Главам управ районов: Отрадное, Бибирево, Лианозово, Северный, Алтуфьевский г. Москвы

Главам муниципальных округов по районам: Отрадное, Бибирево, Лианозово, Северный, Алтуфьевский г. Москвы

Направляю Вам информацию для размещения на сайте управ
и муниципальных округов.

**О схемах телефонного мошенничества**

Телефонные мошенники стали использовать новую схему обмана: представляясь сотрудниками правоохранительных органов, они якобы **расследуют дело о массовой утечке персональных данных из банков**, которое ведется по поручению Центрального банка.

Мошенник звонит человеку и сообщает, что среди скомпрометированных данных могут быть и его сведения. Он предлагает свериться с базой утечек, чтобы привлечь собеседника в качестве потерпевшего.

Далее злоумышленник спрашивает у человека, в каком банке он обслуживается, просит данные карты, в том числе трехзначный код на её оборотной стороне. Чтобы убедить потенциальную жертву в правдоподобности истории, мошенник может направить ему в мессенджер или на электронную почту фото поддельного документа о проведении оперативно-розыскных мероприятий.

Если вы подозреваете, что вас хотят обмануть, прервите разговор. Ни работники банков, ни сотрудники правоохранительных органов никогда не запрашивают данные банковской карты (ее номер, трехзначный код с оборотной стороны, смс-код). Эти сведения нужны мошенникам.

Ни Банк России, ни представители правоохранительных органов не направляют фото удостоверений или какие-либо другие документы.

Кроме того, **мошенники начали предлагать людям обмен банковских бонусов на рубли.**

В последнее время набирает оборот новая схема мошенничества. Злоумышленники обзванивают граждан, представляясь сотрудниками банков, и предлагают обменять на рубли накопленный за покупки кешбэк и другие бонусные баллы. У человека запрашивают банковские данные и смс-код, полученный от банка, якобы для подтверждения операции и оплаты комиссии за услугу. На самом деле мошенники, заполучив эти сведения, просто крадут деньги со счета.

Если вам звонят с подобным предложением и просят предоставить ваши личные данные, прервите разговор. Сотрудники банков никогда не запрашивают по телефону трехзначный код с оборотной стороны карты или код из смс.

По любым банковским вопросам, в том числе по кешбэку, самостоятельно позвоните в банк.

**Банк звонит через мессенджер: в чем подвох?**

Мошенникам все сложнее обходить антиспам-фильтры, которые предупреждают людей о подозрительных звонках. Поэтому злоумышленники переходят на мессенджеры, в которых такой защитной системы нет. Номер абонента обманщики скрывают, а на аватар ставят логотипы известных банков, чтобы вызвать доверие людей.

Клиенты банка часто берут трубку, когда видят знакомый логотип. Злоумышленники представляются сотрудниками банка и под разными предлогами выманивают конфиденциальную информацию. Например, реквизиты карт, логины и пароли от онлайн-банка и коды из уведомлений об операциях. В итоге мошенники получают доступ к счетам и обчищают их.

Обращаем внимание, что секретные данные нельзя сообщать никому, даже представителям банка.

Если вам звонят от имени финансовой организации или ведомства и начинают разговор про деньги, лучше сразу положить трубку и самостоятельно набрать номер горячей линии организации.

**Мошенники начали звонить людям под видом сотрудников службы поддержки оператора сотовой связи.**

В последнее время мошенники начали звонить людям под видом сотрудников службы поддержки оператора сотовой связи.

Злоумышленники сообщают, что номер абонента скоро перестанет действовать. Чтобы избежать этого, человеку предлагают набрать на телефоне комбинацию цифр. В результате он подключает переадресацию звонков и текстовых сообщений, в том числе с смс-кодами от банка, на номера мошенников. Это позволяет им получить доступ к дистанционному управлению банковским счетом и похитить деньги.

Мошенники могут использовать разные легенды - сообщить, что необходимо переоформить договор об оказании услуг связи, поменять тарифный план на более выгодный, отключить платную услугу. Иногда они говорят, что поступила заявка о смене мобильного оператора с сохранением номера.

Независимо от причины звонка цель мошенников - либо получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо убедить абонента подключить ее самостоятельно.

Если вам позвонили с такими предложениями, прервите разговор. Самостоятельно позвоните в службу поддержки мобильного оператора по номеру, который указан на его официальном сайте