М В Д Р о с с и и

Управление
Министерства внутренних дел
Российской Федерации
по Ханты-Мансийскому
автономному округу - Югре
(УМВД России по Ханты-
Мансийскому автономному
округу - Югре)

ул. Ленина, 55, Ханты-Мансийск, 628011
e-mail: udir_86@mvd.ru

Директору Департамента
региональной безопасности
ХМАО-Югры

А.Ф. Золотухину

ул. Студенческая, д.2
г. Ханты-Мансийск

14.07.2023 № 1/12257

на № 44-Исх-5195 от 06.07.2023

О направлении сведений

Уважаемый Алексей Феликсович!

В целях информирования лиц старшего поколения как не стать жертвой мошенников, предлагаем проводить групповые уроки, лекции, тематические занятия. Проработать вопрос с операторами сотовой связи используемой на территории Ханты-Мансийского автономного округа Югры об информировании всех граждан автономного округа путем рассылки СМС сообщений с текстом: «не стать жертвой мошенников, не переводи денежные средства незнакомым лицам, не участвуй в розыгрыше призов, не верь незнакомым людям о том, что твои родственники попали в беду», а также с представителями Федеральной службы по гидрометеорологии и мониторингу окружающей среды и МЧС России по ХМАО-Югре от которых поступают СМС оповещения о складывающейся оперативной обстановке по курируемым направлениям деятельности.

Также сообщаем, что регистрируемые дистанционные имущественные преступления можно условно разделить на несколько видов:

1. С использованием телефонии:

- Звонки от сотрудников «службы безопасности Банков» и сотрудников силовых структур (МВД, ФСБ, прокуратуры) с использованием Sip-телефонии и программ подменны абонентского номера, когда на телефоне потерпевшего определяется официальный номер Банка, либо территориального органа МВД России, ФСБ и прокуратуры;

- под предлогом пресечения сомнительных операций по счетам, оформления кредитов неизвестным лицом, либо под предлогом оказания помощи в установлении и поиске преступников среди сотрудников банков, требуют оформить «зеркальный» кредит, а затем внести денежных средств на

«безопасные ячейки», либо на абонентские номера, подконтрольные неизвестным лицам; требования сообщить номер банковской карты, CVC-код, а затем код в СМС сообщении, необходимый для удаленного управления и хищения денежных средств со счетов граждан.

2. В сети Интернет:

- под предлогом продажи либо покупки товаров на сайтах бесплатных объявлений «Авито», «Юла», а также в социальных сетях «В контакте», «Одноклассники», «Инстаграмм» мошенники убеждают пройти по «безопасной ссылке», после чего денежные средства перечисляются на подконтрольные счета злоумышленников.

- Оплата поездки с использованием сервиса «БлаБлаКар» по предоставляемой злоумышленником ссылке на предоплату в чате сервиса или в мессенджере. Необходимо помнить, что поездки с водителем- попутчиком оплачиваются только наличными и только во время поездки. Переводить деньги заранее или просить предоплату запрещено. Билеты на автобусы можно купить он-лайн, оплатив банковской картой. Обратите внимание на то, что билеты на проезд нужно приобретать через официальные приложения. Ни в коем случае нельзя переводить деньги по предоставляемым водителем ссылкам;

- перечисление денежных средств неизвестным лицам под предлогом участия в инвестиционных проектах на незарегистрированные Центральным Банком России «инвестиционных площадках». Объявления с предложениями принять участия в инвестировании размещаются злоумышленниками в социальных сетях, таких как «В контакте», «Одноклассники», «Инстаграмм», «Тик-Ток», на видеохостингах «Ютуб» и т.д. Необходимо знать, что инвестиционными проектами в Российской Федерации уполномочены заниматься исключительно банки (Сбербанк, Газпром банк, Тинькоф, Альфа-Банк и т.д.). Перечень лицензированных банков размещен на официальном сайте Центрального Банка РФ, там же и размещены правила, порядок и условия участия в инвестиционных проектах.

- Продажа товара на поддельных интернет-сайтах (клонах), или сайтах однодневках;

- Взлом персональных страниц в социальных сетях и использование их для рассылки «друзьям» сообщений с просьбой занять денег или оказать безвозмездную финансовую помощь;

Необходимо отметить, что в текущем году участились такие виды преступления как: родственник попал в ДТП, для решения вопроса необходимо заплатить денежные средства, за которыми приходит курьер (потерпевшие по данному виду граждане престарелого возраста); звонки от сотрудников «службы безопасности Банков» и сотрудников силовых структур (МВД, ФСБ, прокуратуры); дополнительный заработок от вкладов в различные инвестиционные фонды, финансовые биржи, которые создали преступники для реализации своих корыстных умыслов по выманиванию

денежных средств у граждан; продажи либо покупки товаров на сайтах бесплатных объявлений «Авито», «Юла» мошенники убеждают пройти по «безопасной ссылке», после чего денежные средства перечисляются на подконтрольные счета злоумышленников.

Чтобы не стать жертвой мошенников, многое зависит о финансовой грамотности и осведомленности потенциальной жертвы, о способах совершения преступления. Важно знать, что сотрудники служб безопасности банков:

Не интересуются кодами, поступающими в СМС-сообщениях при совершении финансовых операций в «Личном кабинете» клиента;

Не просят «клиентов» перевести денежные средства на резервные счета;

Не убеждают «клиентов» в необходимости оформления зеркальных кредитов с целью предотвращения «оформления кредита» на имя клиента неустановленными лицами;

Не интересуются наличием банковских карт сторонних банков и суммой денежных средств, находящихся на счетах клиента;

Не требуют перечисления денежных средств за «оформление, страхование, услуги курьера» при оформлении он-лайн кредитов;

Сотрудники правоохранительных органов при общении по телефону:

Не сообщают о каких-либо мероприятиях, проводимых МВД, ФСБ и другими силовыми структурами, направленных на изобличение мошенников среди банковских служащих, и вообще каких-либо в принципе;

Не требуют от «клиентов Банка» выполнять какие-либо инструкции якобы сотрудников служб безопасности банков;

Не предупреждают об уголовной ответственности за невыполнение требований, поступающих в телефонном режиме от якобы сотрудников Банков.

При поступлении на телефон входящего звонка с абонентских номеров силовых структур (МВД, ФСБ, ФССП и т.п.), которые размещены на официальных сайтах, необходимо прекратить звонок и перезвонить на указанные номера самостоятельно. Важно дозвониться самому, а не ждать когда Вам перезвонят.

При поиске объявлений на сайтах «Юла», «Авито», «Дром», «Авто.ру» и др. обязательно ознакомиться с правилами и условиями сайта, с правилами оплаты и предоплаты за покупку товара или за использование услуг доставки товара курьерской службой. Существуют правила безопасных сделок, а именно:

- необходимо «общаться» во внутреннем чате сайта и не уходить в другие мессенджеры;
- хранить в тайне свою переписку, паспортные данные и код с карты;
- не отправлять предоплату, если не уверены в порядочности продавца;
- никому не сообщать коды из смс и пуш-уведомлений;

- игнорировать ссылки на оплату, которые присылает собеседник.

При оформлении покупок на Интернет-сайтах, осуществлять мониторинг сети «Интернет» на предмет наличия отрицательных отзывов, а так же даты регистрации сайта (если сайт или страничка в соцсетях создана недавно и отсутствуют отзывы, или имеющиеся отзывы носят отрицательный характер, то вероятнее всего это мошенник). Кроме того необходимо обращать внимание на то, что у любого продавца имеется юридический адрес или адрес фактического нахождения магазина или склада. Информацию с указанием адресов магазинов можно проверить в сети интернет, например, на сервисах Яндекс или на сайте 2ГИС.

Осуществлять покупку билетов на различный вид транспорта необходимо исключительно с помощью официальных приложений, размещенных в «Appel Store» и «Play Market», а так же на официальных сайтах авиа и ж/д компаний. Важно помнить о нахождении в Интернете сайтов-двойников, которые могут иметь наименования, созвучные с официальными сайтами (нужно внимательно изучить весть сайт, перезвонить на телефон технической поддержки, уточнить у оператора всю информацию о предоставляемых услугах).

Врио начальника полиции Р.С. Кондрашов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат BFA6D7ABAA1D3FCD1B674E60DE718345
Владелец **КОНДРАШОВ РУСЛАН СЕРГЕЕВИЧ**
Действителен с 14.03.2023 по 06.06.2024

Исп. Савинов А.М.
8(3467) 398835