ТЕМА 13 / 15

# Кибербезопасность

Кибербезопасность, или компьютерная безопасность – это комплекс мер, направленный на защиту информации пользователей электронных устройств. В широком смысле это отдельная отрасль IT, занимающаяся защитой данных от различных угроз.
В области борьбы с мошенниками кибербезопасность – это правила поведения при обращении с электронными устройствами (компьютерами, смартфонами, мобильными телефонами, банкоматами). Их соблюдение обеспечивает защиту данных – паролей, личных документов, бухгалтерской отчетности и так далее.

## Главные опасности для пользователя в Интернете

### Фишинг

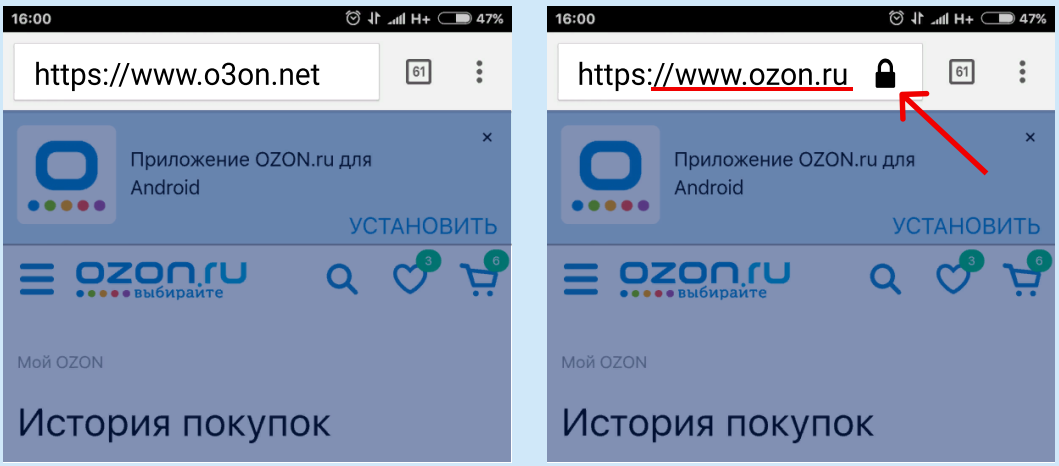
Фишинг – это выманивание у пользователя персональных данных. В Интернете наиболее распространены две формы этого мошенничества:

- кража логина и пароля к почтовым ящикам или соцсетям под видом регистрации для участия в конкурсе, голосовании, подписании петиции и т.д.
- кража данных карты (номер, дата выпуска, код с обратной стороны, одноразовый SMS-код) под видом оплаты товара или услуги, перевода, пожертвования и так далее

**Ссылки на фишинговые сайты мошенники присылают:**

- по электронной почте
- через мессенджеры
- в чатах соцсетей

Фишинговые сайты, как правило, выглядят как **точные копии сайтов реально существующих** компаний, пользующихся доверием. Отличить их можно по адресу: мошенники используют сочетания букв, похожие на реальный URL, но отличающиеся от него хотя бы на один знак.




**Второй признак** – защищенность соединения. Она отображается значком закрытого замка (как на рисунке).

## Публичный WiFi

Публичный WiFi – идеальная среда для проведения атаки Man-in-the-Middle («человек посередине»). Это перехват передаваемых данных.
Все, происходящее на экране смартфона, когда пользователь заходит в Интернет – это обмен данными между устройством и компьютером, где расположен сайт – сервером. Данные, которыми обмениваются два устройства, можно перехватить, расшифровать и использовать.

Технически это возможно всегда, вопрос только в том, насколько это сложно и затратно. Но если пользователь и преступник находятся в одной сети WiFi, злоумышленнику достаточно самых простых методов и недорогого оборудования, чтобы получить пароли к личным страницам и платежным данным пользователей или даже внедрить на их устройства вредоносную программу.

## Вредоносные программы

Киберпреступники часто используют программы-паразиты (вирусы, трояны и другие), которые заставляют компьютер пользователя делать то, что нужно злоумышленнику. Для установки такой программы бывает достаточно зайти на зараженный сайт. Вот самые распространенные задачи, которые выполняют вредоносные программы:

- удаление установленных программ или изменение их работы
- считывание данных и передача их разработчику
- кража персональных данных пользователя, в том числе данных банковских карт и одноразовых SMS-кодов на постоянной основе
- перехват управления устройством
- создание условий для вымогательства, например, шифрование всех файлов на жестком диске и продажа ключа к шифру за крупную сумму
- включение устройства в сети, атакующие другие компьютеры, без ведома пользователя
- майнинг криптовалюты (вред в повышенной нагрузке на процессор и падении производительности)

# Как защититься?

| Что делать? | Зачем делать? |
|---|---|
| Завести сложные пароли – свой для каждого ресурса | Простые пароли мошенники могут подобрать. Если у, например, почты и соцсетей один пароль, то, взломав один ресурс пользователя, преступники получат доступ ко всем. |
| Установить антивирус | Защиты встроенных антивирусных программ зачастую недостаточно. Нужно выбирать продукт от серьезных разработчиков, которые часто обновляют антивирусные базы. Это поможет отбить атаку на этапе скачивания зловредной программы, ее установки или начала работы. |
| Использование браузеров с антифишинговой защитой (Mozilla Firefox, Google Chrome, Opera, Safari) | Браузер сверяет введенный адрес сайта с базами данных фишинговых сайтов. Если сайт обнаружится в базе, браузер покажет предупреждение. **НО!** Если сайт новый и в базах его еще нет, предупреждения не будет. Поэтому такая защита – только вспомогательный инструмент. Главный – внимание пользователя. |
| Не использовать общественные или корпоративные WiFi-сети | Подобные сети значительно облегчают мошенникам перехват ваших данных. В публичных местах нужно использовать доступ к интернету через мобильного оператора. |
| Регулярно обновлять операционные системы компьютера и смартфона | В новых версиях систем разработчики закрывают обнаруженные уязвимости – окошки, через которые преступники могут вмешиваться в работу устройств. |