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. Наряду с этим не отстают от них и преступники, использующие современные технологии в своих криминальных целях.

Число так называемых киберпреступлений в Интернет-сети с каждым годом увеличивается. Большинство преступлений направлено 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 с использованием сети Интернет, средств мобильной связи, расчетных (пластиковых) карт.

Зачастую чтобы выудить 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 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.

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

Для того чтобы не стать жертвой мошенников соблюдайте простые правила предосторожности: - ни при каких обстоятельствах не передавайте и не сообщайте, в том числе посредством сети Интернет, мобильной связи 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 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 и позвоните в службу техподдержки своего банка и следуйте ее инструкции. Для защиты денежных средств клиентов у банка есть вся необходимая информация. Необходимо также всегда иметь при себе телефонный номер кредитного учреждения, чтобы в любой момент проконсультироваться о подозрительных ситуациях. Аналогичным образом необходимо действовать при получении СМС-сообщений подобного содержания.

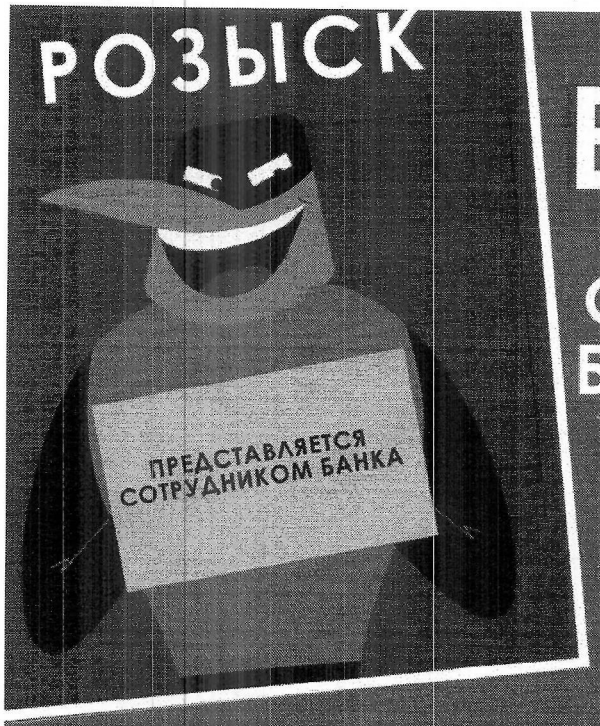
При совершении покупок в Интернете будьте особенно осторожными и внимательными, старайтесь не перечислять деньги дистанционно, не убедившись в благонадёжности продавца, сдержанно относитесь к заманчивым предложениям и скидкам;

Соблюдайте бдительность и осторожность при использовании сети Интернет, старайтесь не разглашать персональные данные. Используя электронную почту, старайтесь не открывать подозрительные и сомнительные письма, содержащие ссылки на сторонние Интернет-ресурсы. Не устанавливайте неизвестные программы на Ваши «девайсы» и технические устройства.

Уважаемые граждане!
Помните, что злоумышленники совершают преступления в основном пользуясь Вашей доверчивостью и неосмотрительностью.

ОМВД России по Ленскому району

УМВД РОССИИ ПО АРХАНГЕЛЬСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ



ВНИМАНИЕ!

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА

НИКОГДА

НЕ ЗВОНЯТ

ПО ПОВОДУ ПРОБЛЕМ СО СЧЕТОМ ИЛИ НЕЗАКОННОГО ОФОРМЛЕНИЯ КРЕДИТА

- НЕ СОВЕРШАЙТЕ ПОД ДИКТОВКУ ОПЕРАЦИЙ, КОТОРЫХ НЕ ПОНИМАЕТЕ
- НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НА ТАК НАЗЫВАЕМЫЕ «БЕЗОПАСНЫЕ» СЧЕТА - ЭТО ОБМАН!
- НЕ СООБЩАЙТЕ ПОСТОРОННИМ НОМЕРА И КОДЫ БЕЗОПАСНОСТИ БАНКОВСКИХ КАРТ

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ: 02 ИЛИ 112

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает, в регионе увеличивается количество случаев телефонного и интернет мошенничества.

1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.

2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!

3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с вашими деньгами.

4. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.

5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.

8. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку – преступление!

9. В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас!

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 02 или 112.