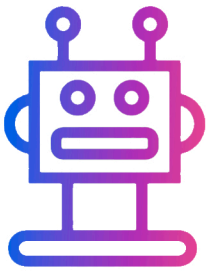
КИБЕРДИКТАНТ.РФ

ПО ФИНАНСОВОЙ IT-ГРАМОТНОСТИ

Работа над ошибками для аудитории 18+



Российская государственная детская библиотека

Банк России

Координационный центр доменов .RU/.РФ

РОЦИТ

Министерство культуры Российской Федерации

Вопрос № 1

Какой пароль из предложенных ниже, на ваш взгляд, является наиболее безопасным?

а) 12345678

б) q1w2e3r4

в) AwThn88+ (правильный ответ)

г) 16.04.1982

Специалисты в области информационной безопасности рекомендуют следовать следующим требованиям при выборе надежного пароля: минимум 8 символов, использование заглавных и строчных букв, а также цифр и знаков. Важно помнить и о периодическом обновлении пароля.

Вопрос № 2

Как называется набор психологических техник, который используется преступниками для получения конфиденциальных данных жертв или побуждения к выполнению определенных действий, необходимых злоумышленникам?

а) Социальная помощь.

б) Социальная инженерия. (правильный ответ)

в) Социальное обслуживание.

г) Социальное исследование.

Мошенники создают такие условия, при которых пользователи добровольно передают им свои конфиденциальные данные или сбережения. Подобный прием «взлома» сознания людей называется социальной инженерией. Большая часть несанкционированных операций происходит именно с помощью методов социальной инженерии, яркими примерами которой являются звонки от «службы безопасности банка», разнообразные СМС с просьбой вернуть ошибочно перечисленные денежные средства или о том, что ваша карта заблокирована.

Вопрос № 3

Какие действия, приведенные ниже, может совершать устройство, зараженное вредоносным программным обеспечением?

а) Предоставлять удаленный доступ к содержащейся на нем информации.

б) Распространять вредоносные программы на другие устройства.

в) Выполнять расчетные операции в интересах злоумышленника.

г) Все ответы верные. (правильный ответ)

Переход по подозрительным ссылкам или открытие подозрительных файлов может привести к заражению устройства вредоносным программным обеспечением, которое способно предоставлять удаленный доступ к содержащейся на компьютере или другом гаджете информации, распространять вредоносные программы на другие устройства, а также выполнять расчетные операции в интересах злоумышленника. Все варианты верные.

Вопрос № 4

Как называется вид мошенничества в Интернете, целью которого является получение доступа к конфиденциальным данным пользователей?

а) Майнинг.

б) Троллинг.

в) Фишинг. (правильный ответ)

г) Скимминг.

Фишинг – это очень распространенный вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователей. Разнообразные фишинговые сайты завлекают жертв супервыгодными предложениями о продаже мобильной техники, услуг, недвижимости и т.д. для того, чтобы ничего не подозревающие граждане оставили злоумышленникам свои контактные данные или данные банковских карт.

Вопрос № 5

Кому можно передавать данные секретного кода на обороте карты (CVV/CVC)?

а) Сотрудникам банка.

б) Сотрудникам правоохранительных органов.

в) Друзьям и родственникам.

г) Никому. (правильный ответ)

Сообщать CVV/CVC-код кому-либо строго запрещено. Сотрудник банка никогда не будет интересоваться информацией о сроке действия вашей карты или о CVV/CVC-коде. Также стоит помнить, что коды, которые приходят по СМС для подтверждения покупки или перевода денежных средств, тоже являются секретной информацией.

Вопрос № 6

Какие действия необходимо выполнить в случае обнаружения несанкционированных операций по вашей карте?

а) Обратиться в банк, который выпустил карту, а затем - в полицию. (правильный ответ)

б) Обратиться к родственникам и друзьям.

г) Обратиться к оператору связи.

д) Обратиться в ближайший МФЦ.

Если вы обнаружили несанкционированные списания со счета, то в первую очередь обратитесь в банк (номер клиентской поддержки указан на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту. Далее необходимо запросить выписку по счету и написать заявление о несогласии с операцией. И, наконец, обратиться с заявлением в отдел полиции по месту жительства или отправить обращение в управление «К» МВД России на сайте мвд.рф.

Вопрос № 7

Что заранее следует предпринять, чтобы свести к минимуму потери при краже или утере бесконтактной банковской карты?

а) Установить максимальный суточный лимит расходования средств. (правильный ответ)

б) Установить минимальный суточный лимит расходования средств.

в) Передать карту родственнику.

г) Ничего не предпринимать.

Максимальный суточный лимит – хороший способ дополнительно обезопасить средства на счете. В настоящее время суточный лимит в большинстве случаев устанавливается банком автоматически, но всегда можно настроить его в приложении или обратиться в банк напрямую.

Вопрос № 8

На вашу электронную почту пришло письмо от банка, услугами которого вы пользуетесь, с информацией, что необходимо обновить пароль от личного кабинета, перейдя по ссылке, так как предыдущий пароль устарел. Что вы сделаете?

а) Перейдете по ссылке, чтобы поменять пароль.

б) Перед тем как перейти по ссылке, позвоните в банк по номеру телефона, указанному на официальном сайте банка или на обратной стороне банковской карты, чтобы уточнить, действительно ли банк рассылает такие уведомления. (правильный ответ)

в) Не будете ничего предпринимать. Изменение пароля не требуется.

г) Перешлете письмо знакомым, которые пользуются услугами этого банка, чтобы они тоже поменяли пароль.

Перед тем, как выполнять подобные действия, обязательно нужно удостовериться в отправителе, и звонка в банк для этого будет вполне достаточно.

Вопрос № 9

В кафе вы решили расплатиться за обед банковской картой. Какой из вариантов расчета правильный?

а) Официант возьмет карту вместе со счетом на кассу и после оплаты принесет вам чек.

б) Официант придет с терминалом к вашему столику и при вас выполнит необходимые операции. (правильный ответ)

в) Официант перепишет номер, срок действия карты, CVV и произведет платеж позднее, чтобы не задерживать вас.

г) Официант сфотографирует данные вашей карты, чтобы произвести платеж, когда ему будет удобно.

Правила безопасности требуют, чтобы расчет был произведен при вас. Официант должен произвести все необходимые манипуляции в вашем присутствии. Данные о сроке действия карты и CVV/CVC-код являются конфиденциальной информацией, их нельзя передавать третьим лицам.

Вопрос № 10

Вы изучаете новинки гаджетов и находите сайт, где предлагается приобрести новую модель ноутбука с большой скидкой (более 50%) относительно стоимости в официальном магазине. Акция подходит к концу, о чем вам сообщает соответствующий рекламный баннер. Вам нужно лишь ввести данные банковской карты, и вы получите желанный компьютер. Стоит ли доверять такому сайту?

а) Буду ориентироваться по отзывам на этом сайте, наверняка другие пользователи делились своими впечатлениями.

б) Введу свои данные, тем более что акция на покупку ноутбука очень скоро завершится.

в) Не буду вводить данные банковской карты. Скорее всего, это мошенничество. (правильный ответ)

г) Оформлю заказ и поделюсь ссылкой с друзьями.

Эта ситуация – яркий пример фишинга. Злоумышленники завлекают жертв, обещая товар или услугу с большой скидкой, чтобы завладеть данными пользователя или побудить его совершить «покупку». Отзывы на таких сайтах – поддельные, а товар, разумеется, к вам никогда не придет.

Вопрос № 11

На номер вашего мобильного телефона позвонил человек, который представился сотрудником службы безопасности банка, услугами которого вы пользуетесь. Он обратился к вам по имени и сообщил, что банк обнаружил подозрительную операцию, которую пытаются совершить по вашей карте. Чтобы остановить мошенников, нужно срочно назвать одноразовый пароль, который придет через несколько секунд по SMS на номер вашего телефона. Что бы это значило?

а) Сотрудник хочет помочь мне, даже позвонил лично, я сейчас же продиктую ему код.

б) Это мошенник! Банки никогда бы не стали торопить своих клиентов и просить назвать им код из SMS. Я закончу разговор и позвоню по номеру банка, указанному на обратной стороне карты или официальном сайте. (правильный ответ)

в) Продолжу разговор и попытаюсь выяснить подробности произошедшего.

г) Попрошу его выслать подробности на электронную почту, чтобы продолжить общение там.

Данная ситуация является примером социальной инженерии. В подобной ситуации необходимо прервать разговор и перезвонить в свой банк, чтобы зафиксировать факт попытки мошенничества, который будет отражен в общей статистике. Банк передаст информацию о номере телефона звонившего в Банк России для проверки и дальнейшего принятия мер.

Вопрос № 12

Вы получили SMS, в котором написано, что на вашу банковскую карту поступили деньги. А через некоторое время вам звонит незнакомый

человек и просит вернуть средства обратно, так как обнаружил, что перевод был совершен ошибочно. Как быть?

а) Перевести требуемую сумму. С кем не бывает?

б) Проигнорировать просьбу и добавить его номер телефона в черный список.

в) Войти в личный кабинет мобильного банковского приложения, посмотреть баланс и историю операций, а также уточнить информацию в банке, позвонив по номеру горячей линии, указанному на официальном сайте банка или обратной стороне банковской карты. (правильный ответ)

г) Договориться встретиться, чтобы отдать денежные средства лично.

Скорее всего, это мошенничество с использованием социальной инженерии. Удостоверьтесь в отсутствии подозрительных транзакций и обратитесь с банк.

Вопрос № 13

Вам пришло такое SMS: «Уважаемый клиент! Ваша карта 1234 1234 1234 1234 (указан номер вашей карты) заблокирована. Для разблокировки свяжитесь с сотрудником Банка по номеру +7 912 345 67 89». Что нужно сделать?

а) Нужно позвонить по указанному номеру, чтобы разблокировать карту.

б) Данное сообщение прислали мошенники. Нельзя звонить по указанному номеру. Необходимо позвонить по номеру горячей линии, указанному на официальном сайте банка или обратной стороне банковской карты, чтобы проконсультироваться. (правильный ответ)

в) Отправлю ответное SMS, чтобы узнать подробности произошедшего.

г) Перезвоню по номеру, с которого пришло SMS.

Еще один пример мошенничества с использованием социальной инженерии. Не звоните по указанному номеру и не отвечайте на SMS. Не переживайте и обратитесь в банк.

Вопрос № 14

В сети вы увидели заманчивое предложение разместить свои накопления в инвестиционной компании, которая обещает гарантированно доход в размере 2% в месяц от инвестированной суммы. Как следует поступить?

а) Обязательно воспользоваться данным предложением, так как оно очень выгодное.

б) Стоит позвонить в эту компанию и узнать подробности предложения.

в) Необходимо обратиться в Банк России через онлайн-приемную (https://cbr.ru/Reception), чтобы проконсультироваться. (правильный ответ)

г) Сообщу о такой возможности друзьям, чтобы инвестировать вместе.

За такой высокой процентной ставкой часто стоят мошенники – лжеброкеры и финансовые пирамиды. Не торопитесь отдавать им свои денежные средства. Вы всегда можете проконсультироваться по подобным вопросам в Банке России.

Вопрос № 15

В социальной сети вы увидели рекламу, которая сообщает вам о возможности получения компенсационных выплат от государства, например, по уплаченному налогу на добавленную стоимость (НДС), в связи с карантинными мероприятиями из-за пандемии COVID-19 или за приобретенные лекарственные средства. Что это может быть?

а) Таким образом государственные органы информируют граждан о возможности получения выплат.

б) Подобную рекламу размещают активные граждане или компании, чтобы привлечь внимание людей к возможности получения выплат от государства.

в) Таким способом злоумышленники заманивают жертв, чтобы украсть их денежные средства и конфиденциальные данные. (правильный ответ)

г) Такую рекламу размещают социальные сети самостоятельно, чтобы проверить бдительность граждан.

Подобная реклама часто встречается в социальных сетях. Ни в коем случае нельзя переходить по таким ссылкам, поддавшись на уловки злоумышленников. Официальную информацию необходимо искать на сайтах, принадлежащих соответствующим ведомствам, или обращаться в единую справочную службу вашего населенного пункта.

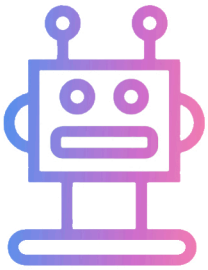
Банк России

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

РОЦИТ

МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Кибердиктант.рф
по финансовой IT-грамотности



Сертификат

выдан

Верхоланцевой Надежде Сергеевне

участнику Всероссийского кибердиктанта по финансовой IT-грамотности,
проходившего 24 октября – 1 ноября 2020 года
в рамках Недели финансовой грамотности

Председатель оргкомитета
Всероссийского кибердиктанта
по финансовой IT-грамотности,
Директор РГДБ

Веденяпина М.А.

Москва
2020