Преступления, совершенные с использованием информационно-телекоммуникационных технологий

По информации УМВД России по г. Сургуту за 9 месяцев текущего года зарегистрировано 843 преступления, совершенных с использованием информационно-телекоммуникационных технологий. Из них мошенничества – 591 преступление, кражи – 252 преступления. Сумма материального ущерба, причиненного жителям города, составила более 109 млн. рублей.

Наиболее распространенными схемами совершения мошеннических действий стали:

1. Осуществление звонков с федеральных номеров («8800…», «8495…», номеров принадлежащих федеральным органам власти РФ), а также с абонентских номеров от имени представителей крупных банков РФ, сотрудников правоохранительных органов и под предлогом пресечения сомнительных операций по счетам, оформления кредита неизвестным лицом, получение мошенником сведений о сроке действия и cvc-кода гражданина, осуществление входа в личный кабинет «банкинг онлайн», либо перемены абонентского номера привязанного к банковской карте.
2. Осуществление звонка от имени оператора сотовой связи, который поясняет, что у гражданина заканчивается срок действия сим-карты, для продления срока действия сим-карты, необходимо сообщить код подтверждения из поступивших на абонентский номер текстовых сообщений, в последующем злоумышленник включает переадресацию вызовов и осуществляет вход в «банкинг онлайн» с последующим списанием денежных средств.
3. Приобретение товара через сайты бесплатных объявлений («Авито», «Юла», «Дром» и т.д.), где злоумышленник поясняет, что товар есть в наличии, однако для его получения необходимо выслать либо стопроцентную предоплату, или половину стоимости товара, если указана большая сумма оплаты.
4. Бронирование поездок через приложение «blabla car». Злоумышленники под видом водителей создают профили и для оплаты поездки просят пройти по ссылке якобы от приложения «blabla car» (безопасная сделка).
5. Приобретение товара, либо заказ услуги через группы социальных сетей «Вконтакте», «Инстаграмм» группы в «Telegram, WhatsApp, Viber», где гражданину предлагается сначала внести стопроцентную предоплату, а после он получит свой товар, либо запись на необходимую услугу.
6. Поиск товара через поисковые системы сети Интернет, где гражданин попадает не на официальный сайт продажи товара, а на фишинговый сайт (дубликат) с измененным расчетным счетом и контактных данных продавца.

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ

- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ

Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Как защитить свои финансы, читайте на fincult.info

Финансовая культура