**Профилактика кибермошенничества**

В условиях пандемии и самоизоляции снизилась уличная преступность, которая раньше традиционно больше всего раздражала граждан. Но взамен вырос новый криминальный «монстр» - киберпреступность.

**1. Метод обмана и введения клиентов в заблуждение с целью кражи денежных средств.**

**Способ обмана:** обычно мошенники звонят потенциальным жертвам под видом банковских сотрудников, представителей иных финансовых организаций или правоохранительных органов. Они сообщают о том, по карте якобы совершена подозрительная операция. Для «предотвращения операции и сохранения средств» мошенники выманивают данные карты, убеждают жертву перевести деньги на «безопасный счет» или установить специальное приложение для «усиленной защиты телефона», которым на самом деле оказывается программа удаленного доступа к телефону. Для убедительности мошенники могут звонить с подменных номеров структур и использовать персональные данные клиентов, которые можно найти в теневом сегменте интернета.

**Как защититься:** положить трубку и перезвонить в банк по официальному номеру, указанному на банковской карте или сайте кредитной организации; никому и ни при каких условиях не сообщать данные банковской карты, код из СМС, сотрудники банка такие данные не запрашивают; нельзя устанавливать на смартфон приложения по просьбе «сотрудников банков»; написать заявление в отделении оператора сотовой связи о том, что вы запрещаете перевыпускать вашу сим-карту по доверенности без вашего личного присутствия.

**2. Оформление кредита в мобильном приложении**

Речь идет исключительно о займе, который банк уже предварительно одобрил клиенту. В этом случае мошенники нацелены на кражу не собственных средств клиента, а кредитных. Так как банк уже готов выдать заемные средства клиенту, то оформление занимает несколько минут, а мошенник может украсть гораздо больше средств, чем есть у клиента на счете.

**Способ обмана:** злоумышленники запугивают жертву недобросовестным работником банка, который сейчас пытается оформить на клиента кредит. Далее обманным путем оформляют предодобренный кредит (убеждают жертву это сделать или получают доступ в мобильный банк и сами проводят операцию).

**Как защититься:** перезвонить в банк по официальному номеру, указанному на банковской карте или сайте кредитной организации; никому и ни при каких условиях не сообщать данные банковской карты, код из СМС, сотрудники банка такие данные не запрашивают; нельзя устанавливать на смартфон приложения по просьбе «сотрудников банков».

**3. Поддельные сайты**

**Способы мошенничества:** мошенники могут создавать поддельные сайты, предлагающие товары и услуги, например, авиа и ж/д билеты, по более низким ценам. После выбора билета и формы оплаты пользователя просят ввести реквизиты своей банковской карты (номер карты, CVV-код). После согласия осуществить оплату происходит передача реквизитов кредитной карты злоумышленникам, о чем пользователь даже и не догадывается.

**Как защититься:** совершать покупки только на официальных сайтах; не верить « огромным «скидкам», «акциям» и «розыгрышам»; проверять доменное имя ресурса. Если оно отличается от оригинального или просто кажется подозрительным – закрывать страницу; при оплате товара необходимо обращать внимание на страницу платежной системы, на которую должен перенаправлять сайт продавца для ввода платежных данных. «сли продавец просит перевести деньги на карту или виртуальный кошелек, то это мошенник, так как компании не оформляют счета на физические лица; при входе в интернет-банк обращать внимание на наличие в адресной строке https:// и значка закрытого замка (это означает безопасное соединение).

**4.** Одним из самых популярных разновидностей мошенничества является скимминг. Суть его состоит в следующем: используя скрытые устройства, преступники считывают данные вашей карты, а затем создают её дубликат, с помощью которого расплачиваются в магазинах и на интернет-площадках.

Доказать банку, что операцию по оплате произвели не вы, очень сложно, поэтому, лучший способ бороться с таким видом кибермошенничества – предупредить его. Для этого:

Не пользуйтесь банкоматами, расположенными на улице. Видеонаблюдение за такими банкоматами может иметь слепые зоны, чем может воспользоваться злоумышленник и установить в нём устройство для скимминга.

Избегайте банкоматов, расположенных в плохо освещённых местах. При таком освещении, мошенникам не составит труда незаметно установить устройство для скимминга.

Используйте банкоматы, оборудованные джиттерами. Джиттер – антискимминговая накладка, заставляющая карту вибрировать при её считывании, что не позволит мошенникам скопировать нужную им информацию. Узнать такое устройство можно по изображению замка на накладке, в которую вы помещаете свою карту.

При наборе PIN-кода прикрывайте клавиатуру банкомата, если он не оборудован специальными лепестками.

**Рекомендации по использованию основных правил самозащиты**

**от киберпреступников**

К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код

Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

Будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_