

Доксинг атакует: как защитить себя и свои личные данные

В Казахстане активно развивается цифровая среда: растет количество онлайн-сервисов, госуслуг и мобильных приложений. Но вместе с этим увеличивается и число случаев доксинга — целенаправленного сбора, публикации или распространения личных данных без согласия человека.

Как злоумышленники получают доступ к личным данным

К сожалению, в современном мире, где мы регистрируемся в соцсетях, маркетплейсах, приложениях, более-менее подготовленным мошенникам достаточно легко получить наши данные. Как именно они это делают, расскажем дальше.

1. Поисковые системы — с их помощью можно обнаружить старые записи, комментарии, упоминания на форумах, а расширенные функции позволяют искать по конкретным сайтам или типам файлов. Дополнительную уязвимость создает привычка людей использовать один и тот же никнейм на разных платформах: это облегчает сбор данных о пользователе сразу из нескольких публичных ресурсов.

2. Социальные сети — открытый профиль фактически превращается в готовое досье с именем, местом работы, городом, фотографиями и кругом общения. Но даже если страница закрыта, доксер может собрать информацию через комментарии под чужими постами, участие в сообществах, публикации друзей. Нередко они просто добавляются в друзья под видом рекрутера или сотрудника компании, чтобы получить доступ к дополнительным данным.

3. Социальная инженерия — злоумышленники могут писать человеку от имени банкира, врача или сотрудника организации, стараясь выведать личные данные напрямую. Многие пользователи не распознают обман и сами передают информацию.

4. Рабочие отношения — если руководитель размещает на сайте или в соцсетях список сотрудников вместе с фотографиями, этим тоже охотно пользуются доксеры. Даже, по скудным сведениям, вроде бы сугубо профессиональным, можно выяснить город проживания и затем найти профиль человека в соцсетях. Коммерческая деятельность также оставляет след — во многих странах данные учредителей компаний доступны открыто.

5. Черный рынок — в даркнете продают утекшие базы госорганов и компаний, в которых можно найти все от сканов паспортов до данных банковских приложений. Стоят такие сведения относительно недорого, а их наличие сильно облегчает доксинг.

Брокеры данных тоже могут неосознанно стать добычей для преступников, потому что такие компании легально собирают и систематизируют персональную информацию из множества источников и продают ее бизнесу. Хотя эти данные и не предназначены для посторонних, они нередко оказываются в руках злоумышленников и могут существенно упростить сбор сведений о человеке.

Что делать, если ваши данные опубликовали?

Фиксируйте факты доксинга: собирайте электронные письма, голосовые сообщения, SMS, делайте скриншоты публикаций или комментариев в соцсетях. Это может потребоваться для обращения в полицию, при досудебной претензии и так далее.

Требуйте удаления контента: если человек или организация распространили ваши личные данные, они нередко сопровождают это ложной или вводящей в заблуждение информацией. Вы можете обратиться непосредственно на платформы или сайты, где опубликованы данные, с требованием удалить материал или исправить его.

Обязательно сообщайте о доксинге в правоохранительные органы, особенно если он сопровождается шантажом или вымогательствами.

Проконсультируйтесь с юристом: он поможет оценить перспективы и возможные риски, а также расскажет, как вы можете защитить себя с точки зрения законодательства Казахстана.

Защитите свою приватность: сократите до минимума личную информацию везде, где только можете — соцсетях, рабочих аккаунтах и сайтах, маркетплейсах и так далее.

Что говорит законодательство Казахстана о доксинге

Конечно, если вы столкнулись с доксингом, лучше сразу обратиться в полицию и к юристам, но мы вкратце расскажем, что говорят законы Казахстана об этом преступлении и ждет злоумышленников.

Статья 18 Конституции РК гарантирует каждому казахстанцу право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства, тайну личных владений и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Таким образом, доксинг является прямым нарушением Конституции.

Далее, если доксер занимается вымогательством, то это *194 статья Уголовного кодекса, которая грозит преступнику ограничением или лишением свободы на срок до четырех лет. При отягчающих обстоятельствах срок может увеличиться вплоть до 15 лет.*

Не забываем также о *статье 147 Уголовного кодекса - «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите».* Незаконный сбор сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия наказывается ограничением или лишением свободы **на срок до трех лет.**

Если преступник распространил сведения о частной жизни лица без его согласия или причинил своими действиями существенный вред правам и законным интересам пострадавшему, то его могут приговорить к лишению свободы на срок **от трех до шести лет.** А если распространил с использованием интернета, то наказание может увеличиться **до семи лет.**

Как защититься от доксинга?

1. **Минимизируйте свой цифровой след:** проверьте соцсети, удалите старые посты, уберите из открытого доступа телефон, адрес, учебное заведение, место работы, данные детей.

2. **Используйте разные пароли:** с одним паролем вы рискуете потерять данные или пострадать на всех аккаунтах. Вам могут помочь менеджеры паролей типа Bitwarden, 1Password, Google Password Manager.

3. **Включите двухфакторную аутентификацию:** сделайте это везде, где только возможно — в WhatsApp, Instagram, Telegram, Google, eGov, Kасpi.

4. **Ограничьте видимость профиля:** закройте списки друзей, отметки на фото, геолокацию, дату рождения, активность. Сделайте соцсети максимально приватными.

5. **Не используйте везде один и тот же никнейм:** одинаковый ник позволяет собрать на вас досье с десятков сайтов. Лучше иметь разные варианты для разных платформ.

6. **Никогда не отправляйте документы в мессенджерах незнакомцам:** не пересылайте удостоверение, ИИН, ЭЦП, банковские реквизиты, билеты, справки — это прямой путь к доксингу и оформлению кредитов.

7. **Проверьте свои устройства на доступы:** удалите старые приложения, разрешения на камеру/микрофон, доступы к контактам, галерее, документам.

8. **Очистите открытые источники:** удалите свои данные с сервисов объявлений, старых форумов, профильных сайтов. Для дополнительной безопасности проверьте себя в поисковиках по имени, номеру телефона и фото.

9. Будьте осторожны с файлами и ссылками: не скачивайте файлы APK, не открывайте незнакомые ссылки «по работе», «от школы», «от банка». Социальная инженерия — главный инструмент доксеров.

10. Разделяйте контакты и используйте «защитный» номер телефона: идеальным будет иметь отдельный номер для соцсетей, регистрации на сайтах, покупок и служб доставки. Основной номер должен быть известен только близким людям — это снижает риск доксинга, спама, угроз и взломов.