**Боты : в чём опасность и как защититься**

Злоумышленники запускают программы-роботы, чтобы собрать конфиденциальную информацию о пользователях для махинаций. Разберем самые популярные схемы мошенничества и расскажем, как защитить личные данные в Сети.

**Собирают публикации**

В Сети пользователи оставляют много следов: фамилию и имя, дату рождения, имена близких родственников, образование, место работы, личные фото. Эту информацию легко найти и систематизировать. Покажу на примере собственной фотографии, которую часто использую для аватарок.

Эту информацию мошенники могут использовать в преступных целях.

Однако собирать сведения о пользователях — работа трудоемкая. Для ускорения процесса мошенники подключают ботов. Они собирают, анализируют и систематизируют информацию, создавая базу данных.

**Как защититься.**Не загружать в интернет личные фото или ограничить их просмотр. Можно использовать в Сети псевдоним и стоковые фото для аватаров.

**Воруют базы данных**

Базы данных крупных порталов — лакомый кусочек для мошенников. Они могут получить ФИО пользователей, домашние адреса, номера телефонов и автомобилей, банк обслуживания.

Порталы надежно защищают базы данных. Чтобы обойти защиту, мошенники объединяют ботов в сеть — ботнеты. С их помощью они совершают хакерские атаки на сервисы и воруют информацию о пользователях.

***Для справики.*** *По данным [Роскомнадзора](https://www.kommersant.ru/doc/5504156?tg" \t "_blank), в 2022 году более 40 крупных баз попали в открытый доступ и больше 300 млн личных данных было скомпрометировано. От рук мошенников пострадали базы данных «СДЭКа», «Яндекс.Еды», «Вайлдберриз», «Ростелекома», ГИБДД.*

После взлома хакеры продают информацию в «теневом интернете» или используют для собственного обогащения. Например, звонят от имени службы безопасности банка и склоняют абонентов перевести им деньги.

**Как защититься.**Защититься можно уже по факту взлома данных.

* Обратитесь в полицию и напишите заявление, что данные паспорта украдены. Если вскроются махинации мошенников, вы сможете подтвердить свою непричастность.
* Через бюро кредитных историй (БКИ) проверьте, не оформлены ли на вас левые кредиты. Сведения можно запросить [через «Госуслуги»](https://www.gosuslugi.ru/600311/1/form?_=1669637041275) — два раза в год их можно получить бесплатно.
* В [личном кабинете налогоплательщика](https://lkfl2.nalog.ru/lkfl/login) проверьте, не зарегистрирована ли на вас юридическая организация. Если обнаружите сведения, подайте в ФНМ заявление об ошибке.
* Запросите в МФЦ справку о лицах, которые интересовались вашей недвижимостью. Дополнительно можете подать в МФЦ заявление о запрете регистрации сделок без вашего участия.

**Распространяют информацию**

В Telegram роботы продают личные сведения. Например, чат-бот «Глаз бога» работает в Сети несколько лет. Роспотребнадзор регулярно блокирует подобные чаты, но владельцы находят способы обойти запрет.

**Как защититься.**Сложно сказать, сколько компаний используют персональные данные без вашего согласия. Но вы можете пожаловаться на ресурс, который незаконно распространяет сведения. Жалобу подавайте в [Роскомнадзор](https://petition.rospotrebnadzor.ru/petition/oper_msg_create/" \t "_blank).

**Рассылают вредоносные ссылки**

Ботов маскируют под личность или организацию. Например, на почту пользователя приходит письмо якобы из ФНС. Лженалоговики уведомляют о задолженности и просят проверить информацию. Для этого пользователю предлагают перейти по ссылке. Иногда в сообщении просят установить на компьютер или смартфон приложение.

В действительности по ссылке находится вредоносная программа. С ее помощью мошенники пытаются проникнуть на ваше устройство и получить доступ, например, к мобильному банку.

**Как защититься.**Нужно соблюдать несколько правил:

* не переходить по ссылкам из писем, которые вызывают сомнения;
* не загружать на компьютер программы и приложения по рекомендациям от незнакомцев.

**Собирают базы данных**

Иногда сервисы запускают бота с коммерческими целями, например, определить целевую аудиторию, собрать базу потенциальных клиентов, предложить услугу.

Например, бот юридической компании подсказывает, как законно списать долги. Пользователь выполняет несложные задания или отвечает на вопросы. В конце бот присылает перечень рекомендаций или предложение позвонить сотруднику.

Такие боты работают с соблюдением закона, и на одном из шагов пользователь соглашается с обработкой и хранением персональных данных. Но небольшим компаниям сложно обеспечить надежную защиту, риск взлома робота очень велик.

**Как защититься.**Остановите бота, если вас просят ввести номер телефона или адрес почты. Помнить, что любые данные могут получить злоумышленники.

**Предлагают легкий заработок**

Бот обещает заработать. Опыт и знания обычно не нужны. Например, предлагает сортировать или лайкать фотографии. Пользователи получают за работу виртуальные деньги, которую можно вывести на карту или электронный кошелек.

Как правило, на вывод устанавливают минимальный лимит. Например, на личном счете должно накопиться более 500 ₽. Когда минимальная сумма накоплена, мошенники выдвигают новые условия: разослать реферальные ссылки, помочь проекту или защититься от злоумышленников. Любая из перечисленных услуг платная — нужно заплатить символическую сумму в 100-150 ₽.

Если пользователь заработал минимальные 500 ₽, ему кажется, что он все равно в выигрыше. Он переводит реальные деньги мошенникам, но не может вывести виртуальную валюту — транзакция не проходит.

**Как защититься.**Не доверять обещаниям быстро и легко заработать. И никогда не перечислять деньги лжеработодателям. Если вас просят оплатить допуслугу, рабочие материалы или внести страховочный платеж, откажитесь от сотрудничества.

**Предлагают рекламу**

Роботы рассылают предложения о рекламе. Сообщение выглядит безобидно, но вирус может скрываться в тексте документа, например, в предварительном договоре о сотрудничестве.

Вредоносная программа запускается при открытии файла. Она ворует связки логин-пароль, данные куки-файлов, скрины веб-камер и экранов, информацию, которую пользователь набирает на клавиатуре.

Мошенники получают доступ к каналу и от имени компании ведут спам-рассылку, запускают сбор денег или предлагают владельцу за деньги вернуть контроль над корпоративным ресурсом.

**Как защититься.**

* Скептически отнеситесь к внезапным предложениям, особенно заманчиво дешевым. Перепроверьте источник, соберите на него информацию и отзывы.
* Не переходите по ссылкам на сторонние ресурсы — лучше перейдите на сайт через поисковик.
* Проверяйте контакты и реквизиты потенциального партнера.
* Не храните пароли в телефоне или компьютере.