

Как не стать жертвой телефонных мошенников?

В Тюменцевском районе количество преступлений связанных с хищением денежных средств граждан с банковских карт и счетов, совершенных с использованием современных технологий, остается на достаточно высоком уровне 18% от общего числа зарегистрированных преступлений. Хотелось разъяснить читателям простые правила, которые могут предотвратить совершение в отношении вас данных видов преступлений.

Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает возможность осуществления противоправных деяний, связанных с использованием информационных технологий. Новые технологии все чаще выступают средством совершения самого широкого круга преступлений. Наиболее распространены хищения денежных средств, мошенничества, кражи с банковского счета и иные преступления.

К сожалению, продолжает фиксироваться рост регистрации преступлений, совершенных с использованием информационно – телекоммуникационных технологий (Справочно: в 2024 году было совершено в отношении жителей района 12 таких преступлений, в 2023 г. -9, ущерб от которых причинен потерпевшим на сумму свыше 2,9 млн рублей (в 2022 г.-2,4 млн.)). В ходе допросов участников уголовного процесса установлено, что граждане в достаточной степени не информированы о наиболее распространенных и новых способах дистанционного хищения денежных средств.

Существует множество способов дистанционного изъятия денежных средств у граждан. Условно их можно разделить на две большие группы: контактные и бесконтактные.

Как правило, при совершении хищений денежных средств граждан дистанционным способом применяются средства связи – мобильные телефоны, либо Интернет — ресурсы.

Анализ рассматриваемой категории преступлений показывает, что подавляющее большинство дистанционных хищений совершаются с помощью так называемых методов «социальной инженерии». Обман, игра на чувствах, шантаж — типичные и широко известные способы манипуляции, с помощью которых преступник завладевает конфиденциальными сведениями о банковских картах, расчетных счетах (их номерах, данными владельцев, сроке действия, CVV/CVN-коде).

При совершении преступлений дистанционным способом преступники используют различные поводы, чтобы завладеть конфиденциальной информацией.

Вот лишь некоторые из них:

- «Ваш родственник, либо близкий человек попал в беду»,
- «Ваша организация будет подвергнута проверке компетентными органами»,
- «С Вашего банковского счета происходят операции по списанию денежных средств»,
- «Вам ошибочно переведены денежные средства»,
- «Вы участвуете в акции и выиграли приз»,

- «Положи мне на телефон деньги, не могу до тебя дозвониться»,
- «Переведите предоплату в счет подтверждения покупки товара»,
- «Я готов приобрести у Вас товар и перечислил денежные средства, верните их, изменились обстоятельства»,
- «Ваш почтовый ящик заблокирован, срочно пройдите по ссылке»,
- «Вам положена компенсация за лекарства»,
- «Ваши инвестиции в наш бизнес — гарантия отличного дохода»,
- «Вы можете предупредить преступление, сообщите свои данные» и другие.

Чтобы избежать негативных последствий для себя и своих близких, в особенности несовершеннолетних, необходимо быть предельно бдительными и помнить основные правила безопасного поведения и общения посредством информационно-телекоммуникационных технологий.

Ниже публикуем профилактическую памятку: как противостоять угрозе киберпреступности, в которой освещены способы профилактики преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Памятка о том, как не стать жертвой кибермошенников.

1. Как защитить свой компьютер от вредоносных программ.

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Рекомендации по обеспечению безопасной работы в Интернете:

- Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы

- Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов

- Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять

- Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой

- Используйте сложные пароли, не связанные с вашей жизнью

- Расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: *ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.

2. Рекомендации о том, как уберечься от мошенничества с банковскими пластиковыми картами.

- Никому и никогда не сообщать ПИН-код карты
- Выучить ПИН-код либо хранить его отдельно от карты и не в бумажнике
- Не передавать карту другим лицам – все операции с картой должны проводиться на Ваших глазах
- Пользоваться только банкоматами не оборудованными дополнительными устройствами
- По всем вопросам советоваться с банком, выдавшим карту
- Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций
- Поставьте лимит на сумму списаний или перевода в личном кабинете банка
- Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно
- Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка

3. Рекомендации о том, как уберечься от телефонных sms-мошенников

Мошенники знают психологию людей. Они используют следующие мотивы:

- Беспокойство за близких и знакомых.
 - Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
 - Желание выиграть крупный приз.
 - Любопытство – желание получить доступ к SMS и звонкам других людей
- Наиболее распространенные схемы телефонного мошенничества:
- Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.
 - SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сын» и т.п.
 - Телефонный номер — «грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.
 - Выигрыш в лотерею, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.
 - Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.
 - Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.
 - Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку. Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Рекомендации:

- Не общайтесь с посторонними людьми по телефону и не сообщайте номера своих банковских карт, коды доступа, смс — сообщения которые поступают к вам на телефон.

- Перед тем, как перевести денежные средства на номер сотового телефона лица, которое сообщает Вам, что он Ваш родственник и попал в трудную ситуацию — свяжитесь с родственниками по достоверно известным Вам телефонам и уточните информацию

- Если Вам сообщили, что Ваша карта заблокирована обращайтесь в отделение банка оператору, не выполняйте указания человека, представившегося оператором.

- По возможности не используйте телефон, на котором подключено приложение «Мобильный банк», так как Ваш телефон может быть заражен вирусом, который в дальнейшем без Вашего ведома переведет денежные средства с банковской карты на чужой счет.

Прокурор Тюменцевского района
Путилин А.А.