ПАМЯТКА
ПО ПРОФИЛАКТИКЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В современном мире информационно-телекоммуникационные технологии затрагивают все сферы жизни человека. Одновременно с этим, распространение получили и преступления, совершаемые с использованием данных технологий.

На территории Российской Федерации распространено дистанционное мошенничество, к которому относятся:

1. «фишинг» – вид дистанционного мошенничества посредством разговора по телефону или направления электронного письма или смс-сообщения, при котором злоумышленники получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств.

2. «фарминг» – направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг;

3. «двойная транзакция» - «ошибка» при оплате товаров или услуг с предложением повторить операцию, в дальнейшем денежные средства описываются дважды по каждой из проведенных операций;

4. «траппинг» - манипуляция с картридером банкоматов, позволяющая не возвращать карту владельцу или списывать все данные карты для дальнейшего их использования.

Чтобы обезопасить себя и своих близких от подобного рода мошеннических схем необходимо знать поведение злоумышленников, а также повышать уровень цифровой финансовой грамотности. Необходимо:

1. Установить на телефон или компьютер современное лицензированное антивирусное программное обеспечение;
2. Не устанавливать и не сохранять без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников;
3. Не использовать пароли, связанные с персональными данными;
4. Не сообщать данные карты, пароли и другую персональную информацию;
5. Поставить лимит на сумму списаний или перевода в личном кабинете банка;
6. В случае возникновения вопросов обращаться в банк, выдавший карту;
7. Не перезванивать по номерам и не переходить по ссылкам, которые приходят на e-mail или по SMS.

Как избежать вербовки и где искать честный заработок? Не поддавайтесь на заманчивые предложения и всегда проверяйте информацию, прежде чем принимать решение. Следуя советам в карточках, вы сможете избежать мошенничества и найти честные способы заработка.

Способы защиты от уловок вербовщиков:

● Не отвечайте на сомнительные запросы в соцсетях. Проверяйте, есть ли у Вас общие друзья с человеком, который просит его добавить.

● Прочитайте его посты, прежде чем отвечать на запрос.

● Проверяйте информацию. Если тебе делают заманчивое предложение по работе — подумай и посоветуйся со взрослыми, прежде чем давать ответ.

● Проверяйте информацию, прежде чем делиться ей через свой аккаунт.

● Избегайте чрезмерного деление информацией и постами.

● Повышайте свою приватность регулярно обновив ее параметры в своих аккаунтах в социальные медиа.

● Будьте предельно аккуратными в выборе друзей в социальных сетях и предельно требовательными к запросам потенциальных друзей от незнакомых пользователей.

● Не поддавайтесь соблазну пройти всевозможные онлайн тесты в социальных сетях, даже если они уверяют вас, что вы “наследная принцесса” или “наследный принц”.

Будьте бдительны и не поддавайтесь на уловки мошенников! Способы и методы совершения краж и мошеннических действий постоянно меняются. В случае малейших подозрений на обман незамедлительно сообщайте об этом в правоохранительные органы по телефону «02» или «112».