Руководителям управляющих организаций

ГОСУДАРСТВЕННАЯ ЖИЛИЩНАЯ ИНСПЕКЦИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

Красный проспект, 18, г. Новосибирск, 630011 Тел. /факс: 202-07-57; 203-59-00
gjinso@nso.ru
ИНН 5406308363 КПП 540601001
ОГРН1055406102223 ОКПО 76695499

06.08.2020 № 3746-04/48

На №_____от _____

О направлении методических материалов

Уважаемые руководители!

В Новосибирской области в текущем году выросло значительное число преступлений, совершаемых мошенниками. Чаще всего мошенники похищают деньги с банковских карт граждан и с их банковских счетов. В день фиксируется по несколько десятков сообщений о таких случаях мошенничества. В регионе только в июле совершено свыше 600 хищений денежных средств с банковских счетов граждан с причинением общего ущерба в размере более 40 миллионов рублей.

В целях повышения информационно-профилактической работы с населением по предотвращению подобных мошеннических действий направляем Вам методические рекомендации Правительства Новосибирской области «О предупреждении наиболее распространенных видов мошенничеств» и Памятку «О безопасном использовании банковских карт» (далее – Памятка).

Полагаем возможным размещение указанных материалов на официальном сайте управляющей организации, информационных стендах (стойках) в представительстве управляющей организации, на досках объявлений, расположенных в подъездах многоквартирных домов, а Памятки - на обороте платежных документов.

Дополнительно сообщаем, методические рекомендации и Памятка размещены на официальном сайте государственной жилищной инспекции Новосибирской области.

Приложение:
1. Методические рекомендации Правительства Новосибирской области «О предупреждении наиболее распространенных видов мошенничеств» на 6 л. в 1экз.;
2. Памятка «О безопасном использовании банковских карт» на 1л. в экз.

Начальник инспекции А.И. Полищук

Кот 2270183

Не менее опасно переходить по указанным в СМС ссылкам. Вместо розыгрыша призов и прочих «акций» можно легко попасть на сайт мошенников и получить вирус, крадущий с телефона абонента не только деньги, но и всю имеющуюся информацию.

Иногда мошенники обращаются к прохожим на улице с просьбой одолжить сотовый телефон, чтобы позвонить. После одного или нескольких звонков отзывчивый владелец мобильника обнаруживает, что баланс значительно меньше.

3. ***Платный код.*** Поступает звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

4. ***Штрафные санкции оператора.*** Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

5. ***Проблемы с банковской картой (счетом).*** Самые примитивные телефонные мошенничества банковскими картами или счетами рассчитаны на страх человека лишиться денежных накоплений и начинаются примерно одинаково: на телефон приходит СМС от «банка» или звонят мошенники, представляясь его сотрудниками. Информация может быть самой неприятной, например, о том, что заблокирована банковская карта или имеется задолженность по кредиту. В лучшем случае для разъяснения ситуации владельцу телефона предлагают позвонить оператору «банка». Те, кто после этого перезванивают, попадают на платный номер и теряют большую сумму со счета телефона.

Гораздо худшие последствия наступают, если по просьбе «банка» владелец телефона сообщает мошенникам номер карты и её пин-код, пароль от «Личного кабинета» интернет-версии банка, персональные данные и прочую информацию, которую следовало бы держать в секрете. В такой ситуации деньги с банковского счета обманутого абонента действительно бесследно исчезают.

6. ***«Мобильный банк»*** - приложение, которое позволит управлять вашим счетом. Участились случаи мошенничеств с использованием услуги «Мобильный банк», позволяющей управлять счетами через мобильное устройство. Данная услуга «привязывает» банковский счет к номеру телефона клиента банка.

Для предотвращения мошенничеств рекомендуем не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, адрес жительства и другую личную информацию. Не использовать в сети Интернет номера своих мобильных телефонов к которым привязаны банковские карты и номера мобильных телефонов, которые используются для работы в «Мобильном банке». В случае если с Вашего телефона, банковской карты похитили денежные средства необходимо немедленно обратиться в банк и заблокировать ваш счет, запретить перевод денежных средств с вашего счета на другие счета, приостановить

потребуйте сообщить сайт магазина в сети Интернет, юридический и фактический адрес.

Убедительно рекомендуем не осуществлять «слепые» покупки в социальных сетях. Администрация соц.сетей исключила разделы объявлений с сайтов и не несет ответственность за совершаемые с использованием сети действия пользователей.

При покупке железнодорожных и авиабилетов не приоретайте дешевые билеты на сомнительных сайтах, тем более расположенных в доменных зонах .com, .mobi, .org, .biz, .net, .info, .tv. и других не связанных с российским интернет-пространством. Осуществляйте покупку билетов на официальных сайтах компаний перевозчиков.

Способы и виды мошенничеств на сайтах объявлений:

1. Вам приходит SMS от имени сайта объявлений с предложением отправить текст на короткий номер в связи с тем, что вам поступили отклики по объявлению, или же ваш аккаунт был заблокирован. Впоследствии с вашего счета будут сняты деньги. Вернуть их будет невозможно. Рекомендуем не отвечать на подобные сообщения и обратиться в службу поддержки или к оператору мобильной связи с жалобой.

2. Мошенник под видом покупателя сообщает вам, что желает приобрести товар, но проживает в другом городе и предлагает оплатить товар путем перечисления денежных средств на карту продавца. Для этого он просит продавца назвать номер карты, владельца карты, срок действия карты, код на обратной стороне, а также сотовый номер привязанный к карте, либо по умолчанию использует номер, указанный в объявлении. После получения этих сведений мошенник использует данные о карте для оплаты покупок в сети Интернет.

Другие виды мошенничества в Интернете

1. На некоторых сайтах можно зарегистрироваться только, указав свой номер телефона, на который якобы должен прийти код для регистрации. Но если код не приходит в течение 5 минут (а он и не придет), вам самостоятельно необходимо отправить СМС на определенный номер. Не делайте этого! С вашего счета будут списаны денежные средства.

2. Инвестирование. На просторах Интернета существует множество сайтов, которые предлагают вложить свои деньги под определенный процент. Но многие из этих ресурсов обычный обман.

3. Методики, обучающие заработку в интернете. Вам предлагают приобрести руководство по заработку в сети Интернет (или методики иного характера), где дается подробная инструкция, как можно заработать определенную, как правило, большую сумму денег в день. Вам необходимо купить диск, оплатить пересылку и т.п. На самом вы приобретете «пустышку».

4. Фишинг - кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты.

Мошенничества с наличными купюрами:

1. Самым простым и распространенным является мошенничество путем замены настоящих купюр в пачке на фальшивые (в основном, сверху и снизу - настоящие, посередине - фальшивые или обычная бумага).

«Телефонные мошенничества» на сегодняшний день остаются одним из наиболее распространенных видов мошенничеств. На домашний (мобильный) телефон гражданину звонят неустановленные лица, представляясь родственником и сообщая легенду о «ДТП с пострадавшим», драке, доставлении в полицию и.т.д, при этом требуя денег «на лечение пострадавшего», либо «для непривлечения к уголовной ответственности».

Преступники (как правило, мужчины) искажают свой голос (картавят, шепелявят), имен при этом не называют. Если пострадавший сразу же называет имя, звонящий подтверждает, что это он. Чтобы человек, которому позвонили, не смог позвонить никому из родственников, его просят не отключаться и ведут с ним разговор до тех пор, пока он не перечислит денежные средства на абонентский номер либо на банковскую карту, номер которой также диктуют по телефону.

Правительство Новосибирской области