Результат – списание денег со счетов, взятие кредита.

Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы. Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика. Важно помнить, что налоговая не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

Удаленное управление устройством под видом технической поддержки

Злоумышленники представляются сотрудниками технической поддержки банка, сообщают, что зафиксирована попытка мошеннических манипуляций с картой жертвы. Убеждают в необходимости сохранить денежные средства и защитить банковское приложение. Жертва соглашается установить на смартфон приложение удаленного управления и разрешить подключение к устройству «сотруднику банка». Мошенники могут направлять файл с программой удаленного управления напрямую клиенту через мессенджер или предлагают ее скачать в Google Play или App Store. Если удалось убедить жертву установить программу удаленного доступа, мошенники просят зайти в мобильное приложение банка и проверить сохранность средств, а затем положить устройство экраном вниз и подождать пока сотрудники настроят приложение или переведут средства на «безопасный счет».

Фиктивные социальные выплаты и компенсации

На специализированных теневых площадках в сети Интернет злоумышленники приобретают похищенные базы данных граждан (ФИО, даты рождения, адрес и пр.), обманутых ранее при покупке БАДов, поддельных лекарств, турпутевок. Используя эту информацию, мошенники обзванивают жертв и представляются сотрудниками Пенсионного фонда России, Росздравнадзора, банков, социальных служб. Жертве предлагается получить компенсацию или выплаты, для получения которых необходимо сообщить реквизиты банковской карты для поступления средств.

«Ошибочный» перевод

Мошенник отправляет деньги на счет жертве, а затем звонит и убеждает вернуть их. В это время обращается в банк, чтобы отменить свой перевод до наступления момента безотзывности.

Наиболее распространенные схемы киберпреступлений

Обман под видом службы безопасности

Злоумышленники представляются представителями службы безопасности банка, Центрального банка России, Росфинмониторинга либо правоохранительного органа и сообщают, что мошенники с использованием персональных данных потерпевшего оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения потерпевшему сообщают о необходимости оформления кредитов и их перевода. Следует отметить, что общение потерпевшего со злоумышленниками является длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.). Для достоверности мошенники могут присылать жертве поддельные документы от имени банка и других организаций. Следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка России не осуществляют работу с физическими лицами.

Злоумышленники «продают» Вашу квартиру или машину

Злоумышленники в ходе телефонного разговора представляются представителями службы безопасности коммерческого банка, Госуслуг, Центрального банка России либо правоохранительного органа. Сообщают о том, что персональные данные с личного кабинета утекли и теперь преступники могут от Вашего имени продать квартиру, машину, используя электронно-цифровую подпись. В целях защиты убеждают срочно продать имущество и перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

СМС от работодателя

Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя (возможно использование подменных номеров) о том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, с которым ему следует пообщаться. После этого звонит мошенник, представляется сотрудник с именем, указанным руководителем, и сообщает о попытках перевода личных сбережений на иностранные счета/финансирование территоризма/Украины и т.п. В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.