ндфп

ФИНАНСОВОЕ МОШЕННИЧЕСТВО:

как обезопасить себя

АНО «Дом финансового просвещения»
ГУ МВД России по Новосибирской области

Стать жертвой мошенника может каждый,
и не важно, используете ли вы банковскую карту
или рассчитываетесь наличными средствами.

ПОЧЕМУ МЫ СТАНОВИМСЯ ЖЕРТВАМИ МОШЕННИКОВ?

Дело в том, что они вызывают у нас разные эмоции

Положительные:

Радость
Надежда
Желание получить деньги

Отрицательные:

Чувство стыда
Паника
Страх

Жертва переводит средства «личному брокеру», который создает иллюзию активной работы и высокой доходности.

При попытке вывода денег всплывает «комиссия», после оплаты которой выясняется, что деньги получить нельзя, так как клиента якобы подозревают в мошенничестве.

Вам сообщают о «мошеннических действиях» в аккаунте. Чтобы избежать блокировки якобы нужно перейти в «системный центр».

Жертва вводит данные и лишается доступа к аккаунту.

Один из вариантов схемы - фейковый подарочный доступ к Телеграм-Premium

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ - ЗЛО

Телефон - основной инструмент мошенников.
Они обычно используют приемы и методы социальной инженерии.

1. **Обман или злоупотребление доверием**
2. **Психологическое давление**
3. **Манипулирование**

Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для хищения денег

ФОРМУЛА УСПЕХА
ТЕЛЕФОННЫХ МОШЕННИКОВ

эффект неожиданности

яркие эмоции

психологическое давление

актуальная тема

ПРАВИЛА
ЗАЩИТЫ СВОИХ ДЕНЕГ

- Никогда никому **не сообщайте свои данные**, данные карточек, пароли и пин-коды от банка
- **Не храните данные карт** и пин-коды на компьютере или смартфоне
- Установите **двухфакторную аутентификацию**
- Установите **антивирус на ваше устройство**
- **Не переходите по сомнительным ссылкам** и на подозрительные сайты
- Используйте для оплаты покупок **в интернете отдельную карту** и кладите на нее нужную сумму

- Будьте внимательны и не доверяйте неизвестным лицам, даже если они говорят убедительно
- Сотрудники банков никогда не запрашивают сведения по остаткам счетов, личные и финансовые данные

Федеральным законом от 24.07.2023 № 369-ФЗ внесены изменения в Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»

ВНИМАНИЕ!

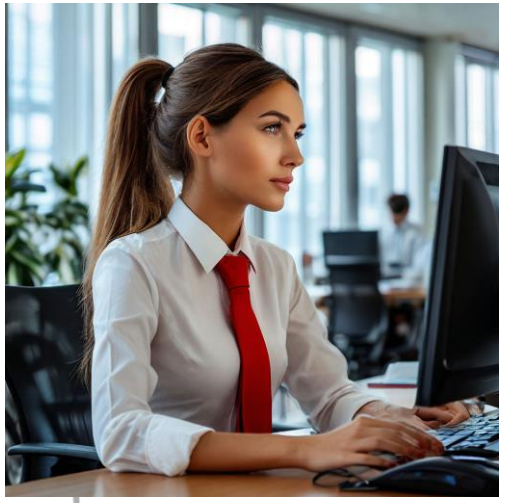
Если вы проявили бдительность, не сообщили никаких секретных данных мошенникам, а деньги все равно списались с карты, позвоните в свой банк и следуйте указаниям специалиста на линии.

Банк обязан вернуть вам деньги по вашему заявлению

МОШЕННИКИ УКРАЛИ ДЕНЬГИ С КАРТЫ.
ЧТО ДЕЛАТЬ?

1 БЛОКИРОВКА КАРТЫ
сразу же

2 СВЯЖИТЕСЬ С БАНКОМ
в течение суток



- в мобильном приложении банка
- звонком на горячую линию банка
- личным обращением в отделение банка

3 СООБЩИТЕ В ПОЛИЦИЮ
как можно скорее

- при личном обращении в ближайший отдел органов внутренних дел

ОСНОВНЫЕ ПОНЯТИЯ

- ✓ Мошенничество, связанное с интернет-магазинами
- ✓ Фишинг
- ✓ Интернет-попрошайничество
- ✓ Вирусы
- ✓ Социальные сети
- ✓ Кибербуллинг
- ✓ Интернет-знакомства
- ✓ Дропперы
- ✓ Сваттинг

МОШЕННИЧЕСТВО, СВЯЗАННОЕ С ИНТЕРНЕТ-МАГАЗИНАМИ

Через интернет могут предложить приобрести всё, что угодно, а распознать подделку при покупке через сеть бывает сложно.

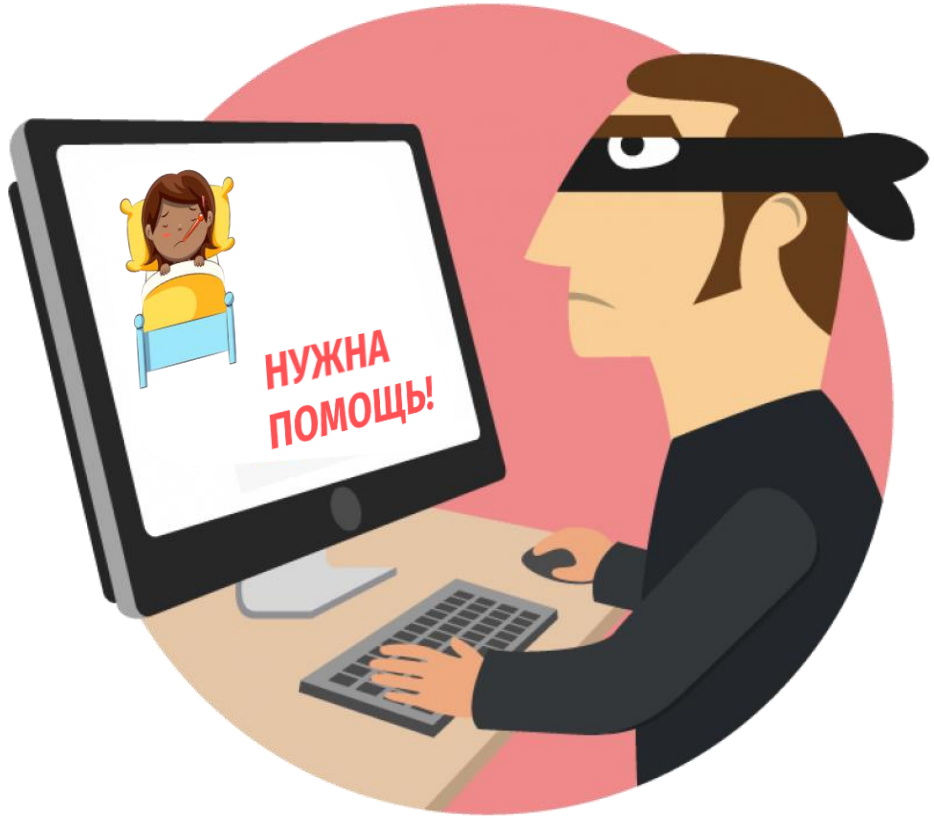
ФИШИНГ

Вид интернет-мошенничества, цель которого – получить данные, содержащиеся на карте. Злоумышленники рассылают электронные письма от имени банков или платежных систем.
Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка.

Для дальнейшей возможности использовать свою пластиковую карту просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счёте.

ИНТЕРНЕТ-ПОПРОШАЙНИЧЕСТВО

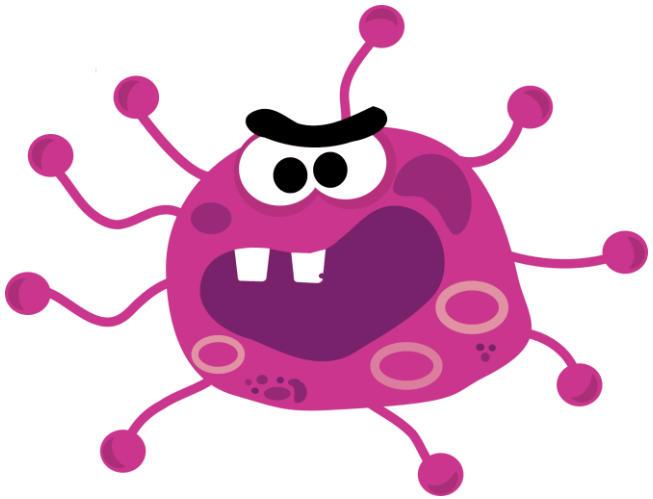
В интернете могут появляться объявления от благотворительной организации, детского дома, приюта или просто от родителей с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.



ВИРУСЫ

Сущность вируса – переадресация со страницы запрашиваемого ресурса на фиктивную. Подмена осуществлялась для самых популярных ресурсов: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники. Набирая на «зараженном» компьютере адрес ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему. После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная.

Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения.



СОЦИАЛЬНЫЕ СЕТИ

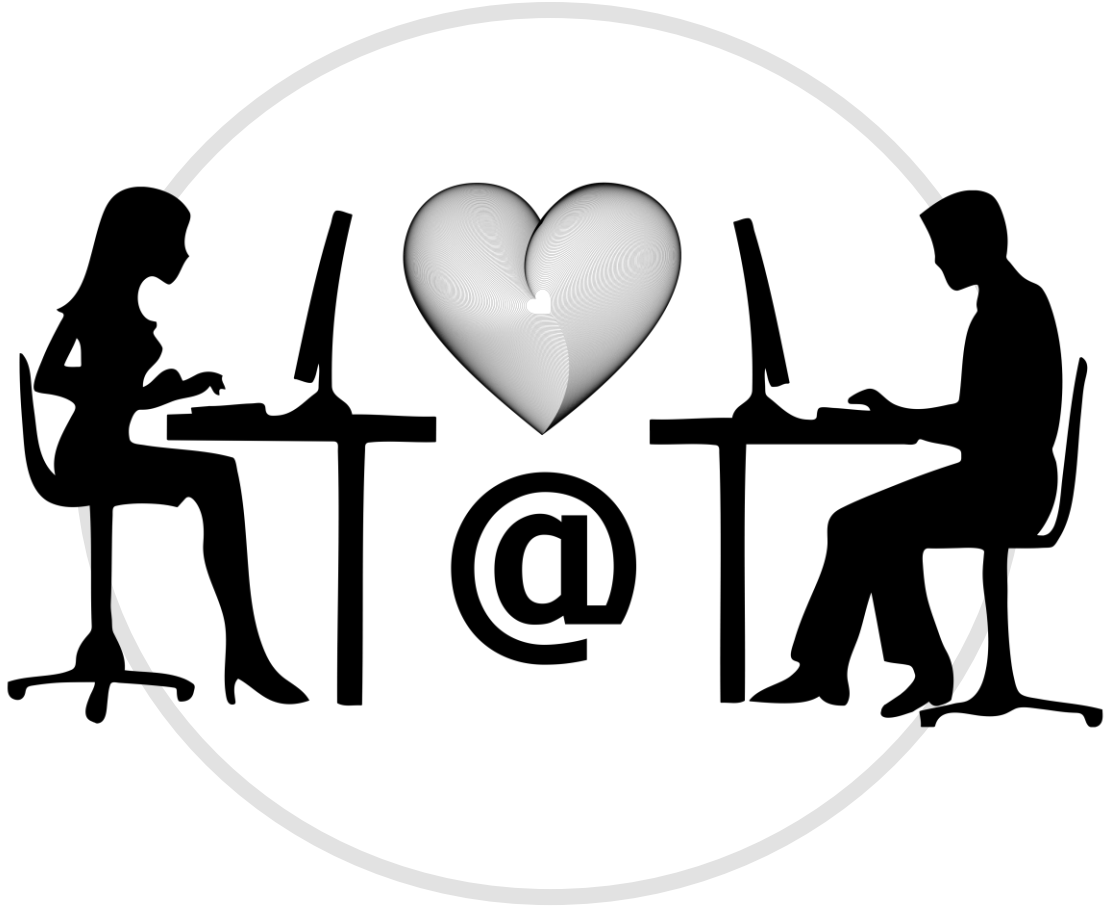
Социальные сети являются одним из способов вовлечения молодых людей в шантаж или же запрещенные группы, распространение порнографических материалов с участием несовершеннолетних.

КИБЕРБУЛЛИНГ

Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «тро́ллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах).

Это необходимо для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий, а возможно и с целью шантажа и выманивания определённой денежной суммы.

ИНТЕРНЕТ-ЗНАКОМСТВА

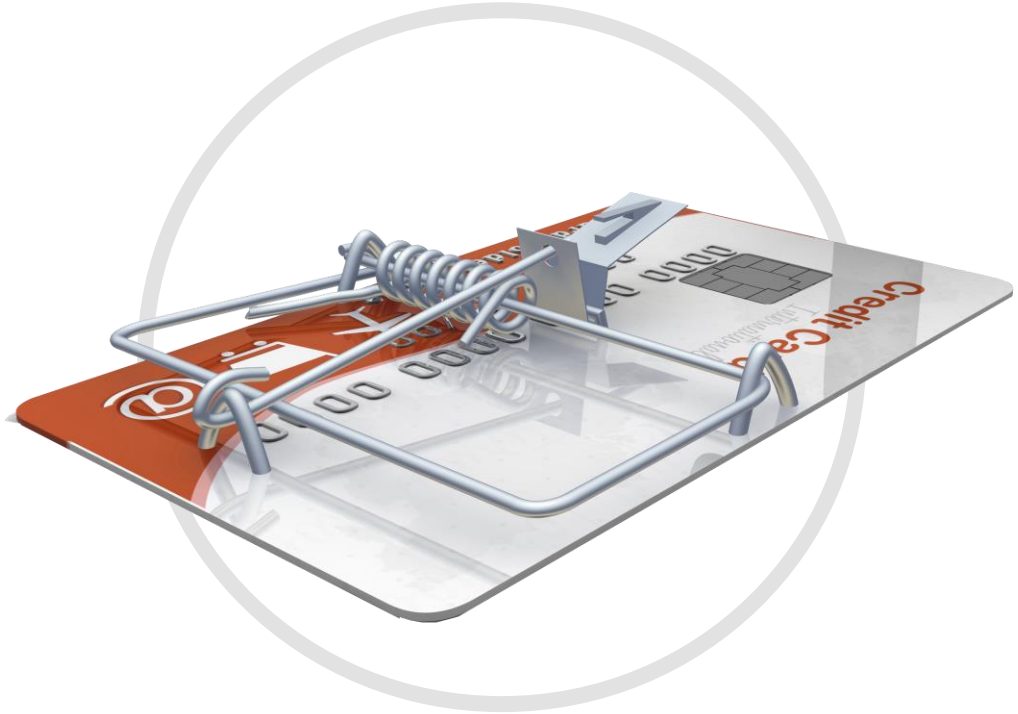


Мошенники с сайтов знакомств – это особый тип людей, способный втираться в доверие, очаровывать, чтобы завладеть деньгами или имуществом.

Им обычно свойственно глубокое знание психологии, умение построить общение так, что жертвы сами добровольно отдают им материальные ценности. Причем в такую ловушку могут попасть как девушки, так и юноши.

ДРОППЕРЫ

Дропперы — это лица, которые задействованы
в нелегальных схемах по выводу средств с банковских карт
за денежное вознаграждение.



Дропперы могут выполнять несколько обязанностей:

1

человек оформляет на своё имя банковскую карту,
отдает её мошенникам за вознаграждение

2

человек предоставляет данные своей банковской карты,
на которую переводят средства, добытые преступным путём,
в дальнейшем он обналичивает переведённую сумму
и передаёт мошенникам

СВАТТИНГ

Сваттинг — это вид правонарушения/преступления,
при котором лицо сообщает в экстренные службы
недостоверную информацию о происшествии,
чтобы направить сотрудников этих служб по ложному адресу.

Цели сваттинга:

- воздействие на общественное создание через нарушение функциональности социальной системы
- «розыгрыш» конкретного лица
- распространение чувства паники в обществе

ндфп

СПАСИБО ЗА ВНИМАНИЕ!