***«Алло, здравствуйте! Вам звонят из службы безопасности банка…»...*** А вы знали, что такой способ обмана называется **вишинг**. **Вишинг (англ. vishing, от voice phishing) —***вид телефонного мошенничества, с помощью которого злоумышленники стараются заполучить конфиденциальную информацию для доступа к деньгам клиента.* Вам может позвонить якобы сотрудник банка, полиции, Социального фонда  России или налоговой службы.
 Самая распространённая схема: звонок от якобы сотрудника банка, который предупреждает о том, что если сейчас вы не предоставите ему данные банковской карты по телефону, то её заблокируют.
Злоумышленники могут прийти и с «хорошими» новостями: предложить выгодную покупку с огромной скидкой или рассказать о выигрыше в какой-либо акции.

Злоумышленники в диалоге с жертвой представляются сотрудниками банков, сотовых операторов, правоохранительных органов, медицинских учреждений, радиостанций и т.д. Такой способ хищения денег называется "вишинг" - от английского voice phishing: голосовой фишинг или выуживание. Под *вишингом* мы понимаем разновидность дистанционного хищения денежных средств, совершаемого с использованием средств телефонной связи и применением технологий, средств и методов социальной инженерии.

Целями вишинга могут быть:

1) выманивание у владельца банковской карты конфиденциальной информации с целью хищения денежных средств;

2) стимулирование владельца банковской карты к совершению определенных действий с банковским счетом или банковской картой с целью хищения денежных средств.

На сегодняшний день к основным способам дистанционных хищений денежных средств, совершаемых с использованием средств сотовой связи, относятся:

**Способ 1. Хищение, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств.**

Преступник от лица сотрудника банка сообщает жертве о фиксации системой безопасности подозрительной операции по ее банковскому счету (попытка снятия или перевода денежных средств, вход в личный аккаунт онлайн-сервиса банка, попытка оплаты товаров и т.д.). Далее под предлогом перевода денег на безопасный счет жертве предлагается продиктовать реквизиты своей банковской карты, в том числе и секретный код для подтверждения перевода. Получив необходимые данные по карте, злоумышленник посредством применения систем дистанционного банковского обслуживания (далее - ДБО) осуществляет перевод денежных средств на подконтрольные ему счета. Иногда жертве предлагается пройти в отделение банка и выполнить под диктовку злоумышленника необходимые операции с банкоматом, которые заключаются в осуществлении денежного перевода со своего счета.

Отдельно стоит отметить, что если совсем недавно злоумышленники осуществляли вызовы путем случайного набора цифр и при этом не имели какой-либо информации о будущем собеседнике, то сегодня все чаще преступники осуществляют противоправную деятельность в отношении конкретных лиц, предварительно располагая личным абонентским номером жертвы, паспортными данными, адресом фактического места жительства, местом работы и другой личной информацией. Такой способ хищения можно определить как целевой. Знание преступником личных данных жертвы существенно облегчает процесс установления доверительных отношений с ней.

Базу с персональными данными граждан можно приобрести в DarkNet и telegram-каналах. Причем возможно купить не только личную информацию (Ф.И.О., номера телефонов, паспортные данные, дата и место рождения), но и банковскую - остаток по счету, дата последней операции и т.д. Подобные базы данных могут распространять недобросовестные сотрудники сотовых операторов, банков, государственных, иных учреждений.

Иногда злоумышленники используют автоответчик, который приветствует абонента, сообщает об определенной проблеме, а уже после этого происходит подключение к злоумышленнику. Также бывают случаи, когда разговор начинает один преступник, представляясь оператором, он же в последующем переводит жертву на якобы "сотрудника службы безопасности", который в последующем и выманивает всю необходимую информацию по карте и пароли.

Такие приемы направлены на повышение доверчивости жертвы к злоумышленнику и сообщаемой им информации.

Отдельно стоит отметить, что при совершении дистанционных хищений преступниками активно используются методы социальной инженерии. Задача любого мошенника – «социального инженера» заключается в том, чтобы «взломать» психологию субъекта атаки, вывести его в сферу доверительных отношений и заставить предпринять необходимые для мошенника действия, которые в обычной жизни человек никогда не стал бы делать.

**Способ 2. Хищение, совершенное под предлогом компенсации за ранее приобретенные БАДы или некачественные лекарства.**

На абонентский номер жертвы звонит злоумышленник, который представляется сотрудником государственных органов (органы здравоохранения, прокуратуры, правоохранительные органы и т.д.), и сообщает, что потерпевшему полагается денежная компенсация за ранее приобретенные им некачественные товары (медицинские препараты, БАДы и др.). Для получения данной компенсации жертве необходимо произвести уплату страхового взноса, подоходного налога, государственной пошлины, услуг адвоката и т.д.

**Способ 3. Хищение, совершенное под предлогом помощи родственнику, попавшему в беду.**

Злоумышленник звонит жертве и обращается к ней под видом родственника (внука, сына и т.д.). Затем встревоженным и чуть слышным голосом сообщает, что он был задержан сотрудниками правоохранительных органов за совершенное им ДТП, нанесение телесных повреждений, сбыт наркотиков и т.д. После в разговор вступает второй злоумышленник ("сотрудник") или тот же злоумышленник, который просто меняет голос и спокойным тоном сообщает жертве, что, для того чтобы ее родственник остался на свободе, необходимо в кратчайшее время осуществить денежный перевод на определенный банковский счет или пополнить счет абонентского номера.

**Способ 4. Хищения через размещенные объявления.**

Злоумышленник ищет на сайтах объявлений (Юла, Авито, Моя реклама, ЦИАН и др.) или в группах социальных сетей (ВКонтакте, Одноклассники и др.) объявления о продаже какого-либо товара. Затем звонит по указанному в объявлении номеру и сообщает жертве, что желает приобрести товар и хочет внести задаток, для чего просит жертву продиктовать реквизиты банковской карты и поступивший секретный СМС-пароль.

**Способ 5. Хищение, совершенное под предлогом получения выигрыша.**

Злоумышленник осуществляет звонок жертве и представляется ведущим известной радиостанции, сотрудником оператора связи, представителем крупного бренда и т.д. Далее злоумышленник сообщает, что жертва выиграла в лотерее ценный приз (денежная сумма, ноутбук, смартфон, туристическая поездка, абонемент и т.д.). Для получения данного приза жертве предлагается оплатить налог на выигрыш и/или продиктовать "сотруднику" реквизиты банковской карты для зачисления выигранных денежных средств.

Необходимо понимать, что злоумышленники постоянно адаптируют и совершенствуют преступные схемы с учетом событий и явлений, происходящих в современном обществе. Такая трансформация и актуальность преступных схем позволяют преступникам на протяжении долгого времени эффективно осуществлять преступную деятельность и систематически получать высокий доход. В 2020 - 2021 гг. актуальность стали приобретать преступные схемы, связанные с пандемией COVID-19. Преступники выманивают конфиденциальную информацию у граждан под предлогом предоставления господдержки, компенсации ущерба от коронавируса, различного рода пособий, также осуществляют массовую рассылку СМС-сообщений с требованием уплатить штраф за нарушение карантина и т.д.

Ведущий специалист отдела инвестиций

и развития малого и среднего

предпринимательства управления

экономического развития и инвестиций

администрации МО Ейский район Н.С. Соловей