**Телефонное мошенничество** - один из самых распространённых видов преступлений. Мошенники используют манипуляции, запугивание и социальную инженерию, чтобы выманить у жертв деньги или личные данные.

Мошенники постоянно придумывают новые способы обмана, но цель у них всегда одна – запугать, вызвать панику и заставить вас быстро передать им деньги или персональные данные.

Если вам звонят и говорят одно из следующего - это 100% мошенники!

* Мы из Национального банка, ваши деньги в опасности! Переведите их на безопасный счет.
* Это КГБ/милиция/Следственный комитет. Вы должны помочь в расследовании!
* Назовите номер банковской карты, код из СМС, паспортные данные.
* Ваша карта заблокирована!
* Ваш родственник попал в беду (ДТП, сбил человека и т.д.).
* Вам нужно срочно установить приложение на телефон.

**Общие признаки телефонного мошенничества:**

* Вам звонят «важные лица» - банковские сотрудники, силовики, следователи.
* Вас пугают потерей денег, уголовным преследованием, проблемами у близких.
* Требуют передать деньги курьеру или перевести на «безопасный» счет.
* Спрашивают персональные данные (номер карты, код из СМС, паспорт).
* Давят на скорость - «нужно решить прямо сейчас, иначе будет поздно!»

**Что делать, если вам звонят мошенники?**

* Прекратите разговор! Просто положите трубку.
* Перепроверьте информацию! Перезвоните в банк, право-охранительные органы, родственникам и т.д.
* Никогда не сообщайте:

✔ Паспортные данные.

✔ Реквизиты карты (номер, CVC-код).

✔ Логин и пароль от интернет-банка.

✔ Коды из СМС.

✔ Не устанавливайте приложения по указанию звонившего!

**Важно! Настоящие сотрудники банков и госорганов:**

* НЕ звонят в мессенджерах (Viber, Telegram, WhatsApp).
* НЕ звонят с зарубежных номеров.
* НЕ требуют перевода денег на "безопасные счета".

❌ **Если слышите подобное - это мошенники! ⛔ Будьте бдительны!**

**Фишинг** - это метод мошенничества, при котором злоумышленники выманивают личные данные (пароли, номера карт, коды из SMS) с помощью поддельных сайтов, писем или сообщений.

#### Основные виды фишинга:

**1.Фишинговые сайты**

* Вам приходит письмо или сообщение с просьбой войти в аккаунт (банк, социальные сети и т.д.).
* Ссылка ведёт на поддельный сайт, похожий на оригинальный, где просят ввести логин, пароль или данные карты.

❌ **Не вводите данные, если у вас есть сомнения в подлинности сайта!**

**2.Фальшивые письма и SMS**

* Приходит сообщение от «банка», «налоговой», «службы безопасности» или «интернет-магазина».
* Вас просят перейти по ссылке или скачать вложение, в котором может быть вирус.

❌ **Проверяйте отправителя, не открывайте подозрительные вложения!**

**3.Фишинг в социальных сетях и мессенджерах**

* Вам пишет «друг» или «коллега» и просит денег, ссылку на опрос или «интересное видео».
* После перехода по ссылке ваш аккаунт может быть взломан.

❌ **Свяжитесь с человеком напрямую, прежде чем выполнять его просьбу!**

#### Как защититься от фишинга?

* **Проверяйте адрес сайта перед вводом данных - он должен начинаться с "https://".**
* **Не вводите пароли и коды из SMS на подозрительных сайтах.**
* **Не переходите по ссылкам из писем и сообщений, если не уверены в их безопасности.**
* **Не скачивайте файлы из неизвестных источников - они могут содержать вирусы.**
* **Используйте двухфакторную аутентификацию (2FA) для защиты аккаунтов.**
* **Настройте антивирус и расширения для защиты от фишинга (например, Google Safe Browsing, Adblock, Adgurd и т.д.).**

**Если вы стали жертвой фишинга** - **срочно смените пароли и свяжитесь с банком, если передали данные карты! Берегите свои данные!**

**Мошенничество на сайтах объявлений и в социальных сетях**

**Как работают мошенники?**

* Выдают себя за известных продавцов (AliExpress, OZON, Lamoda и т.д.).
* Размещают объявления с продажей несуществующих товаров.
* Создают фейковые страницы в соцсетях, копируя бренды.
* Занижают цену на товар, создавая иллюзию выгодной сделки.
* Общаются только в мессенджерах, избегая звонков.
* Требуют предоплату или полную оплату на карту.

**Как не попасться?**

* Тщательно проверяйте информацию о продавце.
* Покупайте только у проверенных продавцов на официальных маркетплейсах.
* Избегайте слишком низких цен.
* Не переводите деньги на карту – пользуйтесь сервисами с защитой покупателя.
* Не соглашайтесь на "предоплату за доставку".

**Установка мошеннических приложений**

**Как мошенники заставляют установить вирус?**

* Присылают ссылку в мессенджере «от имени оператора» или банка.
* Убеждают, что «нужно обновить приложение».
* Приложение получает доступ к SMS и банковским данным.

**Как распознать фальшивое приложение?**

* Оно установилось как «дополнительное» к уже имеющемуся.
* Просит доступ к SMS, контактам и экрану.
* Показывает логотип вашего оператора, но скачано не из официального магазина.

**Что делать?**

* Немедленно отключите интернет.
* Удалите приложение.
* Заблокируйте банковские карты, если заметили странные операции.
* Используйте только официальные магазины (Google Play, App Store).

**Осторожно!**

**Мошеннические инвестиционные биржи**

Мошенники создают фальшивые инвестиционные платформы, заманивая людей обещаниями быстрой и легкой прибыли. Их цель - заставить вас перевести деньги и исчезнуть.

**Признаки мошеннической биржи:**

* Гарантируют высокую доходность при нулевых рисках. Если вам обещают огромные прибыли без риска - это обман. В реальном мире инвестиции ВСЕГДА сопряжены с риском.
* Неясные или запутанные условия. Такие платформы скрывают комиссии, требуют больших сумм для вывода или вовсе блокируют возможность забрать деньги.
* Фальшивые отзывы и поддельные рейтинги. Мошенники создают сайты и поддельные аккаунты, где якобы «успешные инвесторы» рассказывают, как они разбогатели.
* Агрессивное давление. «Вкладывай сейчас, пока не поздно!», «Только сегодня акция!» - если вас торопят, это явный признак мошенничества.
* Нет лицензии и прозрачной информации. Если у компании нет официальной регистрации, лицензий и четких данных о владельцах - бегите.

**Как защитить свои деньги?**

* Проверяйте компанию. Ищите лицензии, официальные документы, отзывы на независимых площадках.
* Не верьте обещаниям «золотых гор». Если доходность кажется слишком хорошей, чтобы быть правдой - это обман.
* Не принимайте поспешных решений. Мошенники давят на эмоции, но вы должны сохранять холодный разум.
* Советуйтесь с экспертами. Прежде чем инвестировать, проконсультируйтесь с независимым финансовым специалистом.
* Используйте только проверенные платформы. Доверяйте только известным и лицензированным инвестиционным компаниям.

❌ **Если вас просят внести деньги на неизвестную платформу - будьте осторожны! Не дайте себя обмануть!**



**Агрегатор мошеннических веб-ресурсов, аккаунтов в социальных сетях и мессенджерах**