# COMMUNITY CONNECT VIDEO 2

El siguiente taller es presentado por Capitol One aprueban y American Library Association a través de la beca Community Connect este taller está diseñado para enseñarle a usar servicios bancarios en línea. Por motivos de privacidad que el chat ha sido desactivado. Si tiene alguna pregunta sobre el tema envíenos sus preguntas utilizando el enlace en la descripción que verá abajo. También le pedimos que conteste las preguntas de la encuesta que se encuentran en la descripción. Para así poder obtener más subvenciones en el futuro acceda a la encuesta haciendo clic en el enlace titulado encuesta. Muchas gracias.

¡Hola! Muy buenas tardes a todos espero que estén bien me da mucho gusto conocerlos y bienvenidos a la segunda sesión del programa de la biblioteca de Yuma para poder mejorar nuestro entendimiento relacionado el ser los servicios bancarios. Puede estar compartiendo a una forma unos vídeos con ustedes. Quiero empezar esta la imitación con ustedes gente aquí un momento.

Gracias por su paciencia, ok.

Entonces tenemos aquí la presentación. Vamos a empezar vamos a tener la presentación esta y vamos a estar viendo la presentación, vamos a estar viendo algunos vídeos, vamos a estar teniendo algunas interacciones. Y algunas cosas que quiero que no tienes que estoy aquí disponible para ustedes al final para contestar cualquier pregunta que ustedes puedan tener relacionado a los temas de los que vamos a hablar el día de hoy. De nuevo muchas gracias por estar aquí bienvenidos. Un poco sobre de mí, mi nombre como les digo es Francis y yo soy de Tucson. Me encanta conectarme con mis raíces Hispanas. Están aquí mis papás al lado derecho mi mamá y mi papá nacidos en Sonora México y estamos aquí acompañándolos aquí estoy yo. Y estoy acompañando los con mis dos hijos adultos. En medio la foto del centro aquí estoy con mi esposo estábamos de vacaciones no me acuerdo dónde andábamos, pero era una cuna como pueden ver aquí era una aventura.  Una aventura y aquí estoy yo sola al lado izquierdo. Yo estoy aquí para realmente apoyarlos dentro de este dentro de este proceso dentro del proceso de aprender todos y dentro del proceso de mejorar nuestro entendimiento sobre el sistema bancario. Yo les puedo decir que a mi papá que está aquí al lado del derecho como lo pueden ver, está el un hispano tradicional y a él le costó mucha batalla a tener hasta cierto punto la confianza en los bancos. Confianza en el sistema bancario para que en los EE.UU. que es muy diferente que el de México. Pero ahora ya está en una posición mucho mejor donde se siente cómodo el con ese proceso y con y con lo que el banco ofrece con seguridad.

El día de hoy vamos a estar hablando un poco sobre la seguridad y la protección en los servicios bancarios por medio del internet. Algunas de las cosas en las que

vamos a hablar incluyen:

- La importancia de la seguridad bancaria.
- como los bancos confirman nuestra identidad

porque a lo mejor hay alguna, alguna inquietud cómo van a verificar que soy yo alguien más puede ir a sacar mi dinero o cosas así vamos a confirmar y vamos a ver cómo los bancos confiaron a nuestra identidad.

- Prácticas de comunicación del banco

Como el banco se comunica con nosotros

- Cómo detectar una estafa

Que es algo real que podría suceder que en veces nos mortifica.

- Aprender a identificar actividades sospechosas

Es algo muy importante tenemos que asegurarnos que sabemos cómo detectar esta actividad de sospechosos y vamos a aprender a hacer esto el día de hoy.

De nuevo confirmando que los últimos 15 minutos nos vamos a reservar para alguna pregunta alguna inquietud de algún comentario voy a estar disponibles para ustedes.

Entonces la importancia de la seguridad bancaria.

Quiero preguntarles a ustedes: ¿Cuáles son algunas de sus preocupaciones con los servicios bancarios por internet?

¿Porque hay preocupaciones? Siempre hay preocupaciones no importa si eres hispano o es americano o eres italiano. Todos tenemos en veces preguntas o preocupaciones. Entonces quiero que reserven esa pregunta cuáles son algunas de sus preocupaciones con los servicios bancarios por internet hay que reservar esta pregunta porque si todavía hay preocupaciones después de este a esta presentación, hay que hablar sobre esas inquietudes o esas preocupaciones que ustedes tengan. También quiero hacer un tipo de encuesta con ustedes. ¿Alguien ha sido víctima de fraude o conoce usted a alguien que ha sido víctima de fraude? En veces cuando existe eso tenemos podemos tener algo de mortificación. Podemos tener algo de mortificación relacionada a usar los servicios bancarios. Otros vamos a darles apoyo para para aliviar algunas de esas inquietudes que ustedes tengan. Quiero darles las gracias de nuevo por estar presentes. Y quiero que piensen en esas mortificaciones son preocupaciones que ustedes tengan. Lo que vamos a hacer vamos a ver un vídeo que explica cómo los bancos están 100% comprometidos con mantener nuestra información segura. Es un vídeo que vamos a ver es un vídeo corto el vídeo que vamos a ver que está corto es únicamente algunos minutos de largo. Creo que es más es como un minuto de largo. Está este vídeo. Si ustedes tienen alguna inquietud no quieren ver estos vídeos otra vez o quieren más información, siempre pueden ir a este sitio de internet que es ready set bank punto org da clase e es el inicio y dentro de este sitio pueden encontrar bastante información. E información sobre line, sobre recursos sin fines de lucro, consejos de aprendizaje, noticias y si bajan aquí, hay algunos vídeos aquí que también pueden ver están todos en español. Pero vamos al primer vídeo aquí que vamos a estar viendo momentito ok voy a voy a abrir los grandes para que lo puedan ver cómodamente.

Ok.

Y por mientras sé que prenda el vídeo lo que voy a hacer, me voy a apagar mi cámara y micrófono para que puedan tener mejor, mejor habilidad de realmente escuchar porque no quiero que escuchen algo que esté pasando aquí atrás grabando Sergio o algo los cada vez que yo pre ponga un vídeo van a ver que la pantalla mía se apaga pero luego vuelvo a aparecer. Ok, vamos a empezar de nuevo un muy corto vídeo.

Video:

# COMMUNITY CONNECT VIDEO 2

Los bancos están comprometidos a mantener su información y su dinero seguros. Están preparados para diferentes tipos de riesgo y han configurado características de seguridad directamente sus sistemas. Esto es debido a que los bancos tienen un interés particular en la prevención del fraude. Así que dependen de muchas estrategias para mantener sus finanzas seguras. Por ejemplo, el robo de identidad es sólo una de las series amenazas de las que se protegen. Este tipo de robo puede tomar diferentes formas. Como alguien tratando de obtener acceso no autorizado a su cuenta o alguien con malas intenciones obteniendo la información de su tarjeta de crédito o de su contraseña. Evitar estas amenazas es tan importante para el banco como para usted. Los bancos trabajan en fortalecer sus sistemas de datos para protegerlos de intentos obtener acceso no autorizado a su información. Para estar un paso por delante de las amenazas, su banco monitorea sus patrones normales de compra. Su banco la editará así se observan compras sospechosas, actividades que parezcan fuera de lo normal para usted, como una transacción por una cantidad muy alta, o una nueva actividad en otro país. Y la protección de su cuenta ayuda a los bancos a evitar daños.

[Música]

vamos a salir de este vídeo aquí y vamos a volver a la presentación. Ok, entonces vimos esas preocupaciones que ustedes tenían. las tenemos estamos pensando en esas preocupaciones que pueden estar ustedes a procesando en este momento. Y también identificando cómo podemos estar seguros.

Ahora, la según nosotros tenemos que ver la seguridad y ver cómo se toma con mayor seriedad. ¿Entonces, mi pregunta para usted este es cuáles son algunas maneras que usted puede tomar para proteger sus cuentas?

Una de las cosas importantes es que tenemos que saber que mientras los bancos tienen la responsabilidad de mantener su dinero y su información privada y segura, nosotros también tenemos que hacer la parte de nosotros.  ¿Entonces qué métodos usan los bancos para mantener las cuentas de bancarias seguras?

Ellos usan algo que se llama cifrado para proteger las cuentas. Autenticación de multifactorial. Entonces ellos quieren asegurarse que las personas que están acezando la cuenta tienen la habilidad de acezar la cuenta. Que tienen el derecho de acceso a la cuenta que son personas que son recipientes de este dinero.

¿Entonces algunas maneras que usted puede tomar para proteger sus cuentas, cuales incluyen esas cuatro qué opciones tiene usted? Puede usted realmente tener bastante cuidado con y no darle el número de pin o la información a personas que no les tenga usted confianza. A personas que no están dentro de lo de la cuenta. Se recomienda que revise a su cuenta y reporte actividades sospechosas en su banco inmediatamente. Lo que me gusta mucho de usar el banco es que si a esta información sospechosa a cargos sospechosos yo le comento al banco y típicamente el banco me apoya y le puede ayudar a rectificar eso. Hacer me entero otra vez para no estar batallando cuando tenemos dinero en efectivo no tenemos esa misma habilidad si se los pierden 100 dólares están perdidos. No podemos recuperar el dinero, es un poco diferente con los bancos. Bastante diferente con los bancos. Entonces además de proteger también quieren confirmar su identidad. Acabamos de revisar el compromiso de los bancos en mantener nuestra información segura. Pero en este siguiente vídeo, revisaremos cómo los bancos confirman nuestra identidad, de qué forma lo hacen, cómo pueden lograr ellos confirmar una

identidad, y en veces puede sonar como un concepto un poco foráneo. Entonces vamos a ver un poco en este vídeo corto este vídeo es a un poquito más de dos minutos. Creo que como dos minutos 50 segundos. Algo así vamos a ver este vídeo de cómo los bancos confirman nuestra identidad. Nos voy a abrir aquí y vamos a ver este vídeo.

Video:

Para ayudar a asegurar que usted y solamente usted tendrá acceso a su cuenta, los bancos le permiten establecer lo que se conoce como autenticación multifactorial. En este caso autenticación significa que ellos están confirmando que usted es quien dice ser. Es la manera en que su banco sabe que usted es auténtico y no un ladrón de identidad. Y la autenticación multi factor simplemente significa que se usa más de un método para verificación de su identidad. Hay tres tipos de factores que los bancos pueden usar para la autenticación. El primer factor es algo que usted conoce como una contraseña u otro tipo de información. El segundo es algo que usted tiene por ejemplo un objeto físico como un teléfono móvil o una tableta. Y luego hay algo único que lo identifica solo a usted como su huella digital. Con la autenticación multifactorial nadie puede obtener acceso a su cuenta con solo un tipo de información. Como una contraseña, un nombre de usuario, o una dirección de correo electrónico. También tienen que tener algo suyo como el número de teléfono móvil asociado a su cuenta o tiene que ser realmente usted mientras más vueltas tenga que dar un malhechor es menos probable que pueda apoderarse de su información. Y algunos bancos están introduciendo opciones biométricas las cuales utilizan factores físicos únicos para verificar su identidad. Como las tecnologías de huellas digitales en smartphones computadoras portátiles y atm. Los bancos e incluso han comenzado a explorar las características de reconocimiento facial y de voz, así como escáneres de iris que se encuentran disponibles por medio de aplicaciones móviles. Nuevas tecnologías de activación por voz también le permitirán consultar sus saldos o hacer pagos mediante comandos de voz. O muchos sitios web de bancos usan autenticación multifactorial para confirmar su identidad cuando usted ingresa a su cuenta desde una computadora o teléfono que su banco no reconoce. En estos casos primero preguntarán por su contraseña luego le enviarán un mensaje de texto o correo con otro código que usted tendrá que ingresar. El paso adicional les ayuda a asegurarse que realmente es usted. Esto puede sonar a una película de james bond pero es muy probable que usted ya esté familiarizado con la autenticación multi factor. Cuando usa aún hay tiempo para retirar fondos, usted desliza la tarjeta y luego se le pide que ingresé su pin. El pin es algo que usted conoce y la tarjeta es algo que usted tiene. Sin estos dos juntos usted no podría completar la transacción.

Vamos a continuar. entonces vimos este vídeo me encantó el vídeo como dio toda la información específica de cómo pueden confirmar nuestra identidad. los tipos de usos que ellos usan que son los tipos multifactorial. Como la contraseña poner nuestro pin o si lo estamos haciendo en línea poner nuestra contraseña que tenemos que usamos. que es como una serie de si ese si es por medio de su tarjeta normalmente son cuatro números que usamos. Si es por medio de cuatro números secretos. Así es por medio de la computadora características también usan nuestro teléfono móvil. Si llamamos de nuestro teléfono móvil piensan que somos nosotros y los hacen más preguntas sobre nuestra identidad. O si usamos nuestro teléfono móvil para entrar al sitio reconocen que es nuestro teléfono móvil que está entrando y si nos piden más información, pero es un factor que usan para confirmar que somos nosotros. Algunas características del usuario ahora con los teléfonos que podemos aplastar un botón y agarrar nuestra huella. Entonces a lo menos que alguien tenga mi huella mismísima nadie puede entrar

a mi cuenta más que yo eso. Me gusta muchísimo a mí lo siento como que es algo muy atractivo me siento muy segura con esta opción con esta huella digital.

¿Porque los bancos usan tres tipos de multifactorial?

Usan estos tres tipos porque ellos realmente quieren asegurarse de que usted la persona que está accediendo su cuenta que está accediendo su dinero, no es un estafador que sólo pudiera tener una parte de su información. Entonces, los estafadores únicamente tienen una parte de la información no toda mi información. Siempre queremos nosotros asegurarnos de que nuestro sitio de web esté utilizando, que estemos utilizando sea seguro. Tenemos que estar en alta alerta a nuestros alrededores para asegurar que alguien en el público no va a querer acezar a esta información cuando la estamos aceptando.

Y ahora lo que vamos a hacer nos vamos a ir a un vídeo que habla un poco sobre, sobre las prácticas de la comunicación. Vamos a ver como los bancos se comunican con nosotros. Vamos a ver este corto vídeo es muy rápido el vídeo, pero antes de empezar este vídeo.

le voy a hacer voy a..

[Música]

voy a pagar aquí.

Antes de que empieza este vídeo lo que me gustaría hacer, me gustaría que pusieran usaran alguna reacción por ejemplo un corazón lo vemos aquí el lado izquierdo o podemos usar una explosión. También podemos usar un dedo para arriba. Quiero que hagan eso si ustedes han usado algún tipo de pin en el pasado. Que quiere decir como esa contraseña de cuatro números. O una contraseña en la computadora quiero que usen una de esas reacciones. En cualquier sitio por ejemplo vamos a poner el ejemplo un ejemplo sencillo. Por ejemplo, en veces tenemos una tarjeta para ir a el safeway que nos da un descuento. Pero tenemos que poner nuestro teclado en nuestro número de teléfono es como un tipo de pín. O si vas a algún sitio que te dan una tarjeta, pero te tienes que memorizar tu número de pin para acezar algo o algo así. Cualquier de ese tipo de contraseñas y ustedes la han usado quiero que vuelvan otra vez a poner su dedito a poner un corazón a poner una reacción. Porque parte de esto también lo hacemos un poco interactivo. Quiero darles las gracias por continuar conmigo. Vamos a lo mejor ahora voy a hacer otra vez una compartida y lo que vamos a hacer vamos a ver este vídeo, aunque hablaba un poco sobre las prácticas de comunicación con nuestro banco.

listos..

Video:

Ya sea usted o su banco quien inicie la comunicación. Conocer qué tipo de detalles puede que se le pregunten puede ayudarle a estar atento ante posibles estafas. Esto aplica a llamadas telefónicas correos electrónicos y mensajes de texto. Comencemos con las comunicaciones que usted recibe del banco. Existen razones de rutina por las cuales su banco podría comunicarse con usted. Por ejemplo, podría necesitar confirmar si fue usted quien intentó hacer un determinado cargo a su cuenta. O alertar le acerca de alguna actividad en su cuenta que parezca inesperada o sospechosa. Cuando su banco se comunica con usted su objetivo normalmente es darle avisos. Ellos no deberían pedirle que comparta información personal en un mensaje de texto correo electrónico o llamada telefónica no solicitada. Si

alguna vez le llegan a pedir cualquiera de estos detalles, evite dar los. Ya que es una señal de una posible estafa. Si tuviera preguntas o algo pareciera fuera de lo normal busque el número de servicio al cliente de su banco y comuníquese con ellos. Cuando es usted quien inicia la comunicación con su banco ya sea por teléfono o por correo electrónico, podrían preguntarle por algunos tipos de información para verificar su identidad. Como su dirección o su fecha de nacimiento. Esto ayuda a buscar los detalles de su cuenta y confirmar que usted es quien dice ser. De esta forma el banco puede darle toda la información que usted necesite. Ya sea que usted se haya comunicado con su banco por teléfono o por correo electrónico, se le pedirá que verifique su identidad al dar su número de cuenta y también puede que se le solicite que responda algunas de las preguntas de seguridad de su cuenta. No se le debería pedir información personal como su contraseña para los servicios bancarios o su pin de edición. Atm si algún representante se desvía de estas prácticas estándar y le pida detalles privados como estos, es una señal de que podría no ser confiable. Manteniéndose alerta ante las preguntas o solicitudes sospechosas usted puede evitar la posibilidad de phishing, táctica en la que un estafador asume la identidad de una compañía e intenta obtener acceso a su cuenta. Si alguna vez alguien llegara a comunicarse con usted y sospecha que la persona con quien habla no es confiable, sencillamente cuelgue y visite el sitio web de su banco para encontrar un número oficial al cual llamar. Simplemente busque un enlace que diga comuníquese con nosotros.

Gracias por continuar conmigo, y muchas gracias por estar de nuevo aquí y vamos a continuar. Vamos a hablar un poco sobre este tema. ¿Cuando el banco se comunica con nosotros cuántos de ustedes han oído hablar de phishing? Este proceso realmente es un término utilizado para para describir cualquier tipo. Cualquier tipo de llamada telefónica correo electrónico o correo como cuando recibimos cartas, correo que le engañe para que proporcione usted información personal. Haciendo usted ellos muchas veces pasar como un negocio o una institución financiera. ¿Es inmediatamente como una bandera colorada para nosotros de decir que parar aquí que está pasando porque necesitan esta información mía? Vamos a ver cuáles son algunas de las señales las vimos aquí en el vídeo. Crea el sentido de urgencia. Ellos crean un sentido de urgencia que necesita ustedes darles la información luego rápido para que para que ellos cuiden de su dinero. O porque algo urgente está pasando. Presentan una situación urgente el banco nunca haría eso. Luego le piden su información personal como su número de seguro social o su domicilio de casa. Ellos deben de tener eso el banco tiene esa información. Recuerden ellos están llamando con un sentido de urgencia y pidiendo la información personal. Una llamada telefónica de un número desconocido. También un número desconocido es algo que nos mortifica porque están llamándonos a nosotros de un número desconocido. Es importante por qué está sucediendo esto. Son señales que podríamos estar siendo estafados. Vamos a ver cómo detectar esa estafa, de qué forma la podemos nosotros detectar. Hemos cubierto mucha información sobre cómo los bancos protegen nuestra información, confirma nuestra identidad y cómo los bancos se comunican para que no seamos víctimas de phishing. los últimos dos vídeos nos mostrarán cómo podemos detectar una estafa y cómo estar atentos ante cualquier tipo de actividad sospechosa en nuestro banco. Entonces para esto lo que vamos a hacer vamos a ver dos vídeos. Vamos a volver a reunirnos después en los vídeos creo que después del primer vídeo, voy a tomar una pequeña pausa y luego volver a el segundo vídeo. Nos vamos al primer vídeo este es el penúltimo vídeo para nosotros.

# COMMUNITY CONNECT VIDEO 2

Video:

¿Abuelita, soy yo miguel cómo estás? ¿Miguel? ¿A ha pasado tanto tiempo suena diferente mayor? Dado mucho tiempo, en fin, bueno yo, yo estoy en problemas. Estoy en chicago ahora y unos tipos acaban de robarme. Necesito dinero para volver a casa a salvo. ¡O no! Y lo que sucede es que yo, yo no quisiera que mis padres se enteren de esto para no preocuparles. ¿Crees que podrías ayudarme? ¡Es urgente! Los bancos hacen todo lo que puede para mantener su cuenta segura. Y eso incluye ayudarle a identificar estafas como la que acabamos de ver. Esta se llama la estafa de la abuela. Y como otras tramas comunes sigue un patrón bien definido. Conocer estas tácticas que alguien puede usar para engañar le hará que sus finanzas se mantengan mucho más seguras. Las estafas toman ventaja de su tendencia natural de querer ayudar y seguir las reglas. Juegan con sus emociones como el miedo y la compasión. El objetivo es presionar le para que usted haga algo que probablemente no haría en circunstancias normales. Veamos cómo se estructuran normalmente las estafas. La primera señal, es cuando alguien se comunica con usted sin que usted lo solicite. Recibe una llamada telefónica un correo electrónico o tal vez una ventana de diálogo y usualmente de forma repentina. Con frecuencia, se trata de alguien con apariencia legítima. Alguien como su nieto o su compañía de seguros. La segunda señal es cuando la persona intenta asustar. Le podría fingir ser del ayer es y decirle que está en problemas para intimidarle y hacer que de información como el número de su tarjeta de crédito o la contraseña de su banco. Lo cual, nos lleva a la tercera señal. Cuando intentan darle un sentido de urgencia. Algo que usted tiene que hacer de inmediato. Podrían decirle que su computadora es infectada y que un técnico necesita obtener acceso a sus archivos inmediatamente. Cuando el mensaje es inesperado, atemorizante, y urgente estas son claves que delatan que algo no está bien. Entonces, ¿qué debe hacer usted al notar estas señales? En primer lugar, resista la presión de responder inmediatamente. Nunca envíen dinero después de una solicitud sospechosa ni comparta detalles bancarios importantes. En su lugar, cuelgue y comuníquese con alguien que usted sepa que es legítimo. Como alguien de su banco en este caso los padres de su nieto. Si se trata de su banco, puede hacer clic en el enlace de comuníquese con nosotros en su sitio web y hablar con un representante oficial. Algunos bancos incluso tienen un enlace mediante el cual usted puede reportar correos electrónicos sospechosos. Y recuerde, también debe estar alerta ante estafas relacionadas con su compañía telefónica o de cable. No solamente con su cuenta bancaria, los estafadores pueden usar otras cuentas para encontrar una puerta trasera y obtener acceso a su información bancaria. Así que vale la pena permanecer alerta ante estas tramas. sin importar el tipo de información de que se trate.

Aquí vimos un poco sobre cómo detectar una estafa. Lo que vamos a hacer ahora vamos a ver un vídeo sobre cómo estar atento a actividades sospechosas. Y voy a abrir el vídeo, lo vamos a poner. Este vídeo es un poco más corto.

Video:

Conocer las señales comunes de fraude en los servicios bancarios por internet es crucial. Y puede ayudarle a mantener sus cuentas y sus finanzas seguras. Podría recibir un correo electrónico solicitando le compartir su información bancaria como su nombre de usuario y contraseña. O podría haber un cargo en su cuenta, incluso uno pequeño que usted no reconozca o recuerde haber hecho. Podría incluso

recibir una llamada telefónica solicitando información confidencial y no saber cuánto detalle seguro compartir. Los eventos sospechosos como estos, normalmente son falta alarmas. Pero mantenerse alerta ayuda a protegerle a usted ya sus finanzas en el supuesto caso que se trata de una amenaza real. Esta es la razón por la cual aún si usted no está 100% seguro de que la actividad sea sospechosa, no debe dudar en colgar y comunicarse con su banco para confirmar la solicitud. Y recuerde nunca de información por correo electrónico o un mensaje de texto. Ni haga clic en enlaces que no parezcan ser confiables. En estas situaciones, la opción más segura siempre es comunicarse con su banco lo antes posible para mayor tranquilidad. Examine el sitio de web de su banco para encontrar un número telefónico donde usted puede comunicar sus preocupaciones y hacer preguntas. Busquen enlace que diga: comuníquese con nosotros o algo similar. Tenga la información de su cuenta la mano, así como los detalles importantes acerca del supuesto fraude. Su banco podría incluso darle una dirección de correo electrónico a la cual usted puede reenviar mensajes sospechosos. Esto les ayuda a decidir si se trata de una amenaza legítima que desinforma de cualquier tipo de estafas phishing que pueden estar circulando. En el caso remoto de que se haga un cargo o fraudulento a su cuenta, su banco probablemente le ofrecerá un crédito provisional por los fondos robados si usted le se informa oportunamente. También debería ofrecerle un reembolso completo después de haber llevado a cabo una investigación y confirmado el fraude. Si usted les informó al poco tiempo de haber ocurrido. Usted puede obtener protección adicional contra estafas como estas manteniéndose alerta al ingresar su contraseña en lugares públicos. Asegúrese de que otras personas no puedan ver su pin cuando esté en una atm o en una fila para pagar. Y si alguna vez pierde o les roban su tarjeta de débito reportero de inmediato a su banco. Para familiarizarse con las precauciones de seguridad de su banco, invierta tiempo en su sitio web. Allí encontrará una gran cantidad de recursos que le permitirán comprender cómo responder a su banco si alguna vez su cuenta llega a estar en riesgo. Recuerde, que en cada etapa de los servicios bancarios por internet su banco es su aliado más importante para mantener sus finanzas seguras y protegidas.

Y volvemos todos juntos a nuestra presentación. Vamos a hablar un poco sobre estas las de actividades sospechosas. Dentro de nuestras interacciones y dentro de nuestra, a nuestra, nuestra habilidad de aprender un poco más el día de hoy sobre lo de los bancos. Podemos ver cuáles son otras estafas que existen. Entonces llamadas o cartas diciéndoles que debe dinero al gobierno, se ganó la lotería, o ganó un premio gigante, pero necesita usted depositar una cantidad de dinero como una garantía. Entonces, eso nos dice inmediatamente esto es una estafa. qué pasa si somos víctimas de fraude? ¿Qué pasa en este momento verdad? Entonces vamos a hablar un poco sobre sobre esto. que hacemos en esos casos? Okay he estado usando mi tarjeta para pagar. ¿Esto y me siento con más confianza con el banco, pero si alguien uso mi tarjeta o un fraude un robo de identidad que hago? Tenemos que reportar el fraude a las autoridades aparte de reportarlo claro al banco, y cualquier agencia de crédito. Queremos llamar a las agencias que reportan, a que reportan su reporte de crédito. Y el banco les puede ayudar en todas estas circunstancias ellos hacen todo lo posible para ayudarles. Identificamos cuáles son algunas maneras en que los bancos pueden prevenir el fraude. Como previenen el fraude los bancos. Los bancos hacen todo lo posible para prevenir el fraude. ¿Pero que hacen específicamente? Ellos revisan cualquier cargo inusual les voy a dar un ejemplo. Yo estaba afuera de la ciudad en otro estado que normalmente no visito, y no se me ocurrió llamar al banco para decirles voy a estar yo en Washington. No se me ocurrió decirles entonces yo voy ellos ven que empiezas en la tarjeta y de repente fue a usar la tarjeta, y no fue

aceptable. ¿Nombre como que me la bloquearon entonces yo llamé al banco porque pues necesitaba mi tarjeta para pagar, y me dijeron oh puedes confirmar su identidad? Confirmé mi identidad volvieron a activar la tarjeta dije una vez que la quitamos la tarjeta porque pensamos que alguien estaba usando la que no eras tú, porque era un cargo inusual. Encriptan nuestros datos. Encriptan nuestros datos para que nadie pueda tener nuestra información específica. Está todo revuelto como muchos números y características letras. Ambos requieren la verificación de identidad de varias formas. No nomás necesitan tener una forma, son varias formas para poder acceder su cuenta. Es algo que los bancos hacen que es importante. Finalizando un poco, un poco sobre esto vamos a ver que si es que fraude ocurre, claro que, en estas ocasiones, y si se lo comunican al banco, el banco hace todo lo posible para investigar y reembolsarle el dinero para que esté entero otra vez usted y no tenga problemas económicos. Sabemos que hay personas que van a intentar aprovecharse de usted para robarle, pero ya usted ahora sabe tres signos para detectar este fraude. El sentido de urgencia, alguien a alguien que no conozca pidiendo la información personal, o llamadas de números desconocidos. también no comparta su información personal con alguien que no tenga confianza. Como su número de tarjeta de crédito, su número de pin, la clave su número de seguro social nada de esa información es le va a dar a otras personas desconocidas. Finalizando, quiero yo darles las gracias a todos porque pasaron conmigo a algunos minutos bastante agradables aprendiendo un poco más sobre los servicios con el banco. Y qué podemos hacer con esos servicios. Quiero yo realmente volver a reintegrar los tres signos para detectar el fraude. Y la importancia de proteger su información usted es proteger esta información que es muy importante. El resumen dentro de este esta serie vimos hoy la seguridad y protección en los servicios bancarios por internet. La importancia de la seguridad bancaria como los bancos confirman su identidad, prácticas de comunicación de su banco, cómo detectar una estafa, aprender a identificar actividades sospechosas. Ahora lo que vamos a hacer vamos a continuar y vamos a tener una discusión por estos últimos 15 minutos. Y voy a estar disponibles para usted para hacer para contestar cualquier pregunta que tenga. A la mejor yo no voy a tener la respuesta que ustedes necesitan. Pero, yo si no tengo la respuesta podría yo encontraron la manera de encontrar esa respuesta para pasársela a ustedes. Me dio muchísimo gusto haberlos conocido aquí a todos y haber estado con ustedes en esta presentación. Ahora nos movemos a las preguntas.

Preguntas:

¿Ok ahora esto quiere decir que se pueden escuchar? Y perfecto veo que alguno..

[Música]

O no.

O no.

O no.

Oh oh oh oh oh.

Ah.

Ah.

# COMMUNITY CONNECT VIDEO 2

Creo que tuvimos unos problemas técnicos, pero creo que han sido resueltos si no están resueltos, a la biblioteca de Yuma nos da avisar. Pero quiero darles las gracias a todos por haber estado presentes el día de hoy. Si veo que algunas personas tienen preguntas sobre la información que acabamos de revisar. Y quería rápidamente tomar unos momentos para contestar algunas preguntas que ustedes tienen. ¿Una de las preguntas que vi e incluía preguntas sobre qué es phishing? Phishing es como un tipo de engaño y la respuesta es sí es como un tipo de engaño. Es un término es el que describe realmente cualquier tipo de ya sea una llamada telefónica un correo electrónico o algún tipo de comunicación donde ellos están buscando phishing en inglés quiere decir pescar. Ellos están pescando para información personal de usted. Ellos quieren esta información y ellos la quieren para poder estafarlo. Entonces en veces se hace en forma de es presentado en forma como de una persona conocida o una persona desconocida. Pero siempre tienen como ese sentido de urgencia cuando ellos están pidiendo la información a usted. Entonces su consejo es que usted monitorea sus cuentas. Siempre vea qué cargos están ahí porque recuerden que cuando alguien está tratando de estafarnos usando phishing ellos están realmente creando ese sentido de urgencia. Ellos están pidiendo información en verso personal que no deben de tener como los seguros sociales por número de pin nuestro número de cuenta completo o cosas así. Y en veces las llamadas vienen de un número desconocido, no conocemos el número no sabemos de dónde viene. Esa fue una pregunta que se hizo que es una excelente pregunta. A otra pregunta que hicieron incluye, ¿qué hago si veo cargos extraños, que hago en esos momentos, que hago? ¡Y tengo un pin y cuenta y me mortificó porque a dejarlos ahí que no deben de estar entonces una de las cosas más importantes es reportar, reportar, reportar, reportar! Por qué ¿por qué es importante reportar lo que vemos que es fraudulento, lo que vemos que no es apropiado. Entonces en esos casos cuando vemos que hay algún tipo de robo o que hay un cargo extraño llamamos a nuestro banco para reportar esto. Si es necesario llamamos a nuestras autoridades, la policía y vamos a cualquier agencia de crédito. Dependiendo del apoyo que tengamos del banco. Muchas veces cuando llamamos al banco para decirles, tengo una un cargo muy sospechoso un cargo extraño, y nos ayudan a determinar si nosotros hicimos el cargo o si no lo hicimos ellos toman acciones para poder hacernos completos otra vez. Ya abandonó su cargo temporal por mientras que hacen su investigación y lo hacen un cargo permanente, hacia nosotros son crédito que él con permanente con nosotros. Y ellos también nos dan muchos recursos en cuanto a llama en este lugar, es una cantidad grande que llama la policía, hay diferentes cosas que se pueden hacer para asegurar la seguridad de ustedes. Lo más importante, es si vemos cargos extraños, podemos nosotros tomar acción. Si nosotros tenemos dinero en efectivo y ese se pierde no hay mucha acción que podemos tomando. Tenemos muchos recursos disponibles para nosotros. Entonces otra pregunta muy excelente gracias por preguntar. Otra pregunta que veo es también estamos en riesgo con las compañías de teléfono. Qué riesgo podríamos tener si ay llamadas que entran para con ustedes de números desconocidos inmediatamente, es como una bandera colorada. Que los dice tengo que ver exactamente quién es esta persona. Puede en vez de presentarse como una compañía de teléfono y pidiendo información o cualquier otro portal otra compañía. O puede presentarse por medio de una llamada a nuestra casa o una llamada a nuestro celular de un número desconocido por medio de la compañía del teléfono. No siempre es importante tener precauciones y es importante para nosotros asegurarnos de que siempre estemos al tanto de lo que nosotros compartimos. Cuando vemos llamadas telefónicas desconocidas entrada, hay que asegurarnos de que sabemos a quién le estamos dando esa información. Nunca queremos compartir nuestra información nuestro seguro social, número de tarjeta de crédito, etcétera con alguien por teléfono. O no. ¿Muy buena pregunta también otra pregunta que yo pienso que es también muy buena es una pregunta

alguien preguntó, en qué tipo de servicios puedo ser estafada? Como es una pregunta muy abierta, pero a la misma vez es una pregunta muy importante. Porque cualquier tipo de servicio bancario puede ser podemos exponernos a pagar a una estafa en cualquier tipo de servicio bancario. Ya sea un depósito, un crédito, o cheque es mandar un cheque en recibir. Y tenemos que tener mucho cuidado porque si podemos ser víctimas de estafa. Pero lo más importante saber es que los bancos hacen todo lo posible para asegurar y revisar los cargos y ellos siempre están viendo algún cargo inusual aquí. Si en un cargo es inusual, voy a poner un alto a esta tarjeta porque no queremos que alguien use la tarjeta si no debe de estar usando la tarjeta. Yo siempre quieren asegurarse que la tarjeta sea usada que sea usada y te vamos a dar únicamente con las personas autorizadas, las personas autorizadas son las que van a estar usando la tarjeta no otras personas. Veo ya nomás hacer un reviso rapidito para ver si hay alguna otra pregunta que entro en estos últimos segundos lo veo que no entro otra pregunta. En general les quiero dar otra vez las gracias por estar presentes en esta sesión. Voy a tener otra sesión el día 27 a las 4 de la tarde. Entonces espero verlos en esa sesión. Pero me dio mucho gusto ser su presentadora y les doy las gracias de nuevo por estar presentes y por tomar tanta precaución en asegurarse de tener la información y la educación necesaria. Por educarse y haciendo la transición a utilizar los servicios bancarios muchas gracias y buenas tardes.