But and again logging in through your known devices as is usually the the best method there and and trying not to use devices that multiple people might be using and provides opportunities for malware on on those devices as well.

24:52 Dominic

Awesome. Thank you, Ken.

24:54 Megan

I just want to reintegrate here scams, fraud, it can all really hit our wallet in our privacy hard if we're not careful. So, just remember to double check the source, avoid sharing sensitive info and just stay vigilant when you're dealing with unsolicited messages or calls.

I want to thank you so much, Dominic and Ken, for being here to share with our listeners the importance of staying safe and secure.

25:21 Dominic

Thank you for having us, Megan.

25:22 Ken

Thank you, I appreciate it.

25:24 Megan

If you haven't already done so, subscribe to the Golden 1 Financial Wellness podcast on Apple, Google and Spotify to get more financial tips and insights. Plus, go to the financial wellness tab at Golden1.com to find a ton of other resources like videos, interactive modules and webcasts.

Explore our Learning Lab and use the ID Theft Risk Tool to help you assess your risk level for fraud and identity theft. You'll also find a wealth of knowledge in the articles section of the lab, as well as some informative videos and infographics.

So once again, thank you for joining us today. This has been Megan

26:03 Dominic

And Dominc

26:04

And Ken

26:05 Megan

wishing you financial, health and happiness and as always, reminding you to

26:11 Megan, Dominic, Ken

stay golden!

26:17 Megan

Golden 1 Credit Union is insured by NCUA.