

ЛЁГКИЕ ДЕНЬГИ ИЛИ ОБМАН

(ВИДЫ МОШЕННИЧЕСТВА)

Мошенничества с использованием банковских карт, интернет
мошенничество, мобильные мошенничества, финансовые пирамиды

Мошенничества с использованием банковских карт

Основные виды:

- 1. Фишинг:** Обманные электронные письма и сайты для получения данных карт.
- 2. Скимминг:** Использование устройств для считывания данных карты на банкоматах.
- 3. Кардинг:** Использование украденных данных карт для покупок.
- 4. Вишинг:** Мошеннические звонки для получения данных карт.

**ОСТОРОЖНО,
МОШЕННИКИ!**

КАК ИХ РАСПОЗНАТЬ?

- ! Они представляются **сотрудниками служб безопасности банков, полиции, прокуратуры, Следственного комитета, Госуслуг**
- ! **Используют подмену номеров** – звонят с номеров банков, Госуслуг, спецслужб
- ! Мошенники **не дают прервать разговор**, постоянно просят вас быть на связи и не общаться с другими людьми
- ! Сообщают, что случилась беда. **Звонят или пишут от имени родственника, попавшего в беду**. Просят перечислить деньги, чтобы ему помочь
- ! Требуют назвать **код из СМС** (для доступа в личный кабинет Госуслуг или банка)
- ! Мошенники **постоянно меняют схемы** совершения преступлений
- ! Обещают **высокий доход**, процент доходности выше, чем в банке

Если вы попались на уловку мошенников, немедленно обращайтесь в **ПОЛИЦИЮ**



112 или **102**

Как избежать:

- Проверять подлинность электронных писем и сайтов.
- Проверять банкоматы на наличие посторонних устройств.
- Использовать одноразовые виртуальные карты для покупок в интернете.
- Не разглашать данные карты по телефону.

Интернет мошенничество

Основные виды:

- 1. Фальшивые интернет-магазины:** Привлекают покупателей низкими ценами.
- 2. Мошенничество в онлайн-объявлениях:** Продают несуществующие товары или услуги.
- 3. Мошенничество в социальных сетях:** Фальшивые аккаунты и страницы.
- 4. Фишинг через социальные сети:** Поддельные ссылки и приложения.

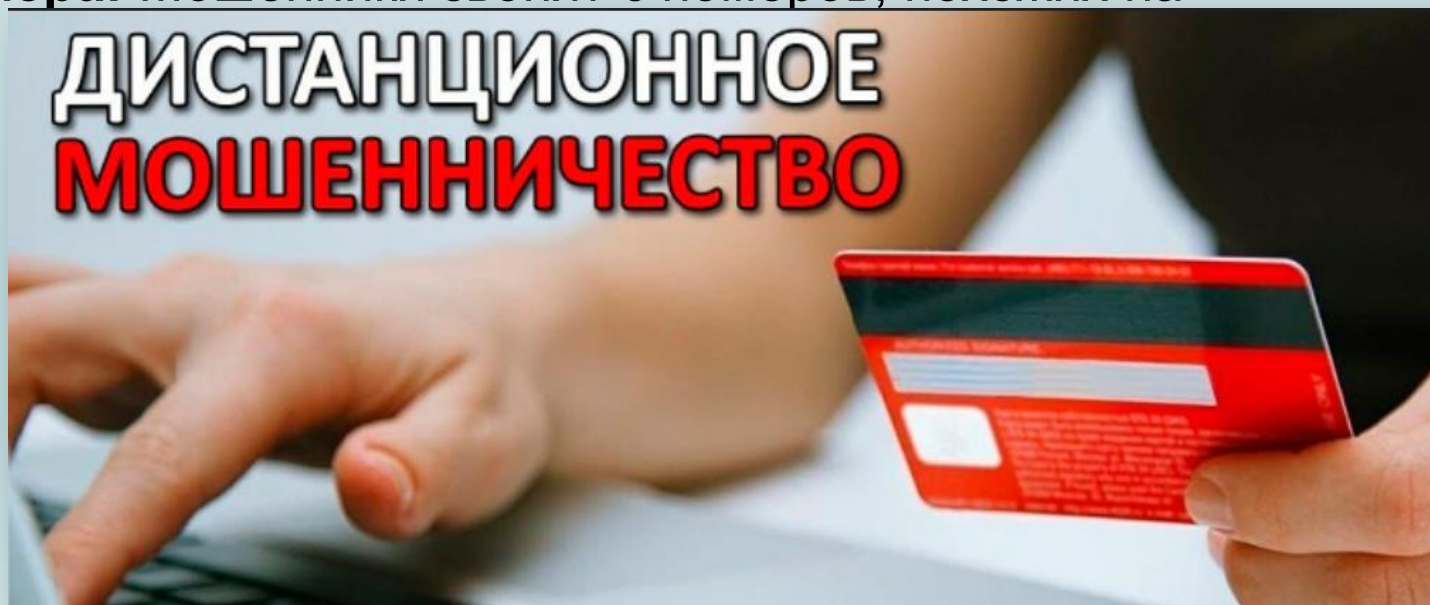
Как избежать:

- Проверять отзывы о магазине перед покупкой.
- Использовать платформы с защитой покупателя.
- Быть осторожными с переходами по ссылкам в социальных сетях.
- Использовать двухфакторную аутентификацию.

Мобильные мошенничества

Основные виды:

1. **SMS-фишинг:** Обманные сообщения с просьбой перейти по ссылке.
2. **Мошенничество через мобильные приложения:** Фальшивые приложения.
3. **Звонки с подменой номера:** Мошенники звонят с номеров, похожих на номера банков.



Как избежать:

- Не переходить по подозрительным ссылкам в SMS.
- Скачивать приложения только из официальных источников.
- Проверять подлинность звонков от банков, перезванивая по официальному номеру.

Финансовые пирамиды

Основные черты:

- 1. Структура пирамиды:** Новые участники платят за 'вход' в систему.
- 2. Примеры:** MMM, схемы Понци.
- 3. Опасности:** Высокий риск потери вложенных средств.
- 4. Как распознать:** Нереально высокие доходы, отсутствие реального продукта или услуги.

Как избежать:

- Проверять лицензии и регуляцию компаний.
- Избегать предложений с обещанием очень высоких доходов.
- Консультироваться с независимыми финансовыми советниками.

Заключение

Важность осведомленности и бдительности:

- Регулярное обучение и информирование населения.
- Использование сложных паролей и двухфакторной аутентификации.
- Проверка банковских счетов и кредитных отчетов.
- С осторожностью относиться к предложениям, которые кажутся слишком хорошими, чтобы быть правдой.
- Не стоит недооценивать значимость карточных данных. Бережно относитесь к ним и не сообщайте посторонним, даже если очень просят – от этого напрямую зависит сохранность ваших финансов.