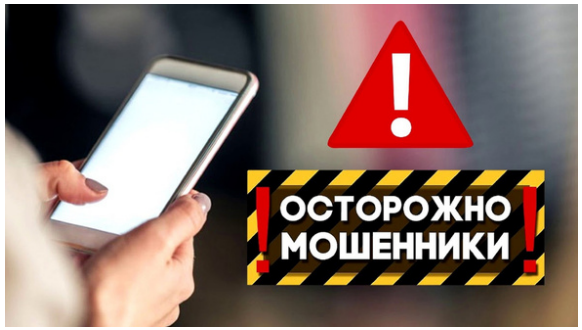
Краевое государственное бюджетное учреждение социального обслуживания «Краевой центр семьи и детей»

Буклет по профилактике преступлений, совершенных 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

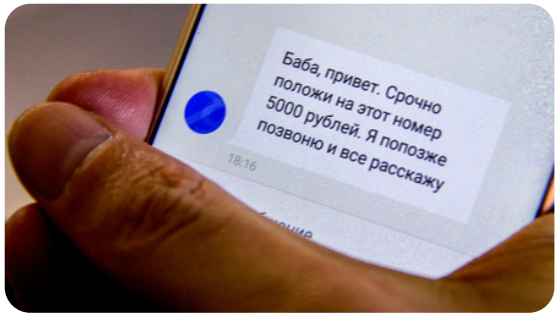
3. «двойная транзакция» - «ошибка» при оплате товаров или услуг с предложением повторить операцию, в дальнейшем денежные средства описываются дважды по каждой из проведенных операций;

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

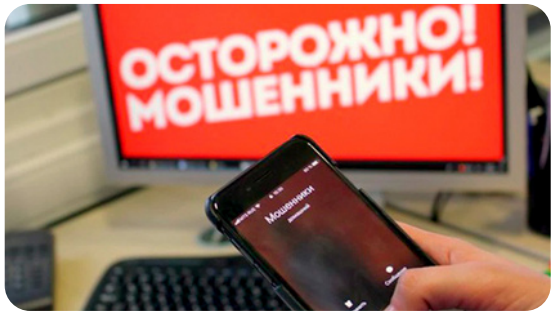
Основные схемы телефонного мошенничества:

1. Обман по телефону.

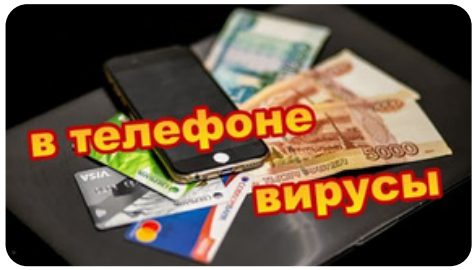
2. SMS-просьба о помощи.



3. Телефонный номер-грабитель.

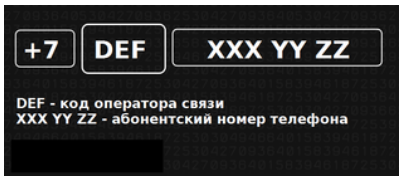


4. Телефонные вирусы.

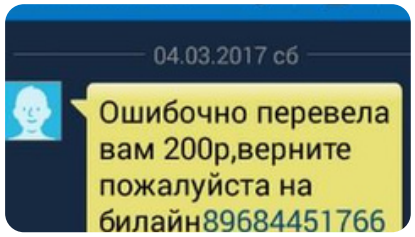


5. Выигрыш в лотерее или какого-либо приза.

6. Простой код от оператора связи.



7. Ошибочный перевод средств.



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.

БУДЬТЕ БДИТЕЛЬНЫ!