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

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

ИЛИ ВИДЫ ИНФОРМАЦИОННОГО МОШЕННИЧЕСТВА С ВАШИМИ КАРТОЧКАМИ

1. ВИШИНГ

Вишинг - метод мошенничества, направленный на получение у клиентов персональных или конфиденциальных данных, или стимулирование держателя на совершение определённых действий со своим карточным счетом (как правило, перевод денег мошенникам), используя телефонную коммуникацию и играя определённую роль.

КАК ЭТО РАБОТАЕТ?

- Мошенники могут представляться работниками банка, службы сервиса клиентов или представителями любых других организаций.
- Использовать скрытые телефонные номера или программы-анонимайзеры, подменяющие номера телефонов на реальные номера, размещенные на официальных ресурсах организаций.

КАК ЗАЩИТИТЬСЯ:

- Остерегайтесь неожиданных звонков с незнакомых номеров.
- Узнайте номер звонящего и сообщите, что сами перезвоните ему.
- Положите трубку и перезвоните в банк по официальному номеру, указанному на банковской карточке или сайте кредитной организации.
- Мошенники могут найти информацию о Вас в сети Интернет, в социальных сетях. Не верьте звонящему только на основании этих данных.
- Не разглашайте коды, логины и пароли к онлайн-банкингу. Банк никогда не спросит Вас о таких данных.
- Не переводите деньги на другой счет на основании требований. Банк никогда не попросит Вас об этом.
- Подозреваете мошенничество – свяжитесь с Вашим банком.

2. ФИШИНГ

Фишинг – действия, направленные на получение персональных, финансовых или конфиденциальных данных клиентов.

КАК ЭТО РАБОТАЕТ?

- Могут быть похожи на письма, которые приходят из банка или из других официальных организаций.
- Призыв к выполнению срочных действий.
- Рассылки в социальных сетях от знакомых или даже друзей.
- Предложения установить приложение или перейти по ссылке.

КАК ЗАЩИТИТЬСЯ:

- Не отвечайте на подозрительные письма.
- Не переходите по ссылкам и не загружайте приложения, введите адрес в своем браузере вручную.
- Сомневаясь, проверьте адрес официального сайта Вашего банка и позвоните в банк.
- Будьте особенно бдительны, если в письме от имени банка запрашивают конфиденциальные данные (например, логины или пароли).
- Никому и ни при каких условиях не сообщайте данные банковской карточки, код из СМС – сотрудники банка такие данные не запрашивают.
- Ни в коем случае не устанавливайте на смартфон приложения по просьбе «сотрудников банков».
- Обновляйте программное обеспечение, используйте антивирусную систему.

3. 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 (другой код).
- 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 пределов 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.