НАРОДНЫЙ УНИВЕРСИТЕТ

Специальный выпуск, посвященный реализации проекта «Цифровая самооборона»

№ 1(28) Июль 2023

«Цифровая самооборона»

Актуальность и социальная значимость проекта по противодействию мошенникам год от года возрастает. Для хищения денег у граждан злоумышленники используют все более изощренные сценарии. Центральный банк регулярно информирует о появлении новых мошеннических схем. Тысячи людей страдают от действий мошенников, теряют деньги, которые в некоторых случаях копили годами. Знания о том, как противодействовать мошенникам, помогут в нужную минуту принять правильное решение.

Проблема «цифровой» безопасности и защиты от мошенников в Челябинской области становится тем актуальнее, чем больше людей старшего поколения приобщается к благам «цифровой» экономики. Преступлений ежегодно становится больше. Информация о выявленных случаях кибермошенничества, опубликованная на сайте Главного управления МВД России по Челябинской области только за 10 дней июля 2023 года, включает обман при покупке товара на сайте бесплатных объявлений, перевод 7 млн рублей под предлогом проверки банка, обман при покупке через Интернет, перевод мошенниками 700 тыс. кредитных рублей и т. д. Только за двое суток ущерб от телефонного мошенничества составил почти 6 миллионов рублей: по 900 тысяч отправили неизвестным пенсионерки из Коркино и Миасса, около 700 тысяч — пенсионерки из Челябинска и Магнитогорска, пожилые жительницы Коркинского и Кунашакского районов потеряли 120 тысяч и 140 тысяч рублей соответственно. Полицейские отметили, что потерпевшие знали о телефонных мошенничествах, но поверили звонившим. Старшее поколение уязвимо перед мошенниками, которые используют методы социальной инженерии.

Общий по стране размер ущерба, нанесённого злоумышленниками за год, вырос на 23,9 %, почти до 4 млрд рублей. Статистика возврата средств банками при их краже со счетов граждан неутешительная — лишь 3,4 % возвращается клиентам. Остальное — «заработок» аферистов. Во многих случаях источник бед — это не только телефонные мошенники, но и фейковые сайты.

В 3-м квартале 2022 года ЦБ РФ инициировал блокировку почти 300 тыс. телефонных номеров. Число поддельных сайтов, маскирующихся под зарубежные бренды, выросло почти в 6 раз. Центробанк в 3 квартале инициировал блокировку почти 4 тыс. сайтов, рост по сравнению с предыдущим годом — на 68 %. Минцифры ввело систему мониторинга фишинговых сайтов. За 2 месяца активности системы выявлено 30 тыс. сайтов, копирующих ресурсы органов власти.

Причинами роста «цифровых» преступлений против людей старшего поколения являются недостаточная просветительская работа в целевой аудитории. Проект содействует формированию у граждан разумного финансового поведения и ответственного отношения к личным финансам.

Общество «Знание» активно работает в Троицке

В течение десятилетий в городе Троицке и Троицком районе Общество «Знание» тесно сотрудничает с ветеранскими организациями.

Ежегодно люди «серебряного» возраста с октября по май становятся слушателями Народного университета Общества «Знание», где они посещают лекции и курсы. В октябре 2023 года будет дан старт 25-му учебному году. Посещая Народный университет, ветераны стали активными участниками проекта «Цифровая самооборона», реализуемого с использованием гранта губернатора Челябинской области, предоставленного Фондом поддержки гражданских инициатив Южного Урала. Проект направлен на выстраивание системы защиты ветеранов Челябинской области от кибермошенников для обеспечения своей «цифровой» и финансовой безопасности. В течение года на площадке Троицкого отделения Общества «Знание» выступают банковские работники, юристы, сотрудники уголовного розыска, представители ТИК. Участниками проекта стали 260 пенсионеров города Троицка и Троицкого района, им был представлен цикл лекций:

- Финансовая безопасность в банковской сфере и риски мошеннических операций;
- Безопасные покупки в Интернете;
- Госуслуги, как источник достоверной правовой информации;
- Как защититься от финансового мошенничества;
- Алгоритм действий потребителей в случае нарушений их прав при покупке товаров дистанционным способом;
- Социальный фонд России упростит получение мер социальной поддержки граждан, увеличив количество электронных сервисов;
- Цифровизация избирательного процесса и безопасность дистанционного голосования.

Интересный и познавательный психологический тренинг провели для людей старшего поколения кандидаты педагогических наук Троицкого филиала ЧелГУ Светлана Осипенко и Ольга Байзулаева, доцент, практический психолог. Также в рамках проекта 100 ветеранов города Троицка и Троицкого района стали участниками курса «Цифровой» и финансовой безопасности. Для участия в проекте «Цифровая самооборона» троичанин в возрасте 55+ может подать заявку по телефону

+7 982 325 94 38 или на электронную почту trznanie@rambler.ru

Немаловажным в совместной работе Общества «Знание и ветеранского актива является взаимодействие с молодым поколением по патриотическому воспитанию молодежи. В рамках Всероссийского просветительского марафона «Знание о героях», организованного Российским Обществом «Знание», в городе Троицке на 8 площадках присутствовало 1396 человек, в том числе ветеранский актив, ветераны боевых действий, учащиеся школ и студенческая молодежь города Троицка. Проходят встречи и уроки мужества в рамках Всероссийской военно-патриотической просветительской акции «Знание.Герои», где спикерами выступают участники специальной военной операции, ветераны боевых действий, эксперты в области истории России. В мероприятиях на 18 площадках принял участие 1161 троичанин. Хочется поблагодарить образовательные учреждения Троицка: Южно-Уральский государственный аграрный университет, Троицкий филиал ЧелГУ, Троицкий технологический техникум, Троицкий педагогический колледж, Троицкий аграрный экономический колледж, а также школы города и района, которые принимают активное участие в акциях, организованных Российским Обществом «Знание». Особые слова признательности нашим лекторам Сабиржану Мухамеджановичу Таужанову, Владимиру Федоровичу Панову, Дмитрию Александровичу Давыдову, которые проводят большую патриотическую и просветительскую работу с подрастающим поколением.

Ветераны приняли участие во всероссийских неделях профилактики онкологических заболеваний и популяризации подсчета калорий. Перед слушателями Народного университета выступили специалисты ГБУЗ «ЧО ЦОЗ МП» Дмитрий Охезин и Евгений Паньков, которые в ходе лекций, как врачи по медицинской профилактике проконсультировали около 40 пенсионеров.

«Серебряные волонтеры» стали активными участниками акции «Одобрено старшим поколением». Они оценивали доступность мест общественного пользования для пожилых людей. Обследовано четыре учреждения культуры: Центральная библиотека города Троицка, МКУ «Библиотечно-информационный центр» с межпоселенческими функциями Троицкого муниципального района, Бобровская Павленковская модельная библиотека, Белозерская Павленковская библиотека.

Для слушателей Народного университета организуются мастер-классы по прикладному творчеству, где в качестве педагогов-наставников выступают «серебряные» волонтеры.

Мастерицы города Троицка и Троицкого муниципального района присоединились к фестивалю «Нужные люди», организатором которого является Общество «Знание» в рамках проекта «Альянс «Серебряный возраст»: «НКО + старшие». Слушателями Народного университета были организованы выставки для троичан в Центральной библиотеке и Бобровской Павленковской модельной библиотеке, где было представлено 110 экспонатов. Это изящные украшения из бисера, вязанные блузоны и салфетки, иконы и картины.

Также 13 троичанок в возрасте 55+ стали победителями в номинациях: «Культура и искусство», «Спорт», «Мы и внуки», «Лидер сообщества», «Серебряное волонтерство» виртуального фестиваля «Нужные люди».

В юбилейный год Троицка подготовлен ряд мероприятий об истории города, о наших знаменитых земляках, чьими стараниями прославлен город. В Обществе «Знание» прошел курс лекций, перед слушателями Народного университета выступила автор, библиограф-краевед Центральной городской библиотеки Елена Бачурина. Она провела виртуальную экскурсию «Пешком по Климова» и рассказала троичанам о знаменитом земляке Федоре Плевако, адвокате и судебном ораторе.

Ольга Книжникова,
директор Троицкого отделения
Общества «Знание»

Социальная инженерия: почему люди сами отдают мошенникам деньги

Великий комбинатор Остап Бендер чтил уголовный кодекс. Банальному грабежу он предпочитал психологические уловки, чтобы жертвы его обаяния добровольно отдавали ключи от квартир, где деньги лежат. Позже для таких махинаций придумали специальное название — социальная инженерия. Рассказываем, какие схемы социальные инженеры используют сегодня и как от них защититься.

Кто такие социальные инженеры?

В широком смысле — это специалисты, которые умеют манипулировать другими. Но обычно мы слышим о тех социальных инженерах, которые с помощью психологических приемов выманивают деньги или данные для доступа к чужому счету.

По статистике в большинстве случаев люди теряют свои сбережения не потому, что их счета взламывают хакеры. Владельцы банковских карт чаще всего сами сообщают мошенникам их полные реквизиты, включая номер, срок действия, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций.

Если вы сами передали мошеннику секретные данные, банк не обязан компенсировать похищенное.

Даже самые умные и осторожные люди иногда попадаются на крючок к махинаторам. Разбираем самые распространенные психологические уловки, которые используют мошенники.

Вызвать доверие

Мошенники часто представляются теми, от кого люди не ждут подвоха: сотрудниками банков, налоговой службы, юридических контор и других официальных организаций.

Социальный инженер может прикинуться вашим приятелем или родственником, например, взломав или сделав дубликат их аккаунтов в соцсетях.

Обычно, прежде чем выйти на контакт, социальные инженеры стараются узнать о потенциальной жертве как можно больше. Они выясняют данные человека, чаще всего — с помощью фишинговых сайтов. Или покупают готовые информационные базы с персональными данными, которые утекли в сеть.

Нередко люди и сами публикуют в соцсетях номера телефонов, электронные адреса и даже выкладывают фотографии своих банковских карт.

Этой информации недостаточно, чтобы сразу украсть деньги. Но вполне хватит для того, чтобы начать разговор и усыпить бдительность. Когда махинаторы обращаются к людям по имени и отчеству, сами называют номер карты или другие конфиденциальные данные, кажется, что они действительно представляют знакомую организацию или человека.

Подделать телефонные номера, документы и сайты

Часто трудно сразу догадаться, что имеешь дело с мошенниками. Они умеют виртуозно маскироваться:

- Подменяют номер, с которого звонят или присылают сообщение. С помощью специального программного обеспечения им удается скрыть настоящий номер, а у вас на экране во время их звонка отображается, например, знакомый телефон банка.
- Подделывают документы: с помощью Фотошопа преступники создают фейковые налоговые уведомления, квитанции о штрафах, счета за квартиры и присылают их на домашний адрес, по СМС или электронной почте. Если человек оплатит такое уведомление, все деньги уйдут к мошенникам:
- Копируют сайты банков, микрофинансовых организаций, страховых компаний, популярных онлайн-магазинов, а также порталы объявлений и платежные страницы. Мошенники рассчитывают, что пользователь либо сразу переведет деньги на их счет, либо оставит конфиденциальные данные своей банковской карты.

Запугать потерей денег

Вызвать страх — уже полдела для обманщика. Испуганный человек гораздо лучше поддается внушению. Например, мошенник звонит «из службы безопасности банка» и сообщает, что по карте «прямо сейчас» проводится подозрительная операция.

Растерянному «клиенту» предлагают срочно назвать трехзначный код с обратной стороны карты, чтобы отменить транзакцию. Или перевести деньги на некий «безопасный счет».

Если человек поддастся панике и выполнит инструкции «экспертов», то, не ведая того, он сам отправит все сбережения мошенникам.

Заманить выигрышем

Мошенники активно эксплуатируют стремление людей к легкому обогащению. Они создают специальные сайты с аттракционами невиданной щедрости. Например, предлагают пройти опрос с заманчивым денежным вознаграждением или поучаствовать в «беспроигрышных» конкурсах, получить социальные выплаты или вернуть налоги.

Эти сайты махинаторы рекламируют в социальных сетях, рассылают в мессенджерах, по электронной почте и СМС. Нередко подобная реклама сопровождается фотографиями и склеенными нарезками из видео с медийными персонами, которые призывают людей участвовать в этой афере. Перейдя по ссылке на сайт конкурса или лотереи, человек видит множество восторженных отзывов от тех, кто якобы уже получил свои деньги.

Однако в реальности вместо денежных призов людей ждут лишь убытки. Организаторы схемы под разными предлогами просят их ввести данные карты, чтобы оплатить символический налог, услуги «юристов» или комиссию за участие. Основная опасность кроется не в потере незначительной суммы. После того как человек оставляет конфиденциальную информацию на фишинговой странице, мошенники получают доступ к деньгам на его счете.

Восстановить справедливость

Как правило, махинаторы ведут базы данных людей, которые уже однажды поддались на их обман и могут снова клюнуть на их уловки. Тем, кто потерял деньги на финансовых пирамидах, псевдолотереях и прочих лохотронах, мошенники предлагают «компенсации».

Цель все та же — под предлогом оплаты «услуг юриста» или «комиссии за перевод денег» человека убеждают указать полные реквизиты карты, чтобы он снова получил шанс потерять свои деньги.

Использовать громкие информационные поводы

Мошенники активизируются на фоне различных катастроф, стихийных бедствий и эпидемий. Например, во время пандемии коронавируса обманщики собирали деньги «на разработку вакцины» под видом Всемирной организации здравоохранения.

Социальные инженеры следят за новостями и настроениями и быстро адаптируются к текущей ситуации. В период самоизоляции они рассылали всем подряд СМС о «штрафе» за нарушение карантина со ссылкой на несуществующие законы.

От имени авиакомпаний предлагают «компенсации» за отмененные рейсы в обмен на секретные данные банковской карты.

Не дать время на размышления

Мошенники специально торопят и давят, чтобы лишить человека возможности принять взвешенное решение в спокойной обстановке. Они требуют немедленно перевести деньги, срочно оплатить какую-либо услугу, «как можно скорее» назвать секретный номер, пароль или код.

«Звонит незнакомый мужчина и говорит, что по ошибке прислал мне 30 000 рублей. Просит отправить их ему по номеру карты, который мол сейчас продиктует. Я так прикинул, что это развод и положил трубку. Проверяю мобильный банк, а деньги реально пришли. Тут тот мужчина звонит еще раз и начинает орать в трубку...»

Если вы чувствуете явный прессинг, когда пытаетесь принять какое-либо финансовое решение, это верный признак, что вы имеете дело с махинаторами. При малейших подозрениях кладите трубку и сами звоните в банк по телефону горячей линии — он есть на сайте организации и на оборотной стороне банковской карты.

Как обезопасить себя от социальных инженеров?

Аферисты постоянно придумывают новые схемы обмана. Единственный способ избежать денежных потерь при встрече с мошенниками — критически воспринимать любые предложения, перепроверять информацию и никогда не торопиться при принятии финансовых решений.

Следуйте базовым правилам финансовой безопасности:

- Никому ни при каких обстоятельствах не сообщайте полные реквизиты банковской карты, включая трехзначный код с обратной стороны; а также ПИН-коды и пароли из СМС от банка.
- Не переходите по сомнительным ссылкам из сообщений и не переводите незнакомцам деньги по первому требованию.
- Не храните много денег на карте, которой расплачиваетесь в Интернете: кладите только ту сумму, которую собираетесь потратить в данный момент. В этом случае, даже если мошенники попытаются украсть деньги, им не удастся вывести слишком много.
- Получив внезапный звонок из какой-либо финансовой организации со срочным вопросом или предложением, положите трубку и позвоните туда сами, найдя номер на ее официальном сайте. Набирайте этот номер вручную. Если с вами связались из компании, клиентом которой вы не являетесь, сначала проверьте ее по справочнику финансовых организаций.
- Не соглашайтесь сходу ни на какие «заманчивые предложения» — будь то «выгодный кредит» или внезапная компенсация. Дайте себе время на размышление, посоветуйтесь со знакомыми, пробейте в Интернете информацию о компании и «уникальной акции», которую она вам рекламирует.
- Не публикуйте в открытом доступе свои персональные данные: номер телефона, домашний адрес, данные паспорта. Мошенники охотно задействуют эту информацию в своих аферах.

Проект «Цифровая самооборона» реализуется с использованием гранта Фонда поддержки гражданских инициатив Южного Урала

Как быстро распознать мошенника

У Ивана Сергеевича зазвонил телефон, номер был незнаком. Солидный мужской голос на фоне шума офиса звучал встревоженно: «Добрый день. Иван Сергеевич? Это служба безопасности банка “Лапша-Финанс”. Мы зафиксировали, что киберпреступники пытаются получить доступ к вашему личному кабинету. Надо срочно перевести все деньги на безопасный счет, иначе их украдут!» Иван Сергеевич немедленно положил трубку. Рассказываем, по каким признакам он вычислил обманщиков.

Аферисты постоянно придумывают новые способы выманить у людей деньги или конфиденциальные данные для доступа к счетам. Но какой бы ни была легенда, есть пять примет, по которым можно сразу же вычислить мошенников.

Признак 1. На вас выходят сами

Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере. Кем бы он ни представился — сотрудником банка, полиции, магазина, вашим троюродным братом-миллионером из Зимбабве — насторожитесь. Раз он стал инициатором контакта, ему что-то от вас нужно.

Быстро проверить, тот ли он, за кого себя выдает, не получится. Номер, который высвечивается при входящем вызове, можно подменить, аккаунты или сайты известных людей или организаций— подделать. Так что стоит быть бдительным и никому не верить на слово.

Признак 2. С вами говорят о деньгах

Основная задача мошенников — получить доступ к чужим деньгам. Схемы обмана почти всегда связаны с финансами: вам предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно» инвестировать свои сбережения (на самом деле — в финансовую пирамиду).

«На днях бабушке позвонили якобы из службы безопасности ее банка. Сказали, что с ее карточки кто-то только что попытался украсть деньги. Они операцию заблокировали, но деньги надо срочно перевести на некий безопасный счет...»

Легенды могут быть какими угодно, но речь всегда про деньги — которые вы можете потерять или получить.

Признак 3. Вас просят сообщить данные

Если ворам нужны ключи от квартиры, то социальным инженерам— «ключ» к деньгам на ваших счетах. Это могут быть конфиденциальные данные вашей карты, включая срок действия и три цифры с ее обратной стороны. Либо логины и пароли к личному кабинету на сайте банка или мобильному приложению. И почти всегда — коды из банковских уведомлений.

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли.

Когда банк замечает сомнительный платеж или перевод с вашего счета, с вами связываются, чтобы подтвердить или отклонить операцию, и только. Конфиденциальные данные для этого не требуются. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.

Признак 4. Вас выводят из равновесия

Мошенники стремятся вызвать у вас сильные эмоции — напугать или обрадовать. Так они сбивают с толку и притупляют бдительность потенциальной жертвы. Например, сообщают: «Ваш онлайн-банк взломали!», чтобы вы от растерянности и волнения выполнили любые просьбы и выдали любую информацию, лишь бы спасти деньги.

Либо, наоборот, огорошивают новостью о внезапном выигрыше в лотерею или обещают быстрое обогащение. Взамен вы должны будете «лишь оплатить небольшой взнос», а для этого — ввести данные банковской карты на сайте. Мошенники создают фишинговые страницы, с помощью которых воруют данные карт и получают доступ к банковским счетам доверчивых пользователей.

«Участвовала в конкурсе в соцсети около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала кроссовки, написала организаторам, после чего мне предложили оплатить доставку в размере 450 ₽...»

Всегда сохраняйте здоровый скептицизм и не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.

Признак 5. На вас давят

Мошенники всегда торопят, чтобы не дать вам времени обдумать ситуацию. Вас принуждают к чему-то, ставят условия: «сейчас или будет поздно». Ситуация, в которой вам не дают права выбора и заставляют немедленно действовать, подозрительна.

Если чувствуете психологический дискомфорт, лучше сразу же прекращайте общение. Ведь чем дольше вы разговариваете с мошенником, тем сильнее он будет на вас давить. На все ваши расспросы у обманщиков есть заготовленные ответы, которые только нагнетают обстановку.

«Попал в ужасную ситуацию. Позвонили из моего банка, назвали мое Ф.И.О. и попросили подтвердить, что я сейчас оформляю кредит на 550 000 рублей. Я очень удивился, потому что ничего не оформлял в тот момент. Сотрудник банка сказал, что если это не я, значит мошенники пытаются взять кредит от моего имени, поэтому надо срочно принять меры».

Никогда не принимайте поспешных решений, особенно если они касаются ваших финансов. Всегда берите паузу, чтобы разобраться в том, что происходит. Возьмите за правило перепроверять любую информацию в первоисточнике.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.

Прислали странное уведомление от имени Федеральной налоговой службы (ФНС)? Заведите личный кабинет на сайте ФНС — в нем можно проверить суммы налогов и сразу же оплатить их.

Получили «письмо счастья» о государственной выплате? Поищите новости об этом в деловых СМИ. А еще лучше — найдите сам закон, указ или постановление, которые вводят выплаты. Обратите внимание на условия, кому они положены.

Не всегда при общении с аферистом вы заметите все пять признаков мошенничества. Но в любой ситуации стоит проявить бдительность.

Как еще защитить свой аккаунт на «Госуслугах»?

Зайдите в раздел «Безопасность». На вкладке «Вход в систему» перечислены разные способы защиты. Чтобы включить любой из них, передвиньте ползунок в нужной графе.

Выберите один или несколько вариантов:

• Установите вход с подтверждением по СМС. При каждой авторизации на ваш мобильный будет приходить новый код для входа. Перед тем как подключать услугу, убедитесь, что в профиле записан актуальный номер телефона.

• Настройте уведомление о входе на «Госуслуги» по электронной почте. Вы будете получать письмо каждый раз, когда вы или кто-то другой будет заходить в ваш аккаунт. Заранее проверьте, верно ли указан ваш e-mail.

• Создайте контрольный вопрос — он защитит вас в случае, если мошенники попытаются инсценировать ситуацию, что вы забыли пароль и хотите восстановить его с помощью кодов из СМС и почты. Даже когда им удастся узнать секретные цифры, они не смогут войти в ваш профиль без правильного ответа на контрольный вопрос. Вы сами выбираете тему, но не устанавливайте слишком простые вопросы, ответы на которые легко найти в ваших соцсетях — например, про даты рождения близких или клички животных.

Не раскрывайте никому свои логин и пароль, паспортные данные, не называйте коды из СМС. Помните, что сотрудники «Госуслуг» не обратятся к вам сами, если вы не подавали им никаких заявок. Если кто-то без вашей инициативы звонит и общается с вами от имени портала, лучше всего повесить трубку.

Когда в почте вы видите письмо от «Госуслуг» о выплатах, штрафах или с информацией, которую вы не запрашивали, не торопитесь кликать по ссылке. Посмотрите адрес отправителя. Настоящие письма от портала приходят только с почты no-reply@gosuslugi.ru.

Зайдите на сайт или в приложение «Госуслуг» и проверьте, есть ли такое же уведомление в личном кабинете.

Помните, что мошенники часто создают поддельные сайты. Поэтому внимательно сверяйте символы в адресной строке страницы, на которой находитесь. Введете логин и пароль от «Госуслуг» на фальшивом портале — злоумышленники смогут взломать ваш аккаунт и набрать кучу займов на ваше имя. А если оставите на поддельной странице свои платежные данные (например, для оплаты штрафа или оформления субсидии), с вашей карты украдут все деньги.

Мошенники создали фальшивые госреестры для «проверки сотрудников банков»

Аферисты нашли новый способ втираться к людям в доверие. Они запугивают человека, что с его банковским счетом или картой что-то происходит, и тут же предлагают собеседнику самостоятельно проверить достоверность информации и их полномочия.

По словам мошенников, это можно сделать на сайте «Единого государственного реестра сотрудников банков». Иногда людям предлагается перейти на другие ресурсы с похожим названием, которые также выдаются за официальные. Хотя на самом деле никаких реестров для проверки сотрудников банков не существует.

По телефону аферист сообщает выдуманные имя и должность, а также код — «личный идентификатор сотрудника». Этот код предлагается вбить на сайте реестра. Когда человек вводит цифры идентификатора, он видит те же данные, что ему сказали по телефону. И может поверить, что на связи настоящий работник банка.

Чтобы сбить собеседника с толку, на поддельных сайтах, помимо информации о выдуманных сотрудниках, для правдоподобности публикуются данные известных банковских руководителей с фото, добавляются ссылки на официальные сайты банков и портал «Госуслуги».

Когда человек проверил код сотрудника банка, злоумышленники сообщают ему «личный идентификатор клиента» и предлагают запросить в том же реестре сведения о своих счетах. Человек вводит новый код, и на сайте появляется информация, что от его имени кто-то запросил кредиты в разных банках. Там же дается рекомендация: следовать инструкциям уже проверенного по базе сотрудника, чтобы отменить эти заявки.

Затем мошенники убеждают жертву попытаться «опередить злоумышленников». Для этого якобы нужно самому оформить кредиты и вывести средства на «безопасный счет». Но если так поступить, деньги просто уйдут преступникам, а доверчивый человек останется с долгами.

В реальности госслужащие и банковские сотрудники никогда не предлагают переводить деньги на «защищенные счета» и тем более оформлять настоящие кредиты для отмены заявок от мошенников. Если незнакомец сообщает о подозрительных операциях по банковскому счету или карте, лучше повесить трубку и самостоятельно позвонить в свой банк по номеру горячей линии. Его можно найти на обратной стороне банковской карты или на официальном сайте банка.

Материалы на 2-й и 3-й страницах газеты получены с сайта «Финансовая культура», созданного Центральным банком РФ. URL: https://fincult.info/

Коркино участвует в «Цифровой самообороне»

Проект «Цифровая самооборона» реализуется на территории Коркинского муниципального округа с использованием гранта губернатора Челябинской области, предоставленного Фондом поддержки гражданских инициатив Южного Урала.

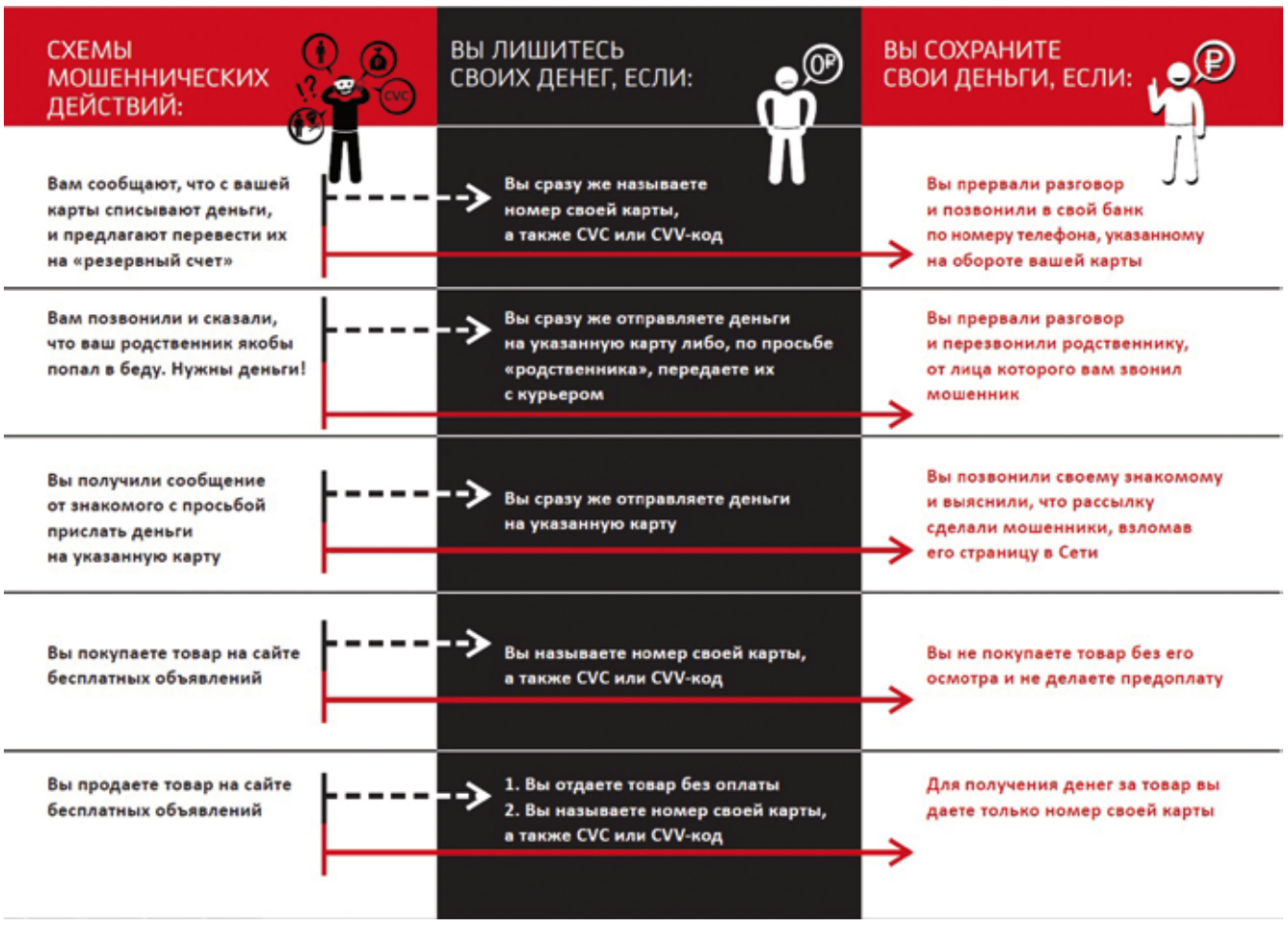
За время реализации проекта проведено более двадцати лекции, охват слушателей превышает 250 человек. Кроме профилактических лекций проводятся тренинги, для того, чтобы люди смогли в игровой форме понять психологию мошенника и жертвы.

Самые популярные темы лекций «Финансовое мошенничество. Как защитить себя», «Безопасность в социальных сетях», «Финансовая безопасность. Лжеюристы», «Навязчивые звонки из банков и как законно с ними бороться». Для чтения лекций приглашаются представители надзорных органов, полиции и прокуратуры, сотрудники финансовых организаций. Преподаватель курса «Цифровая и финансовая безопасность» Лариса Куркина начинает занятия по основам мобильной и компьютерной грамотности с информации о мошеннических действиях и о том, как не попасть на уловку мошенников. Предлагает слушателям не вступать в разговор с незнакомыми людьми по телефону, перезванивать близким, если поступает звонок «о попавшем в беду родственнике», не отвечать на входящие звонки словом «Да».

Участниками лекций становятся пенсионеры, которые приходят на занятия в Общество «Знание», в клубы по рукоделию, работающие со старшим поколением на территориях библиотек, творческие коллективы и работающие пенсионеры. Каждый слушатель узнает для себя новую и полезную информацию, с которой охотно делится со своими родными и близкими. «Если я поделюсь полезной информацией со своими соседями, которые не посещают лекции по состоянию здоровья, надеюсь, что хотя бы так я смогу предостеречь доверчивых пенсионеров от мошеннических действий», — говорит Любовь Валентиновна Кузьменок.

«Лекции, которые организует и проводит для нас, пенсионеров, Общество «Знание», всегда наполнены полезной и актуальной информацией. Интересные лекторы, которые приводят очень много примеров. Когда я читаю про то, как обманывают пенсионеров в других городах, думаю, что меня это не коснется. Но услышав статистику от сотрудника полиции, сколько пострадало от рук мошенников коркинцев, надеюсь что с полученными знаниями меня минует эта участь. Конечно нужно быть бдительными и осторожными при общении с незнакомцами» — делится Лира Николаевна Дерябина, постоянный слушатель Народного университета.

Лариса Куркина, директор Коркинского отделения Общества «Знание»



Информационные ресурсы Общества «Знание»

Сайт организации http://www.znanie74.ru/
Живой журнал https://znanie74.livejournal.com/
Группа в Одноклассниках https://www.ok.ru/group/znanie74
ВКонтакте https://vk.com/znanie_174
Видеоканал https://www.youtube.com/user/znanie174
Телеграм https://t.me/znanie_174
Яндекс Дзен https://zen.yandex.ru/ Канал Znanie174
Архив газеты «НАРОДНЫЙ УНИВЕРСИТЕТ» https://ru.calameo.com/accounts/5028721
Электронная почта info@znanie74.ru **Телефоны: 8(351) 219-37-57, 8 912 803 89 39**

Коркинское отделение

Страница в «Одноклассниках» — Общество Знание город Коркино https://ok.ru/
Страница сообщества в «ВК» Общество Знание город Коркино https://vk.com/public149052136
Адрес эл. почты znanie_korkino@mail.ru
Адрес: г. Коркино, ул. Маслова, 15, первый этаж. **Телефон 8 919 33 97 009.**

Троицкое отделение:

Адрес эл. почты: trznanie@rambler.ru
Страница сообщества в «ВК» https://vk.com/club213266315
Адрес: г. Троицк, ул. Гагарина, 1 (2-й этаж).
Телефон +7 982 325 94 38

НАРОДНЫЙ УНИВЕРСИТЕТ
№ 1(28), июль 2023 года

Ответственный за спецвыпуск: В. Лушников
Издатель Общество «Знание»
Адрес: 454091, Челябинск, ул. Васенко, 63.
Телефон: +7 (351) 219-69-05. E-mail: info@znanie74.ru
Сайт: www.znanie74.ru. Живой журнал: znanie74.livejournal.com
Распространяется бесплатно
Отпечатано в ОАО «Челябинский Дом печати» (Челябинск, Свердловский проспект, д. 60) с готового оригинал-макета.
Заказ № _____ Тираж 999 экз.