Tema:
Estafa bancaria

Grupo № 4
Integrantes:

- ✓ Tnte. LUIS ALBERTO REYES LINARES
- ✓ Insp. ARIEL ANTONIO MERCADO PAVÓN
- ✓ Insp. JOSÉ LEONEL OSEJO LÓPEZ
- ✓ Sub-ofic. mayor OMAR GARCÍA ROCHA

Managua, 25 de mayo del 2023

Тема: Банковское мошенничество

Группа № 4
Состав группы:
Лейт. ЛУИС АЛЬБЕРТО РЕЙЕС ЛИНАРЕС
Инсп. АРИЭЛЬ АНТОНИО МЕРКАДО ПАВОН
Инсп. ХОСЕ ЛЕОНЕЛЬ ОСЕХО ЛОПЕС
Ст.серж. ОМАР ГАРСИА РОЧА

Манагуа, 25 мая 2023 г.

Marco jurídico

- **Ley 641**, Código Penal de Nicaragua, **Art. 230. Agravada** La estafa será sancionada con prisión de tres a seis años y trescientos a quinientos días multa, en los casos siguientes: a) Cuando su objeto lo constituyan viviendas o terrenos destinados a la construcción de aquellas u otros bienes de reconocida utilidad social; b) Cuando se cometa con abuso de las relaciones personales existentes entre la víctima y el estafador, o éste aproveche su credibilidad empresarial o profesional; c) Cuando recaiga sobre bienes que integren el patrimonio histórico, cultural o científico de la nación. d) Cuando se realice por apoderado o administrador de una empresa que obtenga, total o parcialmente sus recursos del ahorro público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya obtenido sus recursos total o parcialmente del ahorro del público; e) Cuando el valor de lo estafado y la entidad del perjuicio, coloque a la víctima o a su familia en un grave deterioro de su nivel de vida. f) Cuando se cometa valiéndose de tarjeta de crédito o débito propia o ajena, o con abuso de firma en blanco, o, g) Cuando se realice mediante cheque, pagaré, letra de cambio en blanco o negocio cambiario ficticio.

Правовые рамки

- **Закон 641**, Уголовный кодекс Никарагуа, **статья. 230.** Мошенничество при отягчающих обстоятельствах наказывается тюремным заключением на срок от трех до шести лет и штрафом в размере от трехсот до пятисот дней в следующих случаях: а) если объектом мошенничества являются жилые дома или земельные участки, предназначенные для строительства тех или других общественно полезных объектов; б) когда совершается злоупотребление личными отношениями между потерпевшим и мошенником или когда мошенник использует его деловой или профессиональный авторитет; в) когда речь идет об имуществе, объединяющем историческое, культурное или научное наследие нации; г) когда это осуществляется представителем или администратором компании, которая получает, полностью или частично, свои ресурсы за счет государственных сбережений, либо тем, кто лично или через зарегистрированное или незарегистрированное предприятие любого характера полностью или частично извлекает свои ресурсы из сбережений населения; д) когда стоимость полученного обманным путем и сущность причиненного ущерба ставят потерпевшего или его семью под серьезное ухудшение их уровня жизни; е) При совершении с использованием собственной или чужой кредитной или дебетовой карты, или со злоупотреблением пустой подписью, или, ж) когда оно осуществляется с помощью чека, простым векселем, пустым переводным векселем или под прикрытием фиктивного валютного бизнеса.

Marco jurídico

- Ley **1042**, **Cyber Delitos**.
- Artículo 15, **Hurto por Medios Informáticos.**
- El que, el que por medio del uso de las tecnologías de la información y la comunicación, se apodere de bienes o valores tangibles o intangibles de carácter patrimonial, sustituyéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para si o para otro, siempre que el valor de lo hurtado sea mayor a la suma resultante de dos salarios mínimos mensuales del sector industrial será sancionado con prisión de dos a cinco años y trecientos a seiscientos días de multas.

Правовые рамки

- Закон **1042**, **СПЕЦИАЛЬНЫЙ ЗАКОН О КИБЕРПРЕСТУПЛЕНИЯХ** .
- Статья 15, **Хищение с помощью компьютерных средств.**
- Любое лицо, которое с помощью информационно-коммуникационных технологий, вступает во владение материальными или нематериальными активами или ценностями имущественного характера, похищая их у их собственника, держателя или владельца, с целью получения экономической выгоды для себя или для другого, всякий раз, когда стоимость украденное превышает сумму, полученную в результате двух минимальных месячных заработных плат в промышленном секторе, наказывается лишением свободы на срок от двух до пяти лет и штрафом от трехсот до шестисот дней.

Marco jurídico

Artículos: 17, **Manipulación Indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares.**

El que intencionalmente y sin la debida autorización por cualquier medio crea, capture, grabe, copie, altera, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismo fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, se le impondrá pena de cinco a ocho años de presión y trecientos a setecientos días de multas.

Правовые рамки

Статья 17. **Ненадлежащее обращение с товарами или услугами с помощью смарт-карт или аналогичных средств.**

Любое лицо, которое намеренно и без надлежащего разрешения любыми средствами создает, захватывает, записывает, копирует, изменяет, дублирует, клонирует или удаляет компьютерные данные, содержащиеся на смарт-карте или на любом носителе, предназначенном для тех же целей; с целью включения, модификации пользователей, учетных записей, регистров, непризнанных видов потребления, будет приговорено к тюремному заключению на срок от пяти до восьми лет и штрафу в размере от трехсот до шестисот дней.

Conceptos

- **Estafa:**
- **La estafa es un delito que consiste en obtener una ganancia mediante el engaño. Es decir, significa generar riqueza haciendo abuso de la confianza de alguien más o mintiendo.**
- **Este tipo de fraude cibernético consiste en la creación de recibos falsos en nombre de grandes empresas. Al realizar el pago, la víctima deposita el dinero en la cuenta de los estafadores.**

Понятия

- **Мошенничество:**
- **Мошенничество - преступление, заключающееся в получении прибыли путем обмана. То есть это означает создание богатства путем злоупотребления чужим доверием или лжи.**
- **Этот вид кибермошенничества предполагает создание поддельных квитанций от имени крупных компаний. При совершении платежа потерпевший вносит деньги на счет мошенников.**

Tipos de estafas bancarios.

- **Phishing**
- El phishing es un **tipo** de estafa que ocurre a través de internet y consiste principalmente en que un tercero de forma fraudulenta obtiene todos los datos de un usuario. Esto incluye claves, cuentas bancarias, números de tarjetas de crédito, códigos especiales de seguridad para posteriormente ejecutar operaciones financieras sin autorización.
- Este tipo de violaciones de seguridad se puede producir por distintas vías. Normalmente los delincuentes crean entornos que suplantan las interfaces bancarias o envían correos electrónicos solicitando información de tus datos para mejorar el servicio, confirmar identidad o por mantenimiento, solicitando que actualices los datos de tu cuenta. También es común que señalen que dispones de poco tiempo para realizar dichos cambios o actualizaciones o tu cuenta será bloqueada.
- Además de intentar vulnerar nuestra seguridad por e-mail, existen grupos organizados que intentan obtener nuestros datos vía llamadas telefónicas y por mensajería de texto, suplantando la identidad de agentes bancarios.
- Es importante que bajo ningún concepto abras los enlaces que suelen incluir estos mensajes, ya que de esa forma capturan tus datos. Las entidades bancarias no enviarán solicitud de datos personales por correo electrónico ni por llamadas telefónicas, descarta ese tipo de mensajes y reporta dichos mensajes.

Виды банковских афер.

- **Фишинг**
- Фишинг - это **вид** мошенничества, которое происходит через интернет и в основном заключается в том, что третья сторона обманным путем получает все данные пользователя. Сюда входят ключи, банковские счета, номера кредитных карт, специальные коды безопасности для последующего несанкционированного осуществления финансовых операций.
- Подобные нарушения безопасности могут происходить различными способами. Обычно преступники создают среды, которые вытесняют банковские интерфейсы или отправляют электронные письма, запрашивая информацию о ваших данных для улучшения обслуживания, подтверждения личности или обслуживания, требуя обновления данных вашей учетной записи. Они также часто указывают, что у вас есть короткое время для внесения таких изменений или обновлений или ваша учетная запись будет заблокирована.
- Помимо попыток нарушить нашу безопасность по электронной почте, есть организованные группы, которые пытаются получить наши данные с помощью телефонных звонков и текстовых сообщений, выдавая личность банковских агентов.
- Важно, чтобы вы ни при каких обстоятельствах не открывали ссылки, которые обычно содержат эти сообщения, поскольку таким образом они захватывают ваши данные. Банки не будут отправлять запросы о предоставлении персональных данных по электронной почте или телефонным звонкам, нужно не отвечать на такие сообщения и сообщать о них.

- **Pharming**
- El pharming es un **tipo** de estafa que se aplica en el sector bancario y es muy complejo. Este consta de la replicación de plataformas y páginas web para que los usuarios al confundir dichas interfaces con las de las entidades bancarias, faciliten sus datos de forma voluntaria. Actualmente los navegadores en la barra de direcciones nos permiten observar los certificados de seguridad de las web, es importante que cotejemos que toda la información esté en orden. Debemos sospechar de una web si al ingresar, su dirección web se transforma automáticamente en una dirección IP numérica.

- **Фарминг**
- Фарминг - это **вид** мошенничества, который применяется в банковской сфере и является очень сложным. Это заключается в копировании платформ и веб-страниц, чтобы пользователи, путая указанные интерфейсы с интерфейсами банковских учреждений, предоставляли свои данные добровольно. В настоящее время браузеры в адресной строке позволяют нам соблюдать сертификаты безопасности в Интернете, важно, чтобы мы проверяли, чтобы вся информация была в порядке. Мы должны с подозрением относиться к веб-сайту, если при входе его веб-адрес автоматически преобразуется в числовой IP-адрес.

- **Key Logger**
- Un Key Logger o capturador de teclado es un medio complejo para realizar fraudes. Estos se pueden tratar de programas o dispositivos físicos que se instalan a un ordenador u otro aparato electrónico para capturar lo que escribe un usuario, para que dicha información sea utilizada posteriormente. Los Hardware dedicados a este tipo de actividades normalmente son dispositivos que se conectan a los ordenadores utilizando puertos USB o PS/2 y almacena los datos que sean ingresados al ordenador mediante el teclado.
- En cuanto a los softwares diseñados para captar datos de seguridad bancarias estos se ejecutan en segundo plano. Pasan desapercibidos en la pantalla y en los procesos activos. Actualmente los programas antivirus los identifican como virus troyanos y los bloquean con cierto grado de eficiencia.

- **Key Logger**
- Key Logger или клавиатурный ловец - сложное средство для мошенничества. Это могут быть физические программы или устройства, которые устанавливаются на компьютер или другое электронное устройство для захвата того, что пишет пользователь, для последующего использования такой информации. Аппаратные средства, предназначенные для таких видов деятельности, как правило, являются устройствами, которые подключаются к компьютерам с помощью портов USB или PS/2 и хранят данные, введенные на компьютер с помощью клавиатуры.
- Что касается программного обеспечения, предназначенного для сбора банковских данных безопасности, то они работают в фоновом режиме. Они остаются незамеченными на экране и в активных процессах. В настоящее время антивирусные программы идентифицируют их как троянские вирусы и блокируют их с определенной степенью эффективности.

Caso: “TARJETA DE CREDITO BAC”

- En fecha del 21 de junio de 2022, a las 10:15 Horas, los ciudadanos nicaragüenses: **José Ernesto Chavarría Barrios**, cedula: 001-201090-0110B y **Juan Rafael Padilla Ortiz**, cedula: 001-161297-1002V, ambos con domicilio en Managua, realizaron transacción bancaria de retiro de dinero en dólares en un cajero del banco BAC en el centro comercial Metrocentro, por la suma de 16,000.00 dólares en cuatro gestiones, llamando la atención al personal bancaria, quienes inmediatamente con los agentes de seguridad del banco los retuvieron le congelaron la cuenta bancaria y entregaron a los dos ciudadanos a las autoridades competentes (Policía).
- En las entrevistas realizadas a los investigados, expresaron que ellos recibieron llamada telefónica por la plataforma WhatsApp por un ciudadano con acento extranjero costarricense quien se les identifico como Daniel Arraiga, con número telefónico 507-765418, a quienes le hicieron una propuesta de trabajo en línea en ventas y compra por línea de internet de vehículos, terrenos, casas, artículos para el hogar y que, para empezar le enviarían a una cuenta bancaria de uno de ellos la suma de U$ 16,000.00 dólares, y que tienen que retirarlo el día siguiente a las 08:00 AM en el banco BAC de Metrocentro, una vez que los retiren se encuentren con su empleado en Nicaragua que los estará esperando en el parqueo en el vehículo Toyota Hilux de color blanco, quienes al salir del banco ellos le harían señas, una vez que realizaron sus transacción, fueron investigados por el banco y la policía que llegaron a entrevistarlos, los dejaron ir con el dinero que ellos sacaran del cajero, se contactaron con los representantes en Nicaragua del trabajo que le ofrecieron quienes le quitaron todo el dinero y solo les dieron a ella U$ 300 dólares a cada uno por la transacción.
- En la investigación e información proporcionada por el banco BAC, el dinero que los investigados sacaron del cajero, pertenecía a la cuenta bancaria de la ciudadana **María Elizabeth García Peralta**, 003-190478-0012T, con domicilio en Masaya, a quien se contactó y se le pregunto de lo ocurrido, expresando que desconocía de los hechos y que a nadie le ha proporcionado sus datos bancario, solo a un funcionario del banco BAC que la llamó vía telefónica, quien le expresó que estaba actualizando sus sistemas y que necesitaban confirmar sus datos generales, número de cuenta y pin, confirmándole sus datos y proporcionando la información requerida, sin saber que le iban a saquear su cuenta bancaria.

Случай: «КРЕДИТНАЯ КАРТА БАК»

- 21 июня 2022 года, в 10:15 часов, граждане Никарагуа: **Хосе Эрнесто Чаварриа Барриос**, удостоверение личности: 001-201090-0110B и **Хуан Рафаэль Падилья Ортис**, удостоверение личности: 001-161297-1002V, оба проживающие в Манагуа, провели банковские операции по снятию денег в долларах в банке БАК в торговом центре Metrocentro, в размере 16,000.00 долларов США в четырех случаях, обращая на себя внимание сотрудников банка, которые сразу же с сотрудниками службы безопасности банка задержали их, заблокировали их банковский счет и передали этих двух граждан компетентным органам (полиции).
- В ходе бесед с подследственными они заявили, что им позвонил на платформу WhatsApp гражданин Коста-Рики с иностранным акцентом, которого зовут Даниэль Арраига, с телефонным номером 507-765418, для тех, которым сделал предложение о работе в режиме онлайн в области продаж и онлайн-покупок транспортных средств, земельных участков, домов, предметов домашнего обихода и что, для начала, им будут отправлены на банковский счет одного из них сумму в 16 000 000 долларов США, и что они должны снять эти деньги на следующий день в 08:00 утра в банке БАК Metrocentro. Затем, как только они снимут деньги, они должны встретиться с сотрудником нанимателя в Никарагуа, который будет ждать их на парковке на автомобиле Toyota Hilux белого цвета. Когда они выйдут из банка, этот сотрудник должен им сделать знак для привлечения внимания. Как только они соверили транзакции, были расследованы банком и полицией, которые пришли с ними на собеседование, затем отпустили их с деньгами, которые они плучили в банкомате банка. Таким образом, они связались с представителями в Никарагуа, забрали у них все деньги и только дали им по 300 долларов каждому за сделку.
- В расследовании и информации, предоставленной банком БАК, деньги, которые подследственные сняли в банкомате, принадлежали банковскому счету гражданки **Марии Элизабет Гарсиа Перальта**, 003-190478-0012T, проживающий в Масайе, с которой связались с посьбой дать разъяснения в связи со случившемся. На что та заявила, что не знает об этих событиях и никому не предоставляла свои банковские данные, только одному сотруднику банка БАК, который позвонил ей по телефону, сказал ей, что он обновляет ее банковские данные и что ей необходимо подтвердить их, а так же номер счета и ПИН-код. Она подтвердила своии данные и предоставила необходимую информацию, не зная, что собираются ограбить ее банковский счет.

GRACIAS POR SU ATENCION!

СПАСИБО ЗА ВАШЕ ВНИМАНИЕ!