**Новые способы дистанционного мошенничества, а также преступлений совершенных, в том числе с использованием IT-технологий**

Несмотря на то, что значительное число граждан уже осведомлены о типичных случаях мошенничества, которое совершается с использованием мобильной связи, злоумышленники совершенствуют способы мошенничества, о которых потенциальные жертвы не знают.

Так, распространение получила мошенническая схема с незаконным использованием подменных абонентских номеров (используются номера банков, в том числе Центрального Банка России, подразделений МВД России, Следственного комитета России, органов прокуратуры Российской Федерации).

В частности, участились случаи незаконного использования подменных абонентских номеров и персональных данных руководства прокуратуры края.

Так, звонок осуществляется якобы сотрудником банка, который информирует о попытке оформления неизвестным третьим лицом кредита в онлайн-банке. Далее, злоумышленник убеждает гражданина в необходимости самостоятельно оформить онлайн-кредит на ту же сумму, обналичить поступившие на банковскую карту деньги и перечислить их на так называемый резервный счет для мгновенного погашения кредита. Для подтверждения информации звонок поступает от якобы сотрудников Центрального Банка России, подразделений МВД России, Следственного комитета России, а также от руководства прокуратуры края, которые подтверждают слова мошенника, представившегося сотрудником банка. При этом для реализации подмены номера звонящего, используются не только технологически сложные системы, но и более доступные варианты, например, с помощью Telegram-бота, который позволяет организовывать звонки с подменой номера прямо из мессенджера.

Более того злоумышленники в целях реализации мошеннических схем и оказания психологического воздействия на потерпевших используют и рассылают в мессенджеры поддельные повестки о необходимости явиться для допроса в качестве свидетеля, с использованием бланков правоохранительных и надзорных органов.

Типичными схемами мошенников, при которых последние получили доступ к денежным средствам граждан, явились такие случаи как:

1) Получение потерпевшими SMS-сообщение или поступление звонков от якобы работников банка о том, что банковская карта заблокирована, а также произошла попытка списания денежных средств. Также «сотрудник банка» просил граждан сообщить номер карты и PIN-код для ее перерегистрации. После сообщения потерпевшими запрашиваемых данных с их счетов списывались денежные средства;

2) На мобильный телефон потерпевших поступало SMS-сообщение о получении выигрыша, для получения которого необходимо было отправить подтверждающее SMS-сообщение, либо внести регистрационный «взнос» через систему электронных платежей. Однако после внесения на счет неизвестных лиц такого «взноса» никакого выигрыша потерпевшие не получили;

3) Имеют место случаи, при которых через сайт магазина в сети «Интернет» граждане заказали понравившийся им товар, однако после его оплаты потерпевшие ни только не получили заказ, но и лишились уплаченных за него денег;

Анализ преступлений, связанных с мошенничеством с использованием информационно – телекоммуникационных технологий показывает, что почти во всех случаях потерпевшие, потеряв бдительность, своими действиями упрощали преступникам доступ к своим денежным средствам.

Для того, чтобы избежать подобной ситуации и не попасть на уловки мошенников помните, что банки не рассылают сообщения о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

Не спешите действовать по инструкции неизвестных вам людей. Убедитесь в достоверности информации, полученной с незнакомых номеров, через уполномоченные организации, родственников или знакомых. Если вам звонят люди и представляются сотрудниками банка или полиции — перезванивайте по официальным номерам финансовых организаций и правоохранительных органов. Никому не сообщайте полные реквизиты банковских карт, ПИН-код, CVC/CVV-коды и одноразовые пароли для подтверждения операций.

Не переходите по подозрительным ссылкам и не оплачивайте покупки через сомнительные сайты.

Помните, что передача банковской карты или ее реквизитов, логина (идентификатора пользователя), PIN-кодов, паролей, контрольной информации и кода клиента, предназначенных для доступа и подтверждения операций  
в удаленных каналах обслуживания, другому лицу (в том числе работнику банка) означает, что Вы предоставляете возможность сторонним лицам проводить операции по счетам.

Если в отношении вас или ваших близких совершены противоправные деяния, немедленно сообщите о случившемся в полицию по телефону 102.

Помощник прокурора Кущевского района

юрист 3 класса П.А. Фоменко