Современные виды краж и мошенничеств, совершаемых дистанционным способом.

1. **Основной мошеннической схемой на сегодняшний день остается предлог:** держателю банковской карты приходит SMS-сообщение, либо осуществляется звонок, (**в основной массе номер телефона злоумышленника начинается с цифр 8-495…**) и **МОШЕННИК, ПОД ПРЕДЛОГОМ ЗАЩИТЫ БАНКОВСКОЙ КАРТЫ ОТ НЕСАНКЦИОНИРОВАННОГО СПИСАНИЯ ДЕНЕЖНЫХ СРЕДСТВ,** начинает выманивать у потерпевшего реквизиты его банковской карты PIN-код и CVC2/CVV2 (код безопасности – цифры с обратной стороны карты), а также срок её действия и другие персональные данные, т.е. аналогично предлогу разблокировки банковской карты, а также под предлогом отмены попытки оформления на потерпевшего кредита.

Следует знать и помнить, что ни один работник банка никогда не будет интересоваться реквизитами Вашей банковской карты, при отмене операции, как минимум при звонке, осуществленном из банка, работник **В ПЕРВУЮ ОЧЕРЕДЬ ПОИНТЕРЕСУЕТСЯ, ВЫ ЛИ ОСУЩЕСТВЛЯЛИ ОПЕРАЦИЮ!!!!** А если даже у Вас действительно появилось сомнение, то необходимо связаться с банком, осуществить звонок на горячую линию, номера телефонов всегда оставляет любой работник банка, поинтересоваться проходили ли какие-то операции или попытки перевода денежных средств с Вашего счета, **ну или как минимум попросить человека который с Вами связался и представился работником банка, любые Ваши данные, хотя бы фамилию…. Наибольший ущерб для граждан Смоленской области от данного вида.**

2. **Вторая схема,** это когда держателю банковской карты приходит SMS-сообщение о блокировании его банковской карты, и также указан номер телефона «службы технической поддержки», как правило, начинающийся на 8-800-… Когда он перезванивает по указному номеру, ему отвечает якобы сотрудник техподдержки банка и просит его подойти к банкомату и диктует ему ряд действий, чтобы снять блокировку карты. Далее, владелец «заблокированной» карты вводит и сообщает известные только ему данные, после чего с карты списываются имеющиеся денежные средства. Несмотря на то, что граждан при получении банковской карты предупреждают, чтобы они не сообщали никакой информации о своей карте: PIN-код и CVC2/CVV2 (код безопасности – цифры с обратной стороны карты), а также срок её действия и свои персональные данные посторонним лицам. При вхождении в приложение Сбербанк-Онлайн в SMS-уведомлении также дублируется информация о том, чтобы никому из посторонних не сообщали присланный код. **Сотрудники банков никогда не запрашивает эту информацию, такие случаи носят мошеннический характер. В случаях сомнительных действий необходимо позвонить по телефонам указанным на банковской карте и заблокировать карту для прояснения ситуации.**

3. Старая «классическая» схема мошенничества, на которую продолжают попадать лица пожилого возраста: мошенники звонят преимущественно в ночное и вечернее время и сообщают, что «мам (бабуль) я попал в ДТП или в полицию» и просят денег для «решения вопроса». Далее в разговор вступает другой мошенник, который представляется сотрудником полиции и уверенно сообщает, что уже не раз помогал людям

таким образом. Деньги, необходимо привезти в определенное место и передать конкретному человеку либо за ними приедет их знакомый человек, либо перевести на указанный счет.

4. Еще одним распространенным видом мошенничества являются мошеннические действия при купли-продажи товара по объявлению, размещенному на одном из многочисленных интернет-сайтов. При этом злоумышленник, может, как продавать, так и покупать товар.

При продаже товара злоумышленник, как правило, просит предоплату, сопровождая свою просьбу различными предлогами: срочно нужны деньги, уже нашелся другой покупатель и т.п. После перевода денежных средств в качестве предоплаты, как правило, связь с продавцом прекращается.

При покупке, злоумышленник приобретает товар, не торгуясь, либо вносит предоплату за съем жилья (квартиры, дома), имитируя спешку, невнимательность. Он якобы (один из вариантов мошенничества) переводит сумму больше, чем просит продавец, но на самом деле проходит регистрацию в приложении Сбербанк-Онлайн, при этом убеждает продавцов сообщать ему все присланные логины и пароли, а затем осуществляет переводы денежных средств с различных счетов продавца на счет его же банковской карты и просит часть денег перевести обратно.

5. **Распространены и такие виды мошенничеств, как взлом аккаунта в социальных сетях и рассылка друзьям пользователя сообщений от его имени с просьбой о перечислении денег, при этом телефонного контакта не происходит. А реальный владелец социальной страницы даже не подозревает, что от его имени просят денег.**

Или же после размещения о продаже чего-либо в сети интернет, начинают приходить SMS-сообщения об обмене и указывается ссылка, перейдя по которой можно посмотреть товар и условия обмена. Но на самом деле перейдя по ссылке, устанавливается программное обеспечение, которое выводит денежные средства с банковской карты (если подключена услуга «Мобильный банк»), блокируется поступление sms-сообщений с номера 900 (наиболее подвержены мобильные термины с операционной системой Андроид).

6. Одним из новых способов мошенничеств, является завладение реквизитами банковских карт под предлогом предоставлении услуги доставки грузов или поездки по объявлениям сервиса поиска попутчиков «BlaBlaCar».

Мошенники регистрируются в сообществе попутчиков, предлагают подвезти жертву и либо требуют предоплату через фишинговый сайт, либо пытаются различными способами узнать реквизиты банковских карт.

Мошенники размещают на BlaBlaCar объявления о свободных местах в машине, ничем не отличающиеся от настоящих, и даже цены указывают в пределах нормы. Маршруты они выбирают как популярные, так и не очень.

Когда пользователь откликается на объявление, мошенники в чате на сайте BlaBlaCar просят его связаться с ними в WhatsApp и отправляют номер телефона. Поскольку политика сервиса запрещает пересылать в сообщениях контактные данные, «водитель» пишет номер словами.

Обсуждение деталей поездки тоже на первый взгляд не вызывает подозрений. Мошенники охотно поддерживают разговор об интересующих

пассажира подробностях и даже сами задают уместные в контексте поездки уточняющие вопросы.

Когда речь заходит об оплате поездки, жертве предлагают «купить билет» по ссылке якобы на BlaBlaCar (название сервиса присутствует в адресе сайта). Почему надо воспользоваться именно таким, непривычным для постоянных пользователей платформы, форматом оплаты, объясняют по-разному. Например, один жулик утверждает, что он «официальный водитель» и наличные не поддерживает. В другом случае убедить жертву пытаются бонусами и кэшбеком, которые водитель якобы получит при оплате через сайт.

На самом деле никаких билетов BlaBlaCar не продает.

Используйте надежную защиту, которая заблокирует фишинговый или мошеннический сайт, если вы попытаетесь на него перейти.

7. Также актуальной схемой мошенников является предлог покупки акций крупных государственных (коммерческих) предприятий в основном энерго – ресурсных.

8. Кроме того поступают звонки от мошенников под предлогом дополнительного заработка на биржевых площадках по торговли акциями, облигациями и иными производными инструментами.

Все виды мошенничеств и краж денежных средств с банковских карт, совершаемых дистанционным способом, невозможно описать, т.к. они постоянно видоизменяются, но способы защиты от них остаются неизменными:

– Не сообщайте никому PIN-код и CVC2/CVV2 (код безопасности – цифры с обратной стороны карты), а также срок её действия и свои персональные данные. Ни один банк не будет по телефону спрашивать у вас эти реквизиты. Для зачисления средств на ваш счёт достаточно лишь 16-значного номера, указанного на лицевой стороне карты.

– Не сообщайте неизвестным лицам PIN-код для входа в ваш онлайн-банк - для перевода денежных средств это не требуется.

– Не используйте карты с основным своим финансовым капиталом для оплаты в сети Интернет.

– Не рекомендуется входить в интернет-банк с чужих компьютеров или из публичных незащищенных сетей Wi-Fi.

– На личном компьютере, смартфоне, планшете установите антивирусное программное обеспечение и своевременно его обновляйте.

– Не скачивайте файлы из непроверенных источников (файлообменные сервисы, социальные сети). Не переходите по ссылкам на информационные ресурсы, полученных от сомнительных источников. Не открывайте файлы из подозрительной электронной почты.

– **При звонке о попавших родственниках в полицию: н**е паникуйте, задайте вопросы личного характера (хотя бы как зовут ваших родственников и их близких), прервите разговор и попытайтесь связаться с тем родственником, который якобы попал в беду;

– При просьбе об одолжении денег в долг, поступившей в социальных сетях, убедитесь, что просьба пришла именно от того лица, которое просит – просто перезвоните ему.

УМВД России по Смоленской области