МВД России
ГУ МВД России по Красноярскому краю

ОТДЕЛ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ЗАКРЫТОМУ АДМИНИСТРАТИВНО-
ТЕРРИТОРИАЛЬНОМУ ОБРАЗОВАНИЮ
ГОРОД ЗЕЛЕНОГОРСК
КРАСНОЯРСКОГО КРАЯ
(Отдел МВД России по ЗАТО г. Зеленогорск)
663690 г. Зеленогорск, ул. Гагарина, д. 54
тел.3-13-99, 3-14-04, 3-45-02,
факс 4-78-51, 4-79-37
dirzelenogorsk@mvd.ru

19 МАР 2021 № 7347
на № _____ от _____

Руководителю Управления образования
Администрации ЗАТО г. Зеленогорска
Парфенчиковой Л.В.

Уважаемая Людмила Владимировна!

Довожу до Вашего сведения, что, несмотря на неоднократные меры профилактического характера со стороны сотрудников полиции, в дежурную часть Отдела МВД России по ЗАТО г. Зеленогорск продолжают поступать заявления от жителей города, в том числе и от учителей школ г. Зеленогорска, о совершении в отношении них неустановленными лицами преступлений - мошенничеств и краж денежных средств с банковских счетов.

В ходе анализа уголовных дел установлено, что в результате неосведомленности граждан в сфере информационно-коммуникационных технологий, постоянно меняющихся методов и способов обмана, преступники завладели денежными средствами жителей г. Зеленогорск в сумме более 39000 рублей.

Появляются новые методы введения граждан в заблуждение с целью завладения данными банковских карт, мошенники находят новые способы незаконного списания средств, преступник старается любыми способами выманить информацию о карте у самого держателя, для достижения своей цели они используют все доступные ресурсы – телефон, интернет-сайты, онлайн-банк, мобильные банки и прочие каналы.

В связи с тем, что многие заявители работают в Вашем трудовом коллективе, с целью профилактики преступлений, связанных с мошенничеством, прошу Вас оказать содействие в информировании коллектива предприятия о наиболее распространенных случаях мошенничеств:

<u>Звонок от сотрудника банка</u>

Цель мошенников – завладеть деньгами граждан. Для этого достаточно получить от клиента банка полные данные карты (номер, дата окончания срока действия и CVV/CVC-код), создать с неё перевод и подтвердить его кодом из SMS, которое придет на телефон, привязанный к карте. Самый

популярный способ сделать это – позвонить и представиться сотрудником банка, либо перевести разговор с якобы «роботом» банка.

Повод может быть любой: агрессивный: «ваша карта заблокирована»; нейтральный: «нам нужно уточнить ваши данные, подтвердите перевод с карты» и т.д.; соблазняющим: «вам пришел перевод на несколько тысяч, чтобы получить его, сообщите данные карты».

В подобном случае необходимо:

1. **Положить трубку.** Все решения, кроме блокировки карты, можно принять позднее. Поэтому пообещайте подумать, выдохните и положите трубку.
2. **Затем перезвонить в банк самим –** номер горячей линии указывается на самой карте. Также он есть на официальном сайте банка и в мобильном приложении.
3. **Заблокировать карту**. На случай если у мошенников могут быть данные вашей карты, заблокируйте её по звонку в банк или в мобильном приложении. То же самое стоит сделать, если вы получили SMS от банка о странном списании средств или видите подозрительную покупку в истории транзакций мобильного приложения.

Сотрудник банка никогда не попросит номер карты и уж тем более CVV/CVC-код или PIN-код. Специалист может только уточнить лишь последние четыре цифры карты, чтобы понять, с какой именно из ваших карт предстоит работать. Сотрудники крайне редко задают дополнительные вопросы – только если вы забыли ответ на секретный вопрос и хотите сменить пароль. Сотрудники банков нечасто звонят клиентам – это скорее исключение. Вы всегда можете обратиться в отделение банка. Там уж точно сотрудники настоящие.

Для убедительности преступники могут «подключать» к разговору «сотрудников правоохранительных органов, которые занимаются раскрытием мошенничеств в сфере банковских краж», либо «органов, контролирующих банковские операции».

В настоящее время, используя базы телефонных номеров, звонящие мошенники сразу обращаются к абоненту по имени отчеству, что потерпевшему дает основание полагать, что он общается с представителем финансовой организации.

Звонок с официального номера телефона банка, который указан на карте или на официальном сайте.

Новая схема мошенничества — через виртуальные АТС звонят клиентам банков с номеров кредитных организаций и выведывают логины и пароли карт. Такая мошенническая схема набирает обороты. Даже несмотря на то, что в целом финансовая грамотность населения растет, звонок из «банка» заставляет людей забыть элементарные правила безопасности. Злоумышленники используют специальное программное обеспечение, чтобы имитировать номера банков. Так им удается ослабить бдительность жертвы уже на этапе звонка, потому что клиенты банка видят знакомый номер. Мошенники представляются сотрудниками банка и знают о клиенте почти все: фамилию, имя и отчество, паспортные данные и в некоторых случаях даже номер карты. Далее преступники начинают запугивать и торопить человека. Обычно они утверждают,

что зафиксировали подозрительную активность по карте, и чтобы ее остановить, нужно срочно назвать либо пин-код, либо одноразовый пароль из СМС.

В подобном случае необходимо:

1. **положить трубку.** Все решения, кроме блокировки карты, можно принять позднее. Поэтому пообещайте подумать, выдохните и положите трубку.
2. **затем перезвонить в банк самим** – номер горячей линии указывается на самой карте. Также он есть на официальном сайте банка и в мобильном приложении.

Оформление кредитов

Охотники до чужих денег начали применять «новую схему»: совершают звонки на телефоны жителей нашего города, и с целью завладения денежными средствами просят граждан скачать в «Плей маркете» якобы Антивирусную программу или программу «помощник», на самом деле гражданин скачивает программу «TeamViewer» или иную программу, которая позволяет управлять одним устройством с помощью другого устройства, то есть на расстоянии, дистанционно. Существует множество аналогов, но программа – приложение TeamViewer самый популярный.

Эта программа может не только обеспечить удаленный доступ, но и передачу файлов с одного компьютера на другой, не загружая его в интернет. TeamViewer можно установить и на Windows и на MacOS и на Linux и на Android с iOS, что позволит управлять любым компьютером на популярной операционной системе с помощью телефона.

После установки гражданином этой программы мошенник под разными предлогами просит открыть Личные кабинеты банков, в которых имеются карты, а потом просто оформляют кредит и переводят сумму к себе на счет через свой компьютер или другое устройство. Цель – завладеть деньгами, способы могут быть разными. Таким образом, мошенник оформляет кредит на вашу карту, а потом просто переводит деньги себе на счет, а Вы за всеми его действиями наблюдаете у себя на смартфоне. После того, как Вы обратитесь в банк, вам распечатают кредитный договор, который оформили мошенники по Вашей карте на Ваше имя.

В подобном случае необходимо:

1. **Положите трубку.** Если вам позвонили от лица сотрудника банка, то просто положите трубку.
2. **Не скачивайте никаких приложений в Плей Маркете.** Если вы все же поддались на уловки мошенников и стали разговаривать, то просто не скачивайте никаких программ и не открывайте Личные онлайн кабинеты банков, где у вас имеются карты.

Смс типа «я перевел вам 25 000 руб. и ссылка на avito-zo.info/49PJ21Sc.

В СМС или письмах на почту злоумышленники хотят заставить получателя перейти по ссылке. Чаще всего это СМС о поступлении денег. Перейдя по ссылке, вы устанавливаете вредоносное ПО, в дальнейшем у вас с банковского счета карты списываются деньги.

В подобном случае необходимо:

1. **Никуда не нажимайте и не переходите по ссылкам**. Не стоит никуда переходить и ничего скачивать. Avito - присутствует специально, чтобы пользователь с большей долей вероятности кликнул.

2. **Удалите смс.**

Схемы обмана при использовании АВИТО

Авито – крупнейшая российская Интернет площадка, на которой можно легко купить или продать любой товар. Авито используют как добропорядочные граждане, так и мошенники. Определить мошенника на сайте «Авито» сложно. Поэтому в процессе проведения сделки нужно быть предельно внимательными. Провести безопасную сделку можно.

В подобном случае необходимо:

1. **пройти мимо**. Внимательно изучить объявление. Если там что-то насторожило – пройти мимо;
2. **сразу отклонять очень уж выгодные сделки**. В 99% случае это ловушка для жадных;
3. **ни в коем случае не делать предоплату** – для этого есть эскроу-счет;
4. **не давать персональных данных**: номер, серию и дату выдачи паспорта, код и срок действия карты;
5. **не переходить по подозрительным ссылкам**. В них могут быть вирусы, скачивающие персональные данные или снимающие деньги через онлайн-банкинг. На официальных сайтах «Авито» в начале адреса стоит закрытый замок. Если его нет или открыт, нужно немедленно уходить;
6. **проверить профиль продавца**. Если там первая сделка, необходимо предпринять максимальные меры предосторожности.
7. **не разглашать никакой информации**. Важно знать и помнить - перевод можно было сделать по номеру карты или по номеру телефона. Откликаясь на объявление, мошенники на «Авито» просят номер карты, срок ее действия и код CVV с обратной стороны, чтобы произвести предварительную оплату. Данные нужны, чтобы убедиться в том, что продавец не мошенник. Многие хозяева карточек не видят подвоха – ведь собираются им переводить деньги. В результате, выдав нужную информацию, владелец лицевого счета лишается всех средств, которые там находились в течение нескольких минут.

В целях информирования граждан и предупреждения преступлений в сфере информационно - коммуникационных технологий прошу довести до учителей школ г. Зеленогорска вышеизложенную информацию.

С уважением

начальник отделения СО
ОМВД России по ЗАТО г. Зеленогорск
майор юстиции Ю.Г. Веретенникова