

## **Прокуратура Амурской области предупреждает:**

### **«Защити себя и свою семью от финансового мошенничества!»**

На фоне пандемии мошенничество с использованием информационно-телекоммуникационных технологий растет с геометрической прогрессией.

Так, в 2019 году таких преступлений совершено 2124 (+ 78,2%; 1192), за 7 месяцев 2020 года – 1891 (+ 97,4%). В числе указанных преступлений удельный вес краж и мошенничеств составляет 85%.

Мошенники, активно и настойчиво общаясь с гражданами по телефону и в социальных сетях, научились выманывать у граждан деньги, порой огромные суммы – сотни тысяч рублей. Имеет место случай причинения гражданину ущерба в сумме более девяти миллионов рублей!

Так, в 1-ом полугодии 2020 года на территории Амурской области зарегистрировано 1034 факта мошенничества (944, + 9 %), в том числе в сфере информационно-телекоммуникационных технологий – 529 (420, +26%).

За 7 месяцев 2020 года зарегистрирован 1231 факт мошенничества, из которых более половины – 685 (56%) совершены с использованием информационных технологий.

**Как правило, общение мошенников с гражданами происходит с применением психологических приемов, зачастую с напором, навязчиво.**

Звонки поступают независимо от времени суток (часового пояса) с расчетом, что в ночное или раннее утреннее время можно застать человека врасплох.

**Содержание таких разговоров состоит в сообщении ситуации, сугубо связанной с сохранностью денежных средств обладателя банковской карты, счета и т.п., и т.д.**

**Карта может быть даже кредитной! И с нее спишутся деньги, которыми Вы так и не воспользовались!**

**Вас безошибочно могут назвать по имени и отчеству, им известен номер Вашего телефона и, возможно, адрес, а также иные персональные данные. В разговоре они просят сообщить дополнительные личные данные.**

**Злоумышленники пишут в социальных сетях от имени Ваших родственников или друзей, которые якобы попали в беду, просят перевести деньги на неизвестный Вам счет, а могут предложить Вам оформление кредита, пособия, получение выигрыша, льгот, в том числе налоговых и т.д.**

**В указанных случаях, общаясь с абонентами, звонившими Вам с неизвестных номеров, Вы имеете дело с финансовыми мошенниками.**

## **МЕРЫ ПРЕДОСТОРОЖНОСТИ:**

**1. Никому не сообщайте свои персональные данные,** тем более коды и пароли, выслушайте звонившего без обсуждения своих данных и положите трубку телефона.

**2. Всегда проверяйте информацию,** перезвоните в офис банка по известному Вам номеру телефона, а лучше обратитесь лично.

3. Обратитесь в налоговую инспекцию, отделение Пенсионного фонда лично, выяснив о полагающихся льготах и выплатах.

**4. Не следуйте никаким инструкциям, не переходите по ссылкам, не перезванивайте по сомнительным номерам;**

**5. Установите антивирус на телефоне и компьютере.**

**6. Не храните данные карт на компьютере или в смартфоне.**

**7. Объясните родственникам и подросткам эти простые правила.**

**8. В случае, если произошло покушение на ваши денежные средства,** или их обманным путем списали, срочно позвоните в банк по телефону, указанному на оборотной стороне карты, примите меры к блокировке карты, обратитесь в отдел полиции (02,002, 020, 112)

## **ПРЕЖДЕ ЧЕМ ВЛОЖИТЬ СРЕДСТВА НАДО ЗНАТЬ:**

**Поверив, вложив деньги в какой-либо навязанный Вам финансовый проект (как правило, по телефону), Вы потеряете свои сбережения, заработанные честным трудом!**

Тогда как финансовые пирамиды маскируются под микрофинансовые организации, инвестиционные, управляющие предприятия, заявляют о высоких процентах по вкладам, отсутствии рисков, гарантируют доход (это запрещено на рынке ценных бумаг), обещают помочь людям даже с плохой кредитной историей...

В последнее время предлагают не только большой доход от вложенной суммы (до 500%), но и дорогие гаджеты за полцены...Но чтобы их получить необходимо лично внести сумму и привести своего знакомого, который также внесет недостающую сумму.

А для создания видимости успешной деятельности финансовой пирамиды ее организаторы даже снимали видеоролики с обладателями новых гаджетов и выкладывали их в сеть. По всем фактам незаконной деятельности материалы переданы в правоохранительные органы.

По данным Центробанка России на Дальнем Востоке активизировали работу черные кредиторы. Только за 1-ое полугодие 2020 года выявлено 50 организаций, нелегально работавших на финансовом рынке (1-ое полугодие 2019 года – 66).

Из них в Амурской области выявлено -5, В Хабаровском крае и Якутии – 10 и 9 соответственно, в Приморье – 16, на Сахалине -5.

В одном случае организацию исключили из реестра финансовых организаций, но она продолжала работать под видом микрокредитной компании.

**В 1-ом полугодии 2020 года из 100 фактов мошенничества с использованием информационно-коммуникационных технологий правоохранительными органами Амурской области раскрыто ЛИШЬ 18! Эта проблема возникает из-за того, что злоумышленники работают на удалении, зачастую из других субъектов РФ.**

**Только за 05.08.2020 в МО МВД России «Благовещенский» обратились более 10 человек, ставших жертвами мошенничества. Большая часть из них «попалась» на сайты-двойники.**

Потерпевшие размещали информацию о продаже чего-либо на сайте бесплатных объявлений. Через известный мессенджер с ними связывались злоумышленники и сообщали, что готовы приобрести товар, однако, они желают воспользоваться услугой сайта – «доставка», так как находятся в другом городе.

Потерпевшие получали ссылку с оплаченной суммой, пройдя по ней вводили данные своей банковской карты и нажимали кнопку «получить деньги». В результате денежные средства списывались с их счета.

В другом случае граждане заходили в личный кабинет банка, вводили данные карт. После этого с их счетов также списывались денежные средства.

Злоумышленники создали так называемые «сайты-двойники» официальных сайтов бесплатных объявлений и банка, в названии которых имеется незначительная разница в знаках или буквах и полностью копирующими внешний вид официальных страниц. Как только гражданин проходил по ссылке, вводил свои персональные данные, злоумышленники автоматически получали доступ к его банковскому счету.

Киберпреступники разработали новую схему кражи средств с банковских карт россиян - с помощью QR-кодов. На листовке с рекламой магазина электроники было написано, что покупатель может получить скидку, отсканировав QR-код. Однако воспользоваться этими бонусами не удалось. Телефон завис и в этот момент потерпевшей от действий мошенников пришло СМС о списании всех денег со счета.

В другом случае жертвой махинаций стал посетитель кафе, работники которого решили упростить процедуру оплаты и поместили на свое меню QR-код, по которому можно рассчитаться за заказ. Мошенники наклеили свой код поверх листовки и получали деньги с посетителей кафе.

**Зачастую рекламу скидок можно увидеть в магазинах, автобусах, что должно настораживать граждан, ведь легально скидка может быть предоставлена клиенту непосредственно при оплате услуг путем расчета, а не считывания какого-либо кода.**

По всем фактам мошенничества возбуждены уголовные дела, проводятся оперативно-розыскные мероприятия по установлению лиц, причастных к данному преступлению.

**Мошенничества граждане могли бы избежать, если бы проверили достоверность сайта и не попали бы на «двойника», не произвели предоплату товара, не следовали по ссылке, не считывали коды, в результате чего злоумышленники получили доступ к счету и списали денежные средства.**

***ЕСЛИ ВЫ ПОДВЕРГЛИСЬ ДЕЙСТВИЯМ МОШЕННИКОВ:***

**Сообщите в Банк России о факте мошенничества по телефону: 8-800-250-40-72 (звонок бесплатный).**

**Сообщите о попытке или факте мошенничества в органы полиции по номеру – 02., 002, 112.**

**ПОМНИТЕ, МОШЕННИЧЕСТВО ЛЕГЧЕ ПРЕДУПРЕДИТЬ, НЕ ПОПАДАЯ НА УЛОВКИ ЗЛОУМЫШЛЕННИКОВ, ЧЕМ ПЫТАТЬСЯ ВЕРНУТЬ СВОИ ДЕНЕЖНЫЕ СРЕДСТВА!**

**Прокуратура Амурской области**