КГБУ СО «ЦЕНТР СЕМЬИ «НАДЕЖДА»

«Осторожно, мошенники! Как не стать жертвой финансового мошенничества?»

Как не попасться на удочку интернет-мошенников ?

Главная их цель — обманным путем получить от вас деньги или завладеть личными данными.

Что относится к личным(персональным) данным?

ПЕРСОНАЛЬНЫЕ ДАННЫЕ -ЭТО любая информация, относящаяся к определенному физическому лицу:

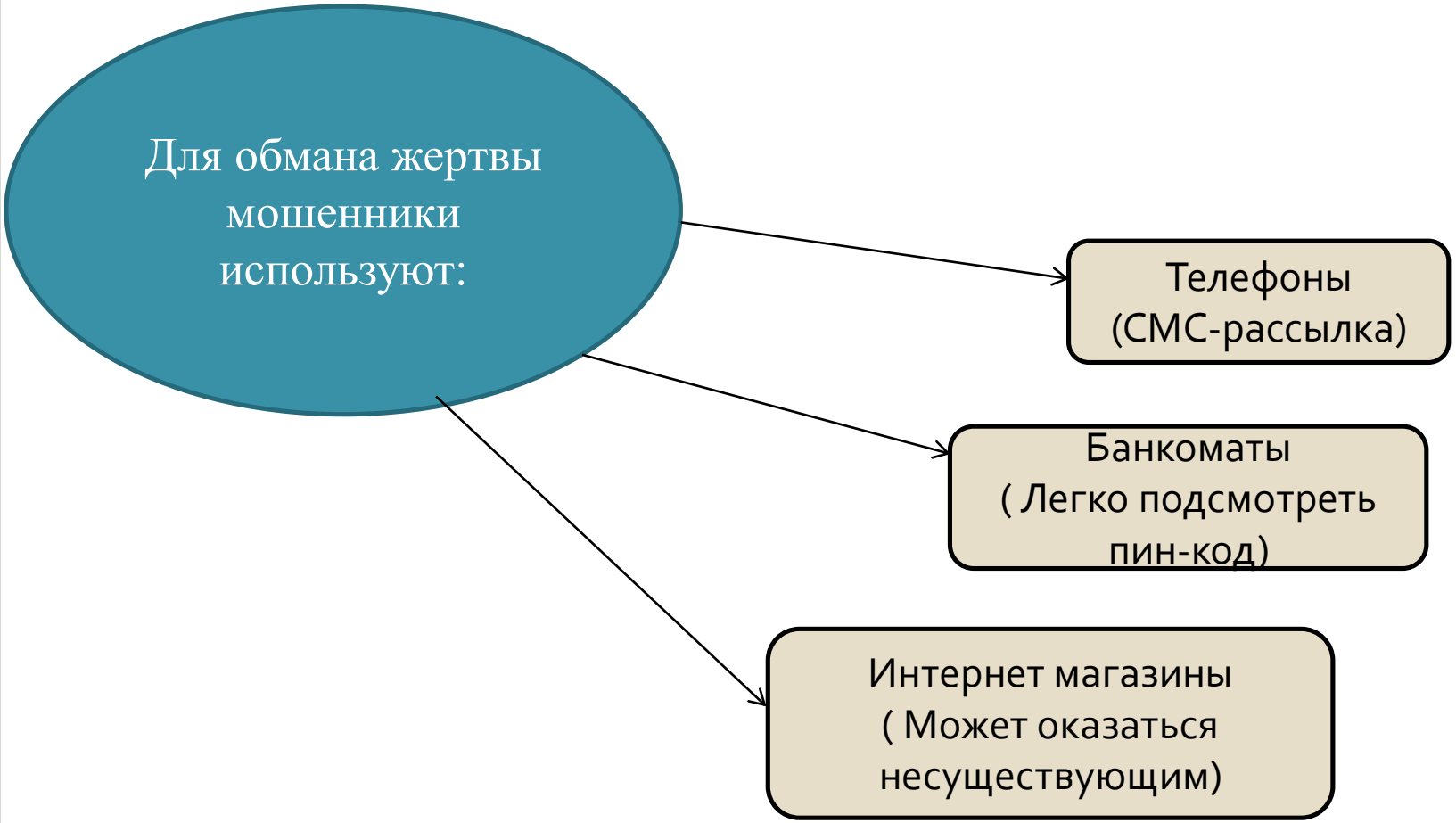
-ФИО;

- Дата рождения;
- Номер телефона;
- Паспортные данные;
- Место рождения;
- Семейное положение;
- Адрес электронной почты и др.

В интернете существует два основных вида угроз:

1. Социальная инженерия - это метод получения необходимого доступа к информации, основанный на особенностях психологии людей.

2. Вирусы и вредоносные программы


Для обмана жертвы мошенники используют:
Телефоны (СМС-рассылка)
Банкоматы (Легко подсмотреть пин-код)
Интернет магазины (Может оказаться несуществующим)

Финансовый обман по телефону:

Чтобы не попасться НИКОГДА нужно:

- Не отвечать на подозрительные письма;
- Не сообщать данные карты никому, даже сотруднику банка.

Если Вас обманули:

- Срочно позвонить в банк;
- Попросите заблокировать карту;
- Обратитесь в банк с паспортом;
- Запросите выписку по счету;
- Напишите заявление о несогласии операции;
- Обратитесь в полицию

Финансовая опасность у банкомата

Какая опасность подстерегает?

- Мошенники могут подсмотреть пин-код, а затем украсть у вас карту
- Данные карты могут сканировать с помощью скиммера, а пин-код заполучить с помощью незаметной видеокамеры или накладки на клавиатуру

Как не попасться?

- Осматривайте картоприемник и клавиатуру, на них не должно быть посторонних предметов
- Набирая пин-код прикрывайте клавиатуру рукой
- Не пользуйтесь банкоматами неизвестных банков

Финансовый обман в интернет-магазине

Вас должны насторожить!

- Очень низкие цены;
- 100% предоплата;
- Внесение денег в электронный кошелек

Как проверить интернет-магазин?

- Поищите отзывы в форумах или на самом сайте;
- Убедитесь в правильности набора адреса сайта в адресной строке браузера;
- попросите администратора интернет-магазина предоставить информацию о юридическом лице, проверьте её в общедоступных базах данных налоговых органов и реестр юридических лиц.

Основные виды мошенничества:

- Взлом аккаунта кого-то из ваших друзей;
- Сбор средств;
- Кликбейт;
- Выигрыши;
- Спам.

Взлом аккаунта кого-то из ваших друзей

— когда вам пишет человек с просьбой одолжить денег. Этот вид мошенничества работает, потому что он простой и дешевый.

Сбор средств

— здесь в ход идет социальная инженерия. Вы читаете, и вам с первых строк хочется помочь и дать денег, вам давят на жалость.

СОВЕТ ! Для того чтобы не отправлять деньги мошенникам, проверяйте всю информацию: позвоните в больницу и узнайте, есть ли у них такой пациент.

ФАКТ Семь из десяти объявлений о сборе средств на лечение — фейк.

Кликбейт

— заголовок, в котором очень захватывающий сюжет прерывается на самом интересном месте, и читателей отсылают смотреть продолжение в источнике.

В большинстве случаев кликбейт относительно безопасен — скорее всего читателя просто перенаправит на страницу с рекламными баннерами.

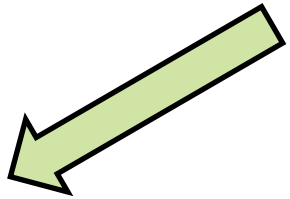
Однако такие новости могут быть опасными, потому что туда можно вложить ссылку с опасным контентом.

Выигрыши

Ситуация!

Например, это баннер, картинка или плашка якобы от браузера Google, где заявляется, что ваш IP-адрес был выбран в качестве победителя.

Как понять что это обман?



Во-первых, собрать базу всех IP-адресов невозможно, а даже если такая база есть, то большинство таких адресов будут серверами, а не личными компьютерами. К тому же, Google никогда не проводит лотереи. Такие розыгрыши — 100 % обман.

Спам

— Такие письма почти гарантированно содержат в себе вирус. Спам сейчас —примерно 80 % всего потока писем. Вы получаете такое письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные.

Советы, которые помогут избежать финансового обмана:

- Подключите услугу смс-оповещения по операциям с вашей банковской картой;
- Заведите несколько банковских карт;
- Установите лимит на съём денег и оплату по карте;
- Не храните пин-код вместе с картой;
- Настройте двухэтапную аутентификацию в соцсетях;
- Установите пароль на учетную запись Windows;
- Не открывайте папку спам;
- Не пытайтесь заработать на подозрительных схемах;
- Мыслите и оценивайте информацию критически.

Вывод:

Проблема не в том, что люди не знают о существовании мошенников, а в том, что они часто легко подвергаются психологическим воздействиям по разным причинам. Поэтому важно не паниковать. Стоит остерегаться незнакомых людей, которые пытаются навязать свои услуги, и не передавать никому коды доступа к своим счетам.

Задание на проверку:

1 Ситуация. Вам пришло SMS-сообщение от неизвестного абонента: «Уважаемый клиент! Ваша карта заблокирована. Была попытка несанкционированного снятия денег. Для возобновления пользования счётом сообщите по телефону *** данные по Вашей карте: Номер карты, PIN-код и CVV-код. В ближайшее время вопрос будет решён».

Расскажите, в чём состоит опасность данной ситуации для личных финансов?

2 Ситуация. Наталье позвонили из банка с предупреждением о попытке несанкционированного снятия денег с её счёта. Чтобы подтвердить её личность, банковские сотрудники предложили сверить персональные данные и номер счёта. Наталья заподозрила мошенников и решила не предоставлять информацию.

Что позволило Наталье сделать такой вывод? Возможно, она ошибается.

Контактные данные:

г. Красноярск, ул. Железнодорожников, д.30, помещение. 211

8 (391) 221-61-27

Письменное обращение по адресу электронной почты: mu005@list.ru

Сайт: центрсемьинадежда.рф

СПАСИБО ЗА ВНИМАНИЕ !