

# МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ



## Как действуют мошенники

Мошенники очень хорошо знают психологию людей и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении. В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

### Мошенники используют следующие мотивы:

- беспокойство за близких и знакомых;
- беспокойство за свой телефонный номер, счёт в банке или банковскую карту;
- желание выиграть крупный приз;
- любопытство – желание получить доступ к какой-либо информации;
- желание помочь больным детям или людям, пострадавшим от стихийных бедствий.

Социальные сети являются кладезем информации для мошенников. Размещая данные о себе на своих страничках, мы не задумываемся о том, кто может этим воспользоваться. Между тем именно благодаря нам самим мошенникам обычно не составляет труда узнать информацию о родственниках, контактах, увлечениях своей потенциальной жертвы и при выманивании денег внушить доверие знанием её личной жизни.

## 3.2. Виды интернет-мошенничества. Как защитить себя?

Наиболее распространенными видами мошенничества на данный момент являются:

### **Телефонное мошенничество**

Существуют наиболее распространённые схемы телефонного мошенничества. Вариантов того, как представят вам их мошенники, очень много, но суть не меняется.

**Обман по телефону.** С вас могут потребовать выкуп или взятку за освобождение якобы из отделения полиции или с места ДТП вашего родственника. Что делать: в этом случае главное не паниковать, позвонить самому родственнику, если не отвечает, то попытаться найти его через друзей и знакомых.

**СМС-просьба о помощи.** Требование перевести определённую сумму на указанный номер с использованием обращения «мама», «друг», «сын» и т.п. Что делать: не спешите переводить деньги, убедитесь, что в них действительно нуждается ваш родственник или знакомый.

**Телефонный номер-грабитель.** Платный номер, за звонок на который со счёта списывается денежная сумма. Что делать: не перезванивайте на неизвестные или предложенные в СМС-сообщениях номера телефонов.

**Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи.** Вас могут попросить оплатить пошлину, налог и т.п., перевести сумму на определённый счёт, сообщить пришедший на телефон код. Что делать: не спешите переводить деньги или сообщать какие-либо данные по телефону. Позвоните по официальным номерам (указанным в справочниках, на сайтах) компании – организатора лотереи или конкурса, убедитесь в том, что вас не обманывают.

**Штрафные санкции и угроза отключения номера** якобы за нарушение договора с оператором вашей мобильной связи. Что делать: позвоните сами своему оператору по официальному номеру, уточните информацию.

**Ошибочный перевод средств.** Вас попросят перевести якобы ошибочно переведённые средства, а затем дополнительно снимут деньги. Что делать: игнорируйте подобные сообщения или (если это телефонный разговор) посоветуйте для возврата ошибочно переведённой суммы обратиться к оператору связи.

### **Мошенничество с банковскими картами**

**Наиболее популярные способы мошенничества с банковскими картами:**

СМС-сообщение о блокировке банковской карты, о несанкционированном движении денежных средств, смене ПИН-кода, окончании срока действия карты и т.д. с требованием перейти по ссылке или перезвонить по указанному телефону.

Телефонный звонок «работника банка», потенциального «покупателя» с предложением пройти к ближайшему банкомату и совершить манипуляции с банковской картой во избежание каких-либо последствий, внесения аванса и т.п.

## **Для сохранности ваших средств соблюдайте основные правила безопасности:**

Никому не сообщайте свой ПИН-код, даже работникам банка. Не вводите ПИН-код при работе в сети Интернет, он может потребоваться только мошенникам.

СМС-сообщения по проводимым операциям по банковским картам рассылаются с определённых коротких номеров (Сбербанк – 900). Для связи с банком необходимо использовать официальные номера Контактного центра, указанные на банковской карте. Если в СМС-сообщении о блокировке карты, движении денежных средств указан другой номер, по которому предлагается позвонить, то это мошенники.

В случае возникновения проблем у банкомата, не принимайте помощь посторонних, позвоните в Контактный центр банка по телефону, указанному на банкомате.

Если к вам обратились по телефону, в Интернете, через социальные сети или другими способами и под различными предложениями пытаются узнать данные о вашей банковской карте (номер карты, трехзначный код на оборотной стороне карты), код, пришедший на ваш мобильный телефон, пароли или другую персональную информацию, будьте осторожны, это мошенники.

При телефонном общении не совершайте никаких действий у банкомата по инструкции «работников банка», если только данный звонок не был инициирован лично вами.

Не переходите по ссылкам в СМС-сообщениях.

При получении СМС-сообщений о снятии денежных средств с вашей банковской карты немедленно обращайтесь в банк, блокируйте карту.

### **Мошенничество в социальных сетях**

Мошенники активно пользуются социальными сетями и различными сервисами общения, например, сайтами знакомств.

### **Популярные способы мошенничества:**

**Распространение ссылок на вредоносное программное обеспечение, порнографические сайты, мошеннические ресурсы и приложения.** Пользователи социальных сетей часто сталкиваются со спамом, который приходит к ним в «личные сообщения» от имени «друзей» или незнакомых пользователей. Это означает, что аккаунты этих людей взломаны. *Как правило, ссылки в таких сообщениях сопровождаются завлекающим текстом, например: «Видела твои фото, я такого не ожидала, посмотри сам!..», «В этой базе данных есть вся информация на любого человека» и т.п.* Что делать: *никогда не переходите по подозрительным ссылкам. Для доступа в социальную сеть используйте уникальный пароль: он должен быть длинным, состоять из цифр и латинских букв. Лучше использовать разные пароли для разных социальных сетей и других интернет-сервисов. Не поддавайтесь на призыв кого-то из «администрации сайта» сообщить ваш логин и пароль под каким-либо предлогом. Регулярно меняйте пароль от социальной*

сети (хотя бы раз в месяц); остерегайтесь мошеннических сайтов с похожими по написанию названиями (vkontakte.ru, vk0ntalkte.ru и т.д.). Эти «фишинговые» страницы рассчитаны на невнимательность и на то, что вы сами предоставите мошенникам свой логин и пароль.

□ **Знакомые незнакомцы.** В социальных сетях и на сайтах знакомств мошенники создают страницы, где указываются данные и размещаются фотографии вымышленных людей. С помощью этих страниц они знакомятся с другими пользователями сайта. Со временем мошенники входят в доверие, предлагают перейти собеседнику на более «близкое» общение и оставляют свой номер телефона. Самым безобидным последствием такого общения будет то, что номер окажется платным и с вашего счёта спишутся деньги.

□ **Просьбы о финансовой помощи, благотворительные акции.** Мошенники часто используют такие поводы, поэтому, прежде чем перевести деньги для помощи, убедитесь, что вас не обманывают. Обратите внимание на наличие нескольких контактов (телефоны, электронная почта, странички в социальных сетях), наличие подтверждающих документов.

### **Мошенничество на сайтах бесплатных объявлений**

Размещая объявления, или покупая что-либо на сайтах бесплатных объявлений (например, «Авито»), будьте внимательны и осторожны, так как мошенники очень часто используют их для обмана. Продавая что-то, вы желаете получить прибыль, но, столкнувшись с мошенниками, можете потерять все свои сбережения.

#### **Как вас могут обмануть:**

**Оплата или предоплата за ваш товар.** Очень часто заинтересованные покупатели предлагают произвести оплату (если сумма незначительная) или предоплату за ваш товар, но сделать это могут по каким-либо причинам только на банковскую карту (находятся в другом городе, нет наличных денег, деньги на расчётном счёту и т.п.), но при этом требуют сообщить не только номер карты и ФИО (больше для перевода ничего не требуется), но и другие данные. Помните, что если вас просят сообщить пришедший на телефон код, пройти к банкомату и совершить какие-то действия, вставив вашу карту (чтобы, например, подтвердить прохождение платежа), сообщить срок действия карты и трёхзначный код на оборотной стороне, то это мошенники. Прекращайте контакты с такими «покупателями» и, если успели сообщить какие-то данные, немедленно блокируйте банковскую карту, позвонив по указанному на ней номеру телефона.

**Предоплата за покупаемый товар.** Покупая что-либо, будьте осторожны, если вас просят произвести предоплату. Вполне возможно, что получив её, «продавец» перестанет отвечать на ваши звонки.

**СМС-сообщения со ссылкой.** На номер, который вы указали при публикации объявления о продаже или желании что-либо купить, может прийти СМС-сообщение с предложением товара, обмена и ссылкой на этот товар. Если вы перейдёте по ссылке, то загрузите на свой телефон вредоносное

программное обеспечение, которое позволит мошенникам получить доступ к вашим банковским картам.

**Будьте осторожны, если вам предлагают:**

- назвать номер банковской карты, трёхзначный код на оборотной стороне карты, ПИН-код;
- произвести манипуляции с банковской картой у банкомата;
- сообщить пришедший на телефон код;
- перевести сумму денег (аванс, залог, пошлина, налог, ошибочно переведённый платеж и т.п.);
- перейти по ссылке в Интернете, в СМС- или ММС-сообщении на смартфоне;
- позвонить по указанному в СМС-сообщении номеру телефона;
- отправить ваш номер телефона;
- отправить СМС-сообщение на короткий номер;
- назвать пароли от ваших личных страничек в социальных сетях.

**1. Советы по безопасности работе в общедоступных сетях Wi-fi:**

- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
  - Используйте и обновляйте антивирусные программы и брандмауер. Тем самым Вы обезопасите себя от закачки вируса на устройство;
  - При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
  - Не используйте публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
  - Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
  - В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без Вашего согласия.

**2. Основные советы по безопасности в социальных сетях:**

- Ограничьте список друзей. У Вас в друзьях не должно быть случайных и незнакомых людей;
  - Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как Вы и Ваши родители планируете провести досуг;
  - Если Вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

- Избегайте размещения фотографий в Интернете, где Вы изображены на местности, по которой можно определить Ваше местоположение;

- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если Вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

### ***3. Основные советы по безопасной работе с электронными деньгами:***

- Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;

- Используйте одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;

- Выберите сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;;

- Не вводите свои личные данные на сайтах, которым не доверяете.

### ***4. Основные советы по безопасной работе с электронной почтой:***

- Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаете и кто первый в рейтинге;

- Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;

- Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

- Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

- Если есть возможность написать самому свой личный вопрос, используйте эту возможность;

- Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым Вы доверяете. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

- Не открывайте файлы и другие вложения в письмах даже если они пришли от Ваших друзей. Лучше уточните у них, отправляли ли они Вам эти файлы;

- После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

### **5. Основные советы по борьбе с фишингом (интернет-мошенничества):**

- Следите за своим аккаунтом. Если ты подозреваешь, что Ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используйте сложные и разные пароли. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному Вашему профилю в сети, а не ко всем;
- Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у Вас в друзьях, о том, что Вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установите надежный пароль (PIN) на мобильный телефон;
- Отключите сохранение пароля в браузере;

### **6. Основные советы по защите цифровой репутации (негативная или позитивная информация в сети о Вас):**

- Подумайте, прежде чем что-то публиковать и передавать у Вас в блоге или в социальной сети;
- В настройках профиля установите ограничения на просмотр Вашего профиля и его содержимого, сделайте его только «для друзей»;
- Не размещайте и не указывайте информацию, которая может кого-либо оскорблять или обижать.

### **Соблюдайте правила:**

- Помните, что в виртуальном пространстве ответственность наступает по реальным законам;
- Уважительно и добросовестно относитесь к другим пользователям сети Интернет.