5. МОШЕННИЧЕСТВО на торговых площадках

- Мошенничество на торговых площадках – взаимодействие с клиентом от имени покупателя/продавца посредством различных мессенджеров с целью завладения денежными средствами держателя.

Как это работает?

- Мошенник пишет не на сайте торговой площадки, а в мессенджере лично продавцу, и говорит, что готов приобрести товар по предоплате.
- Высылает ссылку на поддельную страницу, для получения якобы предоплаты, где держатель вводит данные своей карточки.
- Часто мошенники пишут с номеров, которые не зарегистрированы на территории Республики Беларусь.
- Могут прислать поддельный чек об оплате доставки/пересылки товара.

КАК ЗАЩИТИТЬСЯ:

- Не сообщайте реквизиты карточки, коды и личные данные.
- Не проходите по ссылкам, для осуществления сделки не покидайте пределы торговой площадки.
- Для получения перевода или оплаты Вам не требуется вводить CVV2/CVC2-код – трехзначное число на обороте карточки!
- Позвоните покупателю, чтобы убедиться, что у Вас есть его реальный номер телефона. Вас должно насторожить, когда продавец/покупатель под любым предлогом пытается избежать личного общения по телефону.

6. СТРАННЫЙ БАНКОМАТ

- Банкомат зависает, перезагружается.
- На экране подозрительные изображения.
- Вокруг картоприёмника подозрительные материалы (следы клея, провода и т.п.).
- Несовпадение формы, материала, цвета, контуров деталей банкомата.
- Вблизи есть другие подозрительные устройства.

КАК ЗАЩИТИТЬСЯ:

НЕ ПОЛЬЗУЙТЕСЬ, сообщите в банк по телефонам, указанным на банкомате.

А ЕСЛИ УЖЕ СЛУЧИЛОСЬ...?

ПОДОЗРЕВАЕТЕ НЕСАНКЦИОНИРОВАННЫЕ ОПЕРАЦИИ (МОШЕННИЧЕСТВО) ПО ВАШЕЙ КАРТОЧКЕ ИЛИ С ИСПОЛЬЗОВАНИЕМ ВАШИХ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Срочно заблокируйте карточку (карточки) в ДБО (интернет-банкинге), SMS-банкинге или обратившись в круглосуточную службу сервиса клиентов по телефонам, указанным на обороте Вашей карточки. Затем обратитесь в банк, выпустивший карточку, и следуйте инструкциям специалиста.

РАЗГЛАСИЛИ ТРЕТЬИМ ЛИЦАМ ДАННЫЕ ДЛЯ ВХОДА В ДБО ИЛИ МСИ?

Срочно измените пароль для входа в систему или заблокируйте аккаунт (по звонку в банк или в случае разглашения доступа к МСИ в контакт-центре АИС «Расчет» ЕРИП – 141).

ПОТЕРЯЛИ БАНКОВСКУЮ ПЛАТЕЖНУЮ КАРТОЧКУ?

Срочно заблокируйте карточку в ДБО (интернет-банкинге), SMS-банкинге или обратившись в круглосуточную службу сервиса клиентов по телефонам, указанным на обороте Вашей карточки Затем обратитесь в банк, выпустивший карточку, для её перевыпуска.

БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

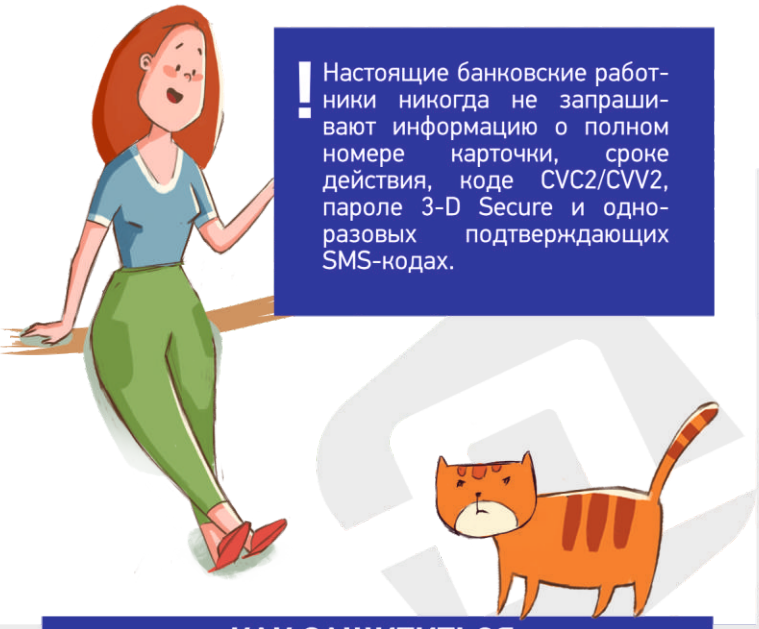
БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

РЕКОМЕНДАЦИИ КАК НЕ ДАТЬ СЕБЯ ОБМАНУТЬ

6 СХЕМ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТОЧКАМИ

1. ЗВОНОК «СОТРУДНИКА БАНКА»

- Мошенники представляются работниками банка, службы сервиса клиентов или представителями любых других организаций.
- Могут использовать скрытые телефонные номера или специальные программы, подменяющие номера телефонов на реальные номера, размещенные на официальных ресурсах организаций.
- В разговоре запрашивают реквизиты вашей банковской карточки, логины и пароли, SMS-коды, сеансовые ключи к интернет-банкингу и мобильным приложениям, просят перевести деньги на другой счет или установить приложение для удаленного доступа к вашему устройству с интернет-банкингом.



! Настоящие банковские работники никогда не запрашивают информацию о полном номере карточки, сроке действия, коде CVC2/CVV2, пароле 3-D Secure и одноразовых подтверждающих SMS-кодах.

КАК ЗАЩИТИТЬСЯ:

- Прервите разговор, не сообщайте реквизиты банковской карточки, логины и пароли, SMS-коды, сеансовые ключи к интернет-банкингу и мобильным приложениям.
- Не переводите деньги на другой счет.
- Не устанавливайте приложение.
- Обратитесь в банк по номерам телефонов, указанным на официальном сайте, или в круглосуточную службу поддержки клиентов по телефонам, указанным на обороте Вашей карточки.

2. «РОДСТВЕННИК» или «ДРУГ» в социальной сети

- Могут быть похожи на письма, которые приходят из банка или из других официальных организаций.
- Содержат призыв к выполнению срочных действий.
- Рассылки в социальных сетях от знакомых или друзей.
- Предложения установить приложение или перейти по ссылке.
  Злоумышленники взламывают страницы в социальных сетях и рассылают от имени владельца аккаунта фишинговые сообщения с просьбой от имени владельца странички занять или перевести некоторую сумму либо с целью выманивания реквизитов банковских платежных карточек, а также паролей для проведения в дальнейшем мошеннических операций.
  Просит перевести деньги на карточку или оплатить мобильную связь, билеты и т.д.

КАК ЗАЩИТИТЬСЯ:

- НЕ ПЕРЕВОДИТЕ деньги, позвоните родственнику/другу и уточните, не взломали ли его страницу и действительно ли ему нужна Ваша помощь.
- Не отвечайте на подозрительные письма.
- Не переходите по ссылкам.
- При обращении родственников/друзей/знакомых через социальные сети с просьбами о помощи в переводе денежных средств на карточку/оплаты мобильной связи, билетов и т.д. убедитесь, что лицо, обратившееся через страницу социальной сети, является именно тем, за кого себя выдает. Если Вы заметили, что к Вам обратился человек, который лишь выдает себя за владельца страницы – пожалуйтесь на мошенничество в соцсети и оповестите владельца страницы о возможном взломе.
- Наряду с номером и сроком действия карточки, логином и паролем от интернет-банкинга, паролем 3-D Secure и SMS-паролем (ключом), не сообщайте CVV2/CVC2-код (трехзначное число на обороте карточки), данный код используется исключительно для расходных операций и абсолютно не нужен для перевода денежных средств на Вашу карточку.
- В случае, если Ваш аккаунт в социальных сетях был взломан, по возможности оповестите об этом подписчиков Вашей страницы и смените пароль.

3. «ОШИБОЧНЫЙ ПЕРЕВОД ДЕНЕГ»

Сообщение с незнакомого номера о том, что на Ваш счёт переведены деньги, и повторное сообщение с просьбой их вернуть, так как перевод совершён по ошибке.

КАК ЗАЩИТИТЬСЯ:

НЕ ВОЗВРАЩАЙТЕ, проверьте состояние счёта, если счёт действительно пополнен третьим лицом, обратитесь в банк для урегулирования вопроса; если пополнения счёта не было, проинформируйте банк о сообщении и номере, с которого оно направлено.

4. «ВЫИГРЫШ ПРИЗА»

Злоумышленники рассылают сообщения о выигрыше ценных призов, провоцируют перевести на их счет некую сумму денег для получения "приза" или участия в розыгрыше и объясняют это тем, что нужно оплатить комиссию, таможенную пошлину, налоги либо транспортные расходы для доставки "выигрыша".

КАК ЗАЩИТИТЬСЯ:

ПОДУМАЙТЕ, принимали ли Вы участие в розыгрыше призов? Знакома ли Вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны Ваши контактные данные? Если не можете ответить хотя бы на один из вопросов, ПРОИГНОРИРУЙТЕ поступившее сообщение.