О профилактике и предупреждении дистанционных преступлений в сфере информационно-телекоммуникационных технологий

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия в своих корыстных интересах. Следственное управление Следственного комитета Российской Федерации по Амурской области предупреждает об основных мошеннических схемах и напоминает правила безопасности

Распространенные схемы телефонного мошенничества:

1.Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанёс тяжкие телесные повреждения). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

2. Розыгрыш призов

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из указанных телефонных номеров. Во время разговора по телефону мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления необходимых документов, оплаты за комиссию перевода) счастливому обладателю новенького автомобиля необходимо перечислить на счет указанную ими сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки поступления денег на счет и получения «кода регистрации». Как только жертва завершает указанные манипуляции, счет обнуляется, а мошенники исчезают в неизвестном направлении. Если вы узнали о проведении лотереи только тогда, когда «выиграли» автомобиль, если вы не заполняли заявку на участие в ней либо каким-либо другим способом не подтверждали свое

© 2024 Следственное управление Следственного комитета Российской Федерации по Амурской области

участие в розыгрыше, то, вероятнее всего, вас пытаются обмануть. Будьте осторожны!

3.SMS-просьба.

Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони». Человек пополняет счёт и перезванивает, телефон по-прежнему не доступен, а деньги вернуть уже невозможно.

4.Ошибочный перевод средств.

Абоненту поступает сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

5. Платный код.

Поступает звонок, якобы 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.

6. Продажа имущества на интернет-сайтах.

При звонке на телефон, размещенный на Интернет-сайтах объявлений правонарушитель просит пополнить счет его телефона, либо сообщить данные и номер карты потерпевшего для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

7.Звонки или сообщения от сотрудников служб безопасности

При поступлении звонка или сообщения от лиц, представляющихся сотрудниками служб безопасности банков, правоохранительных органов, если указанные лица просят или требуют перевести ваши денежные средства на другие счета, оформить кредит, оказать помощь в пресечении мошеннических действий – немедленно прерывайте связь. Для убедительности мошенники могут даже присылать вам сканы документов и удостоверений личности реальных

© 2024 Следственное управление Следственного комитета Российской Федерации по Амурской области

сотрудников – это фальсификация. Ни по телефону, ни в ходе очной беседы сотрудники правоохранительных органов (СК России, ФСБ России, МВД России, Росгвардии и другие) не заявляют требований о переводе денежных средств на какие-либо счета. **Это незаконно!** Если есть сомнения, позвоните сами на телефоны доверия указанных служб (есть на официальных сайтах правоохранительных органов) и уточните достоверность звонка или сообщения с такими требованиями или просьбами.

Приведенный перечень мошеннических схем не является исчерпывающим. Злоумышленники находят все новые и новые схемы и способы для достижения своих преступных замыслов.

Как уберечься от телефонных мошенничеств?

Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

- остановитесь и не принимайте поспешных решений. Мошенники стремятся лишить вас времени для раздумья и требуют незамедлительно выполнить их указания. Возьмите паузу и обязательно посоветуйтесь с близкими, если не получается самостоятельно принять решение;

- не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;

- не следует отвечать на звонки или сообщения с неизвестных номеров с просьбой положить на счет деньги. Критически относитесь к подобным сообщениям из ваших контактов. Часто мошенники взламывают аккаунты пользователей сетей и получают доступ к их телефонным книгам, а затем через подменный номер от лица вашего знакомого используют полученные контакты для рассылки;

- не следует сообщать по телефону кому бы то ни было сведения личного характера.

Своевременное обращение в правоохранительные органы может помочь другим людям не попасться на уловки телефонных мошенников. Противостоять мошенникам возможно проявляя внимательность, здравомыслие и бдительность.

13 Сентября 2023

© 2024 Следственное управление Следственного комитета Российской Федерации по Амурской области

Адрес страницы: https://amur.sledcom.ru/news/item/1823982

© 2024 Следственное управление Следственного комитета Российской Федерации по Амурской области