

## ПАМЯТКА

Советы по определению Интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей



# КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ



### Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке



### Вам позвонили/прислали SMS «из банка» с неизвестного номера



- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы

### Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»



### Вы заподозрили интернет-продавца в недобросовестности



- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты

Информация НЦБ Интерпола МВД России  
о самых распространенных видах мошеннических действий с  
использованием компьютерных технологий.

Уважаемые граждане! Если Вы относитесь к активным пользователям  
Интернета, то рекомендуем Вам обязательно прочитать этот материал!

Мошенничество - это хищение чужого имущества или приобретение права  
на чужое имущество путём обмана или злоупотребления доверием.  
Подобная преступная деятельность преследуется законом независимо от  
места совершения - в реальной или виртуальной среде.

Мошенники постоянно изыскивают все новые и новые варианты хищения  
чужого имущества. Кратко остановимся на самых распространённых.

«Брачные мошенничества»

Типичный механизм: с использованием сети Интернет

преимущественно на сайтах знакомств преступники выбирают жертву,  
налаживают с ним электронную переписку от имени девушек, обещая  
приехать с целью создания в будущем семьи. Затем под различными  
предлогами «невесты» выманивают деньги (на лечение, покупку  
мобильного телефона, приобретение билетов, оплаты визы и т.д.).  
Переписка ведется главным образом студентами лингвистических ВУЗов.  
Направленные жертвами деньги преступники получают на подставных  
лиц. После получения средств переписка под различными предлогами  
прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

Мы настолько привыкли покупать в интернет-магазинах, что часто  
становимся невнимательными, чем и пользуются мошенники. Обычно  
схема мошенничества выглядит так: создаётся сайт-одностраничник, на  
котором выкладываются товары одного визуального признака. Цена на  
товары обычно весьма привлекательная, ниже среднерыночной.  
Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные  
данные. Чаще всего такие интернет-магазины работают по 100%  
предоплате. Переписка о приобретении товаров ведется с использованием  
электронных почтовых ящиков. По договоренности с продавцом деньги  
перечисляются, как правило, за границу через "Western Union" на имена  
различных людей. Конечно же, псевдо-продавец после получения денег  
исчезает!

«Крик о помощи»

Один из самых отвратительных способов хищения денежных средств. В  
интернете появляется душераздирающая история о борьбе маленького  
человека за жизнь. Время идёт на часы. Срочно необходимы дорогие  
лекарства, операция за границей и т.д. Просят оказать помощь всех  
неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

#### «Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространённым является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

#### «Нигерийские письма»

Один из самых распространённых видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взятки чиновникам и т.п.

#### «Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В распоряжении Бюро имеется информация о следующих недобросовестных брокерских компаниях: «MXTrade», «MMC1S» и «TeleTrade».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам-трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Вы можете передать SMS- или фото- или видеосообщения:

- В мессенджеры (WhatsApp, Telegram, Viber и др.)
- В социальные сети (Facebook, ВКонтакте, Одноклассники и др.)
- В электронную почту
- В облачные хранилища (Google Drive, Яндекс.Диск и др.)
- В приложения для обмена файлами (FileZilla, SFTP и др.)
- В приложения для обмена сообщениями (SMS, MMS, RCS и др.)
- В приложения для обмена фотографиями (Instagram, Facebook, VK и др.)
- В приложения для обмена видео (YouTube, Vimeo, Dailymotion и др.)
- В приложения для обмена документами (Dropbox, Google Drive, OneDrive и др.)
- В приложения для обмена аудио (SoundCloud, YouTube, SoundCloud и др.)
- В приложения для обмена файлами (FileZilla, SFTP и др.)
- В приложения для обмена сообщениями (SMS, MMS, RCS и др.)
- В приложения для обмена фотографиями (Instagram, Facebook, VK и др.)
- В приложения для обмена видео (YouTube, Vimeo, Dailymotion и др.)
- В приложения для обмена документами (Dropbox, Google Drive, OneDrive и др.)
- В приложения для обмена аудио (SoundCloud, YouTube, SoundCloud и др.)

Вы можете передать SMS- или фото- или видеосообщения:

- В мессенджеры (WhatsApp, Telegram, Viber и др.)
- В социальные сети (Facebook, ВКонтакте, Одноклассники и др.)
- В электронную почту
- В облачные хранилища (Google Drive, Яндекс.Диск и др.)
- В приложения для обмена файлами (FileZilla, SFTP и др.)
- В приложения для обмена сообщениями (SMS, MMS, RCS и др.)
- В приложения для обмена фотографиями (Instagram, Facebook, VK и др.)
- В приложения для обмена видео (YouTube, Vimeo, Dailymotion и др.)
- В приложения для обмена документами (Dropbox, Google Drive, OneDrive и др.)
- В приложения для обмена аудио (SoundCloud, YouTube, SoundCloud и др.)

Вы можете передать SMS- или фото- или видеосообщения:

- В мессенджеры (WhatsApp, Telegram, Viber и др.)
- В социальные сети (Facebook, ВКонтакте, Одноклассники и др.)
- В электронную почту
- В облачные хранилища (Google Drive, Яндекс.Диск и др.)
- В приложения для обмена файлами (FileZilla, SFTP и др.)
- В приложения для обмена сообщениями (SMS, MMS, RCS и др.)
- В приложения для обмена фотографиями (Instagram, Facebook, VK и др.)
- В приложения для обмена видео (YouTube, Vimeo, Dailymotion и др.)
- В приложения для обмена документами (Dropbox, Google Drive, OneDrive и др.)
- В приложения для обмена аудио (SoundCloud, YouTube, SoundCloud и др.)

