

Отличаются ли в 2026 году схемы кибермошенничества?

Схемы кибермошенничества в 2026 году продолжают эволюционировать и становятся более сложными. Мошенники регулярно разрабатывают новые способы обмана граждан, в том числе комбинированные многоходовые сценарии.

Так, распространённой схемой является последовательное использование нескольких инструментов: сначала потенциальная жертва получает фишинговое письмо, которое ведёт на поддельный сайт; после ввода персональных данных пользователю поступает звонок от лица, представляющегося сотрудником организации, с предложением установить программное обеспечение «для защиты». В действительности такое ПО является вредоносным.

Существенное влияние на трансформацию мошеннических схем оказывает массовое применение технологий искусственного интеллекта. В частности, злоумышленники используют ИИ для создания дипфейков — голосовых и видеоподделок. Это позволяет им имитировать общение с родственниками или знакомыми жертвы, вводя её в заблуждение.

Согласно данным компании «Позитив Технолоджис», в 2026 году зафиксированы случаи деятельности гибридных групп хакеров, сочетающих политическую риторику с тактиками вымогательства. Такие группы осуществляют шифрование и хищение данных с последующим требованием выкупа за их восстановление либо за неразглашение.

Возможные новые схемы кибермошенничества в летний период

В летний сезон мошенники адаптируют свои схемы с учётом специфики поведения отдельных категорий граждан — отпускников, дачников, лиц, активно использующих услуги досуга.

Для туристов и лиц, планирующих отпуск, характерны следующие виды мошенничества:

- поддельные сайты бронирования, имитирующие официальные платформы продажи авиабилетов и бронирования отелей, с намеренно заниженными ценами для привлечения внимания;

- предложения о приобретении билетов или туров через ботов в мессенджерах с оплатой на карту физического лица — такой способ оплаты является признаком мошеннической схемы.

Среди дачников распространены рассылки от имени председателя садоводческого некоммерческого товарищества (СНТ) с требованием произвести оплату «целевого взноса» (например, на ремонт дорог, линий электропередачи или водопровода) по поддельным реквизитам.

Любители досуга сталкиваются со следующими видами обмана:

- фейковые страницы по продаже билетов на концерты, мастер-классы, экскурсии;
- рассылки, имитирующие сообщения о выигрыше скидок или иных привилегий, которые ведут на вредоносные ресурсы.

Наиболее распространённые приёмы кибермошенников летом 2026 года

Среди наиболее популярных приёмов, используемых мошенниками в летний период, можно выделить:

- **Дипфейки.** Применяются для вымогательства денежных средств или получения доступа к персональным данным. В летний период их эффективность возрастает, поскольку граждане чаще используют видеосвязь и могут менее критично относиться к срочным обращениям.
- **Квишинг** (использование QR-кодов для доставки фишингового содержимого). Злоумышленники размещают поддельные QR-коды на самокатах, в объявлениях, на объектах в парках и на остановках. Сканирование таких кодов может привести к переходу на фишинговый сайт либо к загрузке вредоносного программного обеспечения.
- **Фишинговые ссылки в СМС-сообщениях и мессенджерах.** Часто используются темы, связанные с подтверждением брони, акциями на туристические услуги, возвратом налога за отдых. Подобные схемы особенно актуальны в периоды активного онлайн-бронирования.
- **Фейковые мобильные приложения,** маскирующиеся под официальные программы туроператоров и иных поставщиков услуг.

Рекомендации по защите от кибермошенничества в летний период

Для минимизации рисков стать жертвой кибермошенников рекомендуется соблюдать следующие правила:

- Не переходить по ссылкам, полученным из непроверенных источников. Даже если сообщение поступило с адреса, который кажется надёжным (например, от банка или авиакомпании), не следует доверять ему автоматически. Для доступа к

сервисам рекомендуется вручную открывать официальные сайты или использовать официальные мобильные приложения.

- Воздержаться от сканирования QR-кодов в общественных местах (на улице, в транспорте, на объявлениях). Такие коды могут содержать ссылки на фишинговые страницы либо инструменты для распространения вредоносного ПО.
- Использовать менеджер паролей и включать двухфакторную аутентификацию во всех сервисах, где осуществляется доступ к финансовым или персональным данным. Рекомендуется применять уникальные пароли для разных сервисов, чтобы исключить риск компрометации нескольких учётных записей при взломе одной из них.
- При бронировании услуг и совершении онлайн-покупок тщательно проверять домен сайта: обращать внимание на возможные опечатки в адресе, наличие протокола HTTPS, а также на присутствие контактной информации и реквизитов организации.
- Осуществлять оплату исключительно через защищённые платёжные шлюзы. Не следует переводить денежные средства на карты физических лиц, даже если собеседник обещает скидку за прямой перевод.
- После совершения оплаты рекомендуется подтверждать бронь напрямую через официальный канал связи с поставщиком услуги (отелем, авиакомпанией и т. п.).
- Учитывать, что банки и государственные органы никогда не запрашивают коды из СМС-сообщений, пароли или ПИН-коды. Любые подобные запросы следует расценивать как попытку мошенничества.
- В случае получения срочного обращения от лица, которое представляется родственником или знакомым (особенно если речь идёт о необходимости перевода денежных средств), рекомендуется самостоятельно связаться с этим человеком по проверенному каналу связи для подтверждения подлинности обращения.