ПРОКУРАТУРА
НОВГОРОДСКОЙ ОБЛАСТИ

Памятка для граждан:

Как не стать жертвой дистанционных преступлений

Великий Новгород
2020

На территории региона сохраняется устойчивая тенденция к увеличению числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Потенциал современных информационно-телекоммуникационных технологий позволяет использовать их в качестве орудий или средств совершения почти всех известных уголовному законодательству преступлений.

Однако самыми распространенными дистанционными преступлениями являются **хищения**.

В соответствии со статьей 159 Уголовного кодекса Российской Федерации **мошенничество** – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Хищение денежных средств с банковской карты может также квалифицироваться по пункту «г» части 3 статьи 158 Уголовного кодекса Российской Федерации, как **кража**, совершенная с банковского счета, а равно в отношении электронных денежных средств.

Самые распространённые способы мошенничества – обмана по телефону:

- ✓ звонок «якобы» сотрудника правоохранительного органа с сообщением о возникшей проблеме у близкого родственника (ДТП, необходимость срочной операции, возбуждение уголовного дела, арест и т.п.), которую можно решить за плату;
- ✓ сообщение от неизвестного лица, представившегося сотрудником банка, о проблемах с банковской картой (несанкционированное списание, сомнение в действительности сделки, крупный размер списания и т.п.);
- ✓ сообщение от неизвестного лица об ошибочном пополнении средств на телефонном счету (злоумышленник просит вернуть денежные средства, когда фактически на счет денежные средства не поступали);

- ✓ просьба неизвестного, «якобы» попавшего в тяжелую жизненную ситуацию, оказать немедленную финансовую помощь;
- ✓ предложение оплатить выбранный на одном из сайтов сети «Интернет» товар безналичным способом;
- ✓ навязывание какой-либо услуги или товара (установка счетчиков расхода коммунальных ресурсов, оконных рам, дверей и т.п., продажа биологически активных добавок, лекарств, медицинских приборов и т.п.), в т.ч. с подписанием договора, с последующим «якобы» исполнением обязательств или взиманием платы, значительно превышающей существующие в городе цены;
- ✓ оплата комиссии за «якобы» выигранный приз в лотерее, об участии в которой Вы не помните.

«Схемы», используемые злоумышленниками для хищения денежных средств граждан с банковских карт:

- ❖ Мобильный банк:
  при установке приложений из интернета необходимо быть осторожными. Дело в том, что создатели программы специально заражают ее вирусом, который, проникая в смартфон, начинает работать на мошенников. Он заменяет окно мобильного банкинга поддельным, а владелец телефона вводит туда свои данные, ничего не подозревая. Вирус отправляет их мошенникам, которые затем незаконно получают доступ к карточному счету клиента. Для того, чтобы предотвратить такие махинации с банковскими картами устанавливайте только лицензионные приложения, а также антивирусные программы, а также периодически проверяйте количество денег на вашем счету.

- ❖ С помощью беспроводного терминала и бесконтактной технологии PayPass:
  злоумышленники снимают деньги у пассажиров с помощью беспроводного терминала через одежду и стенки сумок. Посредством бесконтактной технологии PayPass с карточки без PIN-кода можно снять до 1000 российских рублей. Чтобы снять деньги со счета, достаточно приложить устройство к карману или сумке, считыватели бесконтактных карт работают на расстоянии до двадцати сантиметров, достать их проблем не составляет.

- ❖ Смс-мошенничество:
  владельцу карты приходит смс-сообщение о том, что его карта заблокирована. Для ее разблокировки предлагается сделать обратный звонок оператору банка по указанному в смс номеру. При телефонном звонке мошенник представляется сотрудником банка и просит дать секретную информацию: номер банковской карты, кодовое слово и цифры пин-кода, якобы необходимых для разблокировки.
  При предоставлении этих данных мошенники могут воспользоваться денежными средствами, находящимися на банковском счете жертвы.

Как уберечь себя от мошенников:

- игнорируйте требования звонящего;
- не сообщайте персональные данные, в том числе обеспечивающие доступ к списанию денежных средств с банковской карты;
- свяжитесь со службой поддержки банка. Как правило, номер телефона, с которого был звонок, банку не принадлежит;
- позвоните своим близким и удостоверьтесь в правдивости информации о них;
- получите информацию о своих дальнейших действиях от лиц, которым Вы доверяете;
- если стали жертвой мошенников, обратитесь в полицию.