COMMUNITY CONNECT VIDEO 2 ENGLISH

The following workshop is presented by Capitol One approve and American Library Association through the community connect grant. This workshop is designed to teach you how to use online banking services. For privacy reasons the chat has been deactivated. If you have any questions on the subject send us your questions using the link in the description that you will see below. We also ask that you answer the survey questions found in the description. In order to obtain more grants in the future, access the survey by clicking on the link titled survey. Thank you.

Hi! Good afternoon everyone, I hope you are well, I am very pleased to meet you and welcome to the second session of the Yuma library program to improve our understanding of banking services. He may be sharing some videos with you. I want to start this imitation with you folks here for a moment.

Thanks for your patience, ok.

So we have here the presentation. We are going to start we are going to have the presentation this and we are going to be watching the presentation, we are going to be watching some videos, we are going to be having some interactions. And some things that I want that you do not have that I am here available for you at the end to answer any questions that you may have related to the topics that we are going to talk about today. Again, thank you very much for being here, welcome. A little about me, my name as I say is Francis and I am from Tucson. I love connecting with my Hispanic roots. My parents are here on the right side, my mother and father, born in Sonora, Mexico, and we are here accompanying them, here I am. And I am accompanying them with my two adult children. In the middle of the photo of the center, here I am with my husband, we were on vacation, I don't remember where we were but it was a crib, as you can see here, it was an adventure. An adventure and here I am alone on the left side. I am here to really support you within this within this process within the process of learning all and within the process of improving our understanding of the banking system. I can tell you that my dad, who is here on the right side as you can see, is a traditional Hispanic and it took him a lot of battle to have confidence in the banks to some extent. Confidence in the banking system so that in the United States, which is very different from that of Mexico. But now he is in a much better position where he feels comfortable with that process and with and with what the bank offers for sure.

Today we are going to be talking a little about security and protection in banking services through the internet. Some of the things that we'll talk about include:

• The importance of bank security.

• How banks confirm our identity

Because maybe there is some, some concern, how they are going to verify that I am someone else can go and get my money or things like that, we are going to confirm and we are going to see how the banks trusted our identity.

• Bank communication practices

How the bank communicates with us

• How to spot a scam

That it is something real that could happen that sometimes mortifies us.

• Learn to identify suspicious activities

It is very important we have to make sure that we know how to detect this suspicious activity and we are going to learn how to do this today.

Again confirming that the last 15 minutes we are going to reserve for any question, any concern or comment, I will be available to you.

So the importance of bank security.

I want to ask you: What are some of your concerns with online banking?

Why are there concerns? There are always concerns no matter if you are Hispanic or American or Italian. We all have questions or concerns at times. So I want you to reserve that question, what are some of your concerns with internet banking services, you have to reserve this question because if there are still concerns after this presentation, you have to talk about those concerns or those concerns that you have. I also want to do a kind of survey with you. Has anyone been a victim of fraud or do you know someone who has been a victim of fraud? Sometimes when there is, we can have some mortification. We can have some mortification related to using banking services. Others are going to give you support to alleviate some of those concerns that you may have. I want to thank you again for being here. And I want you to think about the mortifications are concerns that you have. What we are going to do is we are going to watch a video that explains how banks are 100% committed to keeping our information safe. It is a video that we are going to see it is a short video the video that we are going to see that is short is only a few minutes long. I think it's more is like a minute long. There is this video. If you have any concerns, you want to see these videos again or you want more information, you can always go to this internet site readysetbank.org and within this site you can find a lot of information. Information about online, about non-profit resources, learning tips, news and if you download here, there are some videos that you can also see are all in Spanish. But we are going to the first video here that we are going to be watching for a minute, ok I am going to maximize it so that you can see it comfortably.

Okay.

I know what I'm going to do to turn on the video, I'm going to turn off my camera and microphone so that they can have a better, better ability to really listen because I don't want them to hear something that is happening back here recording Sergio or something. Once I put a video they will see that my screen turns off but then I reappear. Ok, let's start again a very short video.

Video:

Banks are committed to keeping your information and money safe. They are prepared for different types of risk and have configured security features directly on their systems. This is because banks have a vested interest in preventing fraud. So they rely on many strategies to keep their finances safe. For example, identity theft is just one of a series of threats they protect themselves from. This type of theft can take different forms. Like someone trying to gain unauthorized access to your account or someone with malicious intent by obtaining your credit card information or password. Avoiding these threats is as important to the bank as it is to you. Banks are working to strengthen their data systems to protect them from attempts to gain unauthorized access to your information. To stay one step ahead of threats,

go upstairs as long as you don't pull your four normal shopping nests. Your bank will edit it so suspicious purchases are observed, activities that seem out of the ordinary for you, such as a transaction for a very high amount, or a new activity in another country. And protecting your account helps banks avoid damage.

[Music]

we are going to leave this video here and go back to the presentation. Ok, so we saw those concerns that you guys had. We have them, we are thinking about those concerns that you may be processing at this time. And also identifying how we can be sure.

Now, according to us, we have to see security and see how it is taken more seriously. So my question to you is what are some ways that you can take to protect your accounts?

One of the important things is that we have to know that while banks have a responsibility to keep your money and information private and secure, we also have to do our part. So what methods do banks use to keep bank accounts safe?

They use something called encryption to protect the accounts. Multi-factor authentication. So they want to make sure that the people who are accessing the account have the ability to access the account. That they have the right type of access to the account that are people who are recipients of this money.

So some ways you can take to protect your accounts, which include those four, what options do you have? You can really be quite careful about giving the pin number or information to people you don't trust. To people who are not within the account. It is recommended that you check your account and report suspicious activity at your bank immediately. What I like a lot about using the bank is that if I tell the bank about these suspicious information and suspicious charges, the bank typically supports me and can help you rectify that. Do I find out again so as not to be struggling when we have cash we do not have that same ability if they lose 100 dollars are lost. We can't get the money back, it is a little different with the banks. Quite different with banks. So in addition to protecting, they also want to confirm your identity. We have just reviewed the banks' commitment to keeping our information secure. But in this next video, we will review how banks confirm our identity, how they do it, how they can confirm an identity, and at times it can sound like a bit of a foreign concept. So let's see a little bit in this short video, this video is just over two minutes away. I think like two minutes 50 seconds. Something like this, we are going to see this video of how banks confirm our identity. I'm going to open up here and we're going to see this video.

Video:

Now, according to us, we have to see security and see how it is taken more seriously. So my question to you is what are some ways that you can take to protect your accounts?

One of the important things is that we have to know that while banks have a responsibility to keep your money and information private and secure, we also have to do our part. So what methods do banks use to keep bank accounts safe?

They use something called encryption to protect the accounts. Multi-factor authentication. So they want to make sure that the people who are accessing the account have the ability to access the account. That they have the right of access to the account that are people who are recipients of this money.

So some ways you can take to protect your accounts, which include those four, what options do you have? You can really be quite careful about giving the pin number or information to people you don't trust. To people who are not within the account. It is recommended that you check your account and report suspicious activity at your bank immediately. What I like a lot about using the bank is that if I tell the bank about these suspicious information and suspicious charges, the bank typically supports me and can help you rectify that. Do I find out again so as not to be struggling when we have cash we do not have that same ability if they lose 100 dollars are lost. We can't get it back, God is a little different with the banks. Remove different with banks. So in addition to protecting they also want to confirm your identity. We have just reviewed the banks' commitment to keeping our information secure. But in this next video, we will review how banks confirm our identity, how they do it, how they can confirm an identity, and at times it can sound like a bit of a foreign concept. So let's see a little bit in this short video, this video is just over two minutes away. I think like two minutes 50 seconds. Something like this, we are going to see this video of how banks confirm our identity. I'm going to open up here and we're going to see this video.

We are going to continue. We saw this video, I loved the video as it gave all the specific information on how they can confirm our identity. The types of uses that they use that are multifactor types, such as the password to put our pin or if we are doing it online, put our password that we have to use. For your card, normally there are four numbers that we use. If it is by means of four secret numbers. So it is through the computer features also use our mobile phone. If we call from our mobile phone they think it is us and ask us more questions about our identity. Or if we use our mobile phone to enter the site they recognize that it is our mobile phone. If they ask us for more information but it is a factor, they use to confirm that it is us. Some user features now with phones come with a button and grab our fingerprint. So unless someone has my own fingerprint, no one can enter my account other than that. I like it very much, I feel very safe with this option with this fingerprint.

Why do banks use three types of multi-factor?

They use these three types because they really want to make sure that you, the person who is accessing your account who is accessing your money, is not a scammer who might only have part of your information. So scammers only have part of my information, not all of my information. We always want to make sure that our websites we are using, are safe. We have to be on high alert to our surroundings to ensure that someone in the public will not want to access this information when we are accessing it.

And now what we are going to do we are going to go to a video that talks a little about, about communication practices. Let's see how the banks communicate with us. Let's see this short video, it is very fast.

I'm going to do it, I'm going to ...

[Music]

I will start here.

Before this video begins what I would like to do, I would like you to use some reactions, for example a heart we see here on the left side or we can use an explosion. We can also use the thumbs up. I want you to do that if you guys have used some kind of pin in the past. What does it mean like that four-number password? Or a password on the computer I want them to use one of those reactions. In any

place for example we are going to put the example, a simple example. For example, sometimes we have a card to go to the Safeway that gives us a discount. But we have to put our keyboard on our phone number is like a kind of pin. Or if you go somewhere they give you a card but you have to memorize your pin number to access something or something like that. Any of those type of passwords and you have used it, I want you to use your thumbs up icon or to put a heart as a reaction again. We can make it a bit interactive. I want to thank you for continuing with me. Maybe now I am going to share once again and what we are going to do we are going to see this video, although it spoke a little about communication practices with our bank.

ready ..

Video:

Either you or your bank initiate the communication. Knowing what kinds of details you might be asked can help you be on the lookout for potential scams. This applies to phone calls, emails, and text messages. Let's start with the communications you receive from the bank. There are routine reasons why your bank might contact you. For example, you might need to confirm whether it was you who tried to charge your account. Or alert you to some activity on your account that seems unexpected or suspicious. When your bank contacts you, their goal is usually to give you notices. They should not ask you to share personal information in an unsolicited text message, email or phone call. If you are ever asked for any of these details, avoid giving them. Since it is a sign of a possible scam. If you have questions or something seems out of the ordinary, find your bank's customer service number and contact them. When you initiate communication with your bank either by phone or by email, they may ask you for some types of information to verify your identity. Like your address or your date of birth. This helps to look up your account details and confirm that you are who you say you are. In this way the bank can give you all the information you need. Whether you have contacted your bank by phone or email, you will be asked to verify your identity by providing your account number and you may also be asked to answer some of the security questions for your account. You should not be asked for personal information such as your password for banking services or your edit pin. ATM if any representative deviates from these standard practices and asks you for private details like these, it is a sign that they might not be trustworthy. By staying alert to suspicious questions or requests, you can avoid the possibility of fishing, a tactic in which a scammer assumes the identity of a company and attempts to gain access to your account. If someone ever reaches out to you and suspects that the person you are speaking to is untrustworthy, simply hang up and visit your bank's website to find an official number to call. Just look for a link that says contact us.

Thank you for continuing with me, and thank you very much for being here again and we will continue. Let's talk a bit about this topic. When the bank communicates with us, how many of you have heard of phishing? This process really is a term used to describe any type. Any type of phone call, email or mail, such as when we receive letters, mail that misleads you into providing personal information by passing themselves off many times as a business or a financial institution. It is immediately a red flag for us to say to stop here, what is happening, why do they need this information from me? Let's see, what are some of the signals we saw here in the video? Create the sense of urgency. They create a sense of urgency that you need to give them the information then quickly so that they can take care of their money. Or because something urgent is happening. They present an urgent situation, but the bank would never do that. Then they ask for your personal information like your social security number or

your home address. They shouldn’t have to ask for that because the bank has that information already. Remember they are calling with a sense of urgency and asking for personal information. A phone call from an unknown number. Also an unknown number is something that mortifies us because they are calling us from an unknown number. It is important to know why this is happening. They are signs that we could be being scammed. We are going to see how to detect this scam, how we can detect it. We have covered a lot of information on how banks protect our information, confirm our identity, and how banks communicate so that we are not victims of phishing. The last two videos will show us how we can detect a scam and how to be alert to any type of suspicious activity in our bank. So for this, what we are going to do, we are going to see two videos. We are going to meet again later in the videos. I think after the first video, I'm going to take a little pause and then go back to the second video. We go to the first video this is the penultimate video for us.

Video:

Granny, I'm Miguel, how are you? Michael? Has it been so long does it sound different, older? Given a lot of time in short, well me, I'm in trouble. I'm in Chicago right now and some guys just robbed me. I need money to get home safely. Or not! And what happens is that I, I do not want my parents to find out about this so as not to worry them. Do you think you could help me? It is urgent! Banks do everything they can to keep your account safe. And that includes helping you identify scams like the one we just saw. This is called the Grandma Scam. And like other common plots, it follows a well-defined pattern. Knowing these tactics someone can use to cheat will keep your finances that much more secure. Scams take advantage of your natural tendency to want to help and follow the rules. They play with their emotions like fear and compassion. The goal is to pressure you into doing something that you probably wouldn't do under normal circumstances. Let's see how scams are typically structured. The first sign is when someone contacts you without your request. You get a phone call, an email, or maybe a dialog box, and usually suddenly. Often times, it is someone who looks legitimate. Someone like your grandson or your insurance company. The second sign is when the person tries to scare. You could pretend to be from yesterday and tell you that you are in trouble to intimidate you into information such as your credit card number or your bank password. Which brings us to the third sign. When they try to give you a sense of urgency. Something that you have to do immediately. They could tell you that your computer is infected and that a technician needs to access your files immediately. When the message is unexpected, scary, and urgent, these are clues that reveal that something is not right. So what should you do when you notice these signs? First, resist the pressure to respond immediately. Never send money after a suspicious request or share important bank details. Instead, hang up and contact someone you know is legitimate. Like someone from your bank in this case the parents of your grandson. If it is your bank, you can click the contact us link on their website and speak with an official representative. Some banks even have a link through which you can report suspicious emails. And remember, you should also be on the lookout for scams related to your phone or cable company. Not just with your bank account, scammers can use other accounts to find a back door and gain access to your bank information. So these plots are worth keeping an eye on, regardless of the type of information in question.

Here we saw a bit about how to spot a scam. What we are going to do now we are going to watch a video on how to watch out for suspicious activities. And I am going to open the video, we are going to put it. This video is a bit shorter.

COMMUNITY CONNECT VIDEO 2 ENGLISH

Video:

Knowing the common signs of online banking fraud is crucial. And it can help you keep your accounts and finances safe. You may receive an email asking you to share your banking information such as your username and password. Or there could be a charge to your account, even a small one that you don't recognize or remember making. You could even get a phone call requesting confidential information and not know how much safe detail to share. Suspicious events like these are usually missing alarms. But staying alert helps protect you and your finances in the event that there is a real threat. This is the reason why even if you are not 100% sure that the activity is suspicious, you should not hesitate to hang up and contact your bank to confirm the request. And remember to never give out information via email or a text message. Do not click on links that do not appear to be reliable. In these situations, the safest option is always to contact your bank as soon as possible for peace of mind. Check your bank's website for a phone number where you can communicate your concerns and ask questions. Look for a link that says: contact us or something similar. Have your account information handy as well as important details about the alleged fraud. Your bank may even give you an email address to which you can forward suspicious messages. This helps them decide if it is a legitimate threat that misrepresents any kind of phishing scams that may be circulating. In the remote event that your account is charged or fraudulent, your bank will likely offer you a provisional credit for the stolen funds if you inform them promptly. It should also offer you a full refund after you have conducted an investigation and confirmed the fraud. If you informed them shortly after it happened. You can get additional protection against scams like these by staying alert when entering your password in public places. Make sure other people cannot see your pin when you are in an ATM or in line to pay. And if your reporter debit card is ever lost or stolen immediately go to your bank. To familiarize yourself with your bank's security precautions, spend time on their website. There you will find a wealth of resources to help you understand how to respond to your bank if your account is ever at risk. Remember, at every stage of online banking, your bank is your most important ally in keeping your finances safe and secure.

And we all return together to our presentation. Let's talk a bit about these suspicious activities. Within our interactions and within our, our, our ability to learn a little more today about banking. We can see what other scams are out there. So calls or letters telling you that you owe money to the government, you won the lottery, or you won a giant prize but you need to deposit an amount of money as collateral. So that immediately tells us this is a scam. What if we are victims of fraud? What happens at this moment right? So let's talk a bit about this. What do we do in those cases? Okay I have been using my card to pay. This and I feel more confident with the bank but if someone used my card or an identity theft fraud, what do I do? We have to report the fraud to the authorities apart from clearly reporting it to the bank, and any credit agency. We want to call the credit agencies to report your account. And the bank can help them in all these circumstances,they do everything possible to help you. We identify some of the ways banks can prevent fraud. How banks prevent fraud. Banks do everything possible to prevent fraud. But what specifically do they do? They review any unusual charges. I'll give you an example. I was out of town in another state that I don't normally visit, and it didn't occur to me to call the bank to tell them I'm going to be in Washington. It did not occur to me to tell them then I go they see that you start on the card and suddenly it was time to use the card, and it was not accepted. The bank blocked it so I called the bank because I needed my card to pay, and they said oh, can you confirm your identity? I confirmed my identity they reactivated the card. They said we removed the card because we thought someone was using the one that was not you, because it was an unusual charge.

They encrypt our data. They encrypt our data so that no one can have our specific information. It is all mixed up like many numbers and characteristic letters. Both require identity verification in various ways. They don't just need to have a form, there are several ways to access your account. It is something that banks do that is important. Finishing a bit, a little about this, we are going to see that if fraud occurs, of course on these occasions, and if they communicate it to the bank, the bank does everything possible to investigate and reimburse the money so that it is whole again you and do not have financial problems. We know that there are people who will try to take advantage of you to rob you, but you now know three signs to detect this fraud. The sense of urgency, someone you don't know asking for personal information, or calls from unknown numbers. Also don't share your personal information with someone you don't trust. Like your credit card number, your pin number, the key, your social security number, none of that information needs to be given to strangers. In closing, I want to thank you all because you spent some very pleasant minutes with me learning a little more about the services with the bank. And what can we do with those services. I really want to reintegrate the three signs to detect fraud. And the importance of protecting your information is to protect this information which is very important. The summary within this this series we saw today the security and protection in internet banking services. The importance of bank security how banks confirm your identity, your bank's communication practices, how to spot a scam, learn to identify suspicious activity. Now what we are going to do we are going to continue and we are going to have a discussion for these last 15 minutes. And I will be available for you to ask and to answer any questions you have. Maybe I won't have the answer you need. But, if I don't have the answer, could I find a way to find that answer to pass it on to you. I was very happy to have met you all here and to have been with you in this presentation. Now we move on to the questions.

Questions:

Ok now does this mean that they can be heard? And perfect I see that some ...

[Music]

Or not.

Or not.

Or not.

Oh oh oh oh oh.

Ah.

Ah.

I think we had some technical problems, but I think they have been solved if they are not solved, the Yuma library gives us a warning. But I want to thank everyone for being here today. If I see that some people have questions about the information we just reviewed. And I wanted to quickly take a few moments to answer a few questions that you guys have. One of the questions I saw and it included questions about what is phishing? Phishing is like a type of hoax and the answer is yes it is like a type of hoax. It is a term that really describes any type of either a phone call, an email or some type of communication where they are looking for fishing in English means to fish. They are fishing for personal information about you. They want this information and they want it so they can scam you. So sometimes it is done in the form of is presented in the form of a known person or an unknown person.

But they always have that sense of urgency when they are asking you for the information. So this advice is that you monitor your accounts. Always see what charges are there because remember that when someone is trying to scam us using phishing they are really creating that sense of urgency. They are asking for information that is personal, information that they should not have like social security, pin number our full account number or things like that. And sometimes the calls come from an unknown number, we don't know the number, we don't know where it comes from. That was a question that was asked which is an excellent question. Another question they asked includes, what do I do if I see strange charges, what do I do at those times, what do I do? I have my pin and my account and it mortified me because to leave them there, that they should not be, then one of the most important things is to report to report to report to report! Why is it important to report what we see to be fraudulent, what we see to be inappropriate? So in those cases when we see that there is some type of theft or that there is a strange charge we call our bank to report this. If necessary we call our authorities, the police and go to any credit agency. Depending on the support we have from the bank. Many times when we call the bank to tell them, I have a very suspicious charge, a strange charge, and they help us determine if we made the charge or if we did not, they take action to be able to make us whole again. The bank will do their research and determine if it is a permanent charge, towards us, if not, they will credit that amount to us permanently. And they also give us a lot of resources in terms of calls in this case, it is highly recommended that the police get called, there are different things that can be done to ensure your safety. Most importantly, if we see strange charges, we can take action. If we have cash and it is lost, there is not much action we can take. We have many resources available to us. So another very excellent question thanks for asking. Another question I see is we are also at risk with the phone companies. That the risk we could that when we receive calls from unknown numbers immediately, it is like a red flag. Let’s see what are some of the signs we saw on the video? They try to create a sense of urgency when calling you. Or it can be presented through a call to our house or a call to our cell phone from an unknown number through the telephone company. It is always important to take precautions and it is important for us to make sure that we are always aware of what we share. When we see incoming unknown phone calls, we have to make sure we know who we are giving that information to. We never want to share our information to your social security number, credit card number, etc. with someone over the phone. Very good question, also another question that I think is also very good is a question someone asked, in what kind of services can I be scammed with? As it is a very open question but at the same time it is a very important question. Because any type of banking service can be copied, it can cause us to expose ourselves to pay a scam by mistake in any type of banking service. Either a deposit, a credit, or a check is to send a check to receive. And we have to be very careful because we can be victims of scam. But the most important thing to know is that banks do their best to insure and review charges and they are always seeing unusual charges here. If a charge is unusual, you can put a stop to the card because you do not want someone to use the card if they should not be using the card. I always want to make sure that the card is used and we are going to give access to the authorized people, the authorized people are the ones who will be using the card, not other people. I can see that I just do a quick check to see if there is any other question that I enter in these last seconds I see that I do not have another question. In general, I want to thank you again for being present at this session. I'm going to have another session on the 27th at 4 in the afternoon. So I hope to see you at that session. But I was very pleased to be your presenter and thank you again for being here and for taking such care to ensure that you have the necessary information and education. For making the transition to using banking services thank you very much and good afternoon.