по карте или счету, или сообщить персональные данные, не спешите выполнять операции, навязываемые Вам собеседником. Помните, что работник банка никогда не спросит Ваши персональные сведения о карте. В этой связи лучше прекратите разговор, позвоните в службу техподдержки своего банка и следуйте ее инструкции. Для защиты денежных средств клиентов у банка есть вся необходимая информация. Также важно иметь при себе телефонный номер кредитного учреждения, чтобы в любой момент проконсультироваться в подозрительных ситуациях. Аналогичным образом необходимо действовать при получении СМС-сообщений подобного содержания;

- при совершении покупок в Интернете будьте особенно осторожными и внимательными, старайтесь не перечислять деньги дистанционно, не убедившись в благонадёжности продавца, сдержанно относитесь к заманчивым предложениям и скидкам;

- установите антивирус на компьютеры, смартфоны себе и родственникам.

Уважаемые граждане!
Помните, что злоумышленники совершают преступления, в основном пользуясь Вашей доверчивостью и неосмотрительностью.
Объясните пожилым родственникам и подросткам эти простые правила и будьте бдительны!

В СЛУЧАЕ СОВЕРШЕНИЯ В ОТНОШЕНИИ ВАС КИБЕРПРЕСТУПЛЕНИЯ, НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В ПОЛИЦИЮ.

Пример составления заявления о преступлении

Начальнику ОП № 8
УМВД России
по г.Н. Новгороду
от ФИО
проживающего по адресу:
тел. XXX-XXX-XX-XX

Заявление

Прошу привлечь к уголовной ответственности неустановленное лицо, которое позвонило мне на сотовый телефон, представилось сотрудником безопасности банка, после чего, введя меня в заблуждение, что с моей банковской карты совершаются операции, попросило меня продиктовать последние цифры моей банковской карты, после чего сообщить пароли пришедшие мне в СМС сообщениях. В результате действий неустановленного лица, с моей карты были похищены денежные средства в размере 30 тысяч рублей.

Об ответственности за заведомо ложный донос по ст. 306 УК РФ предупрежден.
Дата *Подпись*

Сообщить о факте мошенничества:
02 / 102
со стационарного телефона
с мобильного телефона
либо обратиться в ближайший отдел полиции

ПРОКУРАТУРА СОРМОВСКОГО РАЙОНА г. НИЖНЕГО НОВГОРОДА

ЗАЩИТИ СЕБЯ И СВОИХ БЛИЗКИХ ОТ КИБЕРМОШЕННИКОВ

ПАМЯТКА ДЛЯ ГРАЖДАН

В СВЯЗИ С РАСПРОСТРАНЕНИЕМ КИБЕРПРЕСТУПЛЕНИЙ ПРОКУРАТУРА ПРОСИТ ГРАЖДАН БЫТЬ БОЛЕЕ БДИТЕЛЬНЫМИ

С развитием современных информационно-телекоммуникационных технологий представить жизнь современного человека без уже ставших привычными нам технических устройств, электронных средств платежа, невозможно. Их простота и доступность в использовании привлекают все большее и большее число пользователей.

В то же время и преступники все активнее используют современные технологии в криминальных целях. В Российской Федерации отмечается рост преступлений, совершенных с применением IT-технологий, на 22,7%

В 80% случаев эти преступления направлены на получение личной информации пользователя (реквизиты банковских карт, паспортные данные, логины, пароли доступа и др.) и последующее хищение денежных средств или иного имущества граждан.

Особенно распространено совершение таких преступных деяний путем обмана м использованием сети Интернет, средств мобильной связи, расчетных (пластиковых) карт.

Зачастую, чтобы выяснить личные данные граждан и завладеть в последующем их денежными средствами, злоумышленники пользуются доверием людей, используют простые, но эффективные способы манипуляции, психологические навыки. Людям звонят рано утром, поздно вечером, нередко на выходных, надеясь застать врасплох. Преступники говорят уверенно, приводят «железные» доводы, сыплют профессиональной терминологией, запугивают своих жертв. Это может быть игра на родственных чувствах, боязнь потерять деньги или, наоборот, радость от их внезапного получения. В запасе у мошенников много историй, потому что теперь они нацелены не просто на похищение какой-то конкретной суммы, а на получение доступа к счетам и картам в целом.

Распространение получила схема, когда по телефону собеседник представляется сотрудником банка, говорит о том, что сработала система безопасности, и в данный момент по карте клиента проводится подозрительная операция.

Чтобы ее остановить, необходимо назвать, к примеру, кодовое слово или ПИН-код. В дальнейшем мошенники, применяя психологические манипуляции, давят на людей, стимулируют их к совершению определенных действий со счетом или карточкой, необходимых для похищения денежных средств. Зачастую гражданам на телефон присылают SMS-сообщения подобного содержания.

Популярны среди населения покупки в интернет-магазинах и на сайтах объявлений типа «Avito». При этом продавец нередко просит перечислить ему аванс за товар либо его полную стоимость с карты на карту. После перевода мошенник, естественно, исчезает.

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ, СОБЛЮДАЙТЕ ПРАВИЛА БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ:

- всегда проверяйте полученную информацию;

- не переходите по неизвестным ссылкам, не перезванивайте по сомнительным телефонным номерам;

- если получили сообщение о том, что родственник попал в беду, срочно свяжитесь с ним напрямую;

- не храните данные банковских карт на компьютере или в смартфоне;

- ни при каких обстоятельствах не передавайте и не сообщайте свои персональные данные кому-либо, в том числе номера, ПИН-коды и другие реквизиты банковских карт; номер паспорта; логины и пароли доступа; коды, которые банк направляет вам в виде СМС-сообщений;

- старайтесь не передавать третьим лицам свою банковскую карту, сотовый телефон, иные технические устройства;

- при поступлении звонков от лиц, представляющихся сотрудниками банка и предлагающих совершить какие-либо операции