Об уголовной ответственности за хищения персональных данных, денежных средств в сфере и с использованием информационно-телекоммуникационных технологий (далее – ИТТ) и меры предосторожности.

Стремительный рост числа преступлений в сети Интернет свидетельствует о том, что преступники теперь используют цифровую/виртуальную среду также активно, как и реальный мир, что создает для них новую специализацию в преступной сфере: в 2023 году в Российской Федерации было зарегистрировано более 2 миллионов преступлений, из которых более 500 000 (>25%) были преступлениями с использованием ИТТ.

В секторе ИТТ происходят различные преступления, в основном это интернет и мобильное мошенничество с целью хищения денег с банковских счетов граждан ст. 159 УК РФ. Среди других преступлений - кража с помощью платежных карт (пластиковых карт) - п. «г» 3 ст. 158 УК РФ; производство, использование и распространение вредоносных программ - ст. 273 УК РФ; распространение незаконной информации через интернет - ч. 2 ст. 128.1 УК РФ.

Важным элементом защищенности Ваших персональных данных и денежных средств являются знания.

Для этого рассмотрим некоторые из наиболее распространенных техник, используемых злоумышленниками в сфере ИТТ. К ним относятся:

1. Фишинг - вид интернет-мошенничества, который используют для получения доступа к личной информации пользователя: логинам, паролям, номерам телефонов, данным банковских карт и так далее посредством массовых рассылок электронных писем на электронную почту, текстовых сообщений.

2. Вишинг (голосовой фишинг) - это специальное манипулирование телефонными сетями с целью получения личной и финансовой информации жертв. После создания копии системы банка жертву просят (предпочтительно через поддельное электронное письмо) позвонить по номеру банка для подтверждения деталей.

Система банка копирует и отклоняет данные, введенные жертвой.

3. SMS-мошенничество - мошенники рассылают SMS-сообщения о транзакциях жертвы (блокировка банковских счетов и кредитных карт) и просят потерпевшего сообщить данные счета и пароли в полученном SMS-сообщении, что приводит к хищению средств;

4. Мошенничество с предоплатой - покупка и продажа товаров на разнообразных сайтах (Юла, Avito.ru и др.),

5. Поиск работы (JOB.ru, HH.ru или интернет ресурсы RABOTA.ru, HeadHunter.ru и др.);

6. Взлом аккаунтов в социальных сетях и отправка сообщений друзьям и знакомым с требованием денег - мошенники пользуются беспечностью людей и используют специальное программное обеспечение для входа в аккаунты в социальных сетях и отправки сообщений всем знакомым от имени

взломанного пользователя с описанием сложной жизненной ситуации и просят финансовой помощи или одолжить денег;

7. Мошенники, выдающие себя за сотрудников полиции или следователей, сообщают родственникам жертв, что те подозреваются в совершении несчастного случая или преступления, и предлагают им иммунитет от судебного преследования, если они переведут определенную сумму денег на указанный счет;

8. Участие в онлайн-опросах, сообщение о выигрышах в лотерею и компенсация за ранее оказанные услуги - мошенники предлагают крупные суммы денег пользователям Интернета, которые участвовали в онлайн-опросах или сообщили о выигрыше в лотерею. Иногда требуется «депозит» для получения соответствующих документов или уплаты пошлины.

Как нужно действовать, чтобы не дать злоумышленнику похитить Ваши персональные данные, денежные средства?

В случае если к вам обратились по сотовой связи или же в онлайн, и под разными поводами пробуют признать данные о вашей банковской карте, пароли или же иную индивидуальную информацию, будьте аккуратны: это видимые симптомы действий злоумышленников.

Если у Вас появились подозрения, советуем закончить общение и как можно быстрее связаться с банком по телефонному номеру, обозначенному на оборотной стороне вашей банковской карты. Не следуйте рекомендациям третьих лиц.

Сохраняете вашу карту в недоступном от посторонних людей месте. В случае если совершено хищение с Вашей банковской карты, немедленно пишите заявление в ближайший отдел полиции.

Уважаемые граждане, ни в коем случае не наносите информацию на банковскую карту о код-пароле (пин-код) для доступа к банковской карте посредством терминала, не храните такую информацию в непосредственной близости с банковской картой в виде записей на листе и тому подобное. Такие действия создают беспрепятственную возможность для злоумышленников по обналичиванию денежных средств с банковского счета.

При заявлении в полицию необходимо приложить копию выписки счета, полученную предварительно в банке, где станет заметно перемещение денежных средств по счету. Кроме того возможно обеспечить детализацию телефонных звонков и смс, это в случае, если хищение денежных средств произошло методом телефонной связи.