GeekBrains

Базовая безопасность при работе с компьютером

Компьютерная грамотность

Оглавление

Вступление

План урока

Пароли для входа

- Как придумать надёжный пароль?
- Как запомнить пароль?
- Где хранить пароли?

Вирусы и антивирусы

Меры предосторожности в сети

Как определить, что компьютер заражён?

Антивирусные программы

VPN

- Какой VPN выбрать?
- Итоги

[00.00.05]

Вступление

Здравствуйте! Меня зовут Елена Бредова, я работаю в IT-сфере с 1999 года и прошла длинный путь от HTML-кодера до владельца студии.

Сегодня мы погрузимся в важную тему — базовую безопасность при работе с компьютером.

[00.00.36]

План урока

На занятии поговорим про:

- пароли — какими они должны быть, как их хранить и использовать;
- вирусы и антивирусы;
- VPN — что это, и зачем нужно.

[00.01.02]

Пароли для входа

Представьте ситуацию: аккаунт Ольги в «Одноклассниках» взломали, весь урожай из «Фермы» собрали и вывезли, а друзьям поставили единицы. Теперь на встрече одноклассников Ольге не рады. История смешная, но показательная: мошенничество преследует нас не только в обычной офлайн-жизни, но и онлайн. Нужно быть внимательными, чтобы не потерять личные данные, деньги, репутацию и даже технику.

Разговор о базовой безопасности начнём с паролей. Они должны быть сложными: из букв (заглавных и строчных), цифр и спецсимволов (#, $, & и так далее). Длина ещё важнее сложности: пароль из 7 символов компьютер подберёт за несколько часов, а пароль из 10 символов — за несколько лет. Поэтому минимальная длина пароля — 8 символов, но чем больше, тем лучше.

Не используйте в качестве пароля личные данные (например, дату рождения, номер СНИЛС или фамилию). Такие пароли легко запомнить, но они уязвимы, их можно быстро раскрыть с помощью некоторых баз.

Для каждого сайта создавайте отдельный пароль. Иногда базы с личными данными на разных сервисах попадают в открытый доступ — среди них могут быть и пароли. Если ваш общий пароль для разных сайтов станет известен, вы можете потерять доступ ко всем из них.

[00.04.50]

Как придумать надёжный пароль?

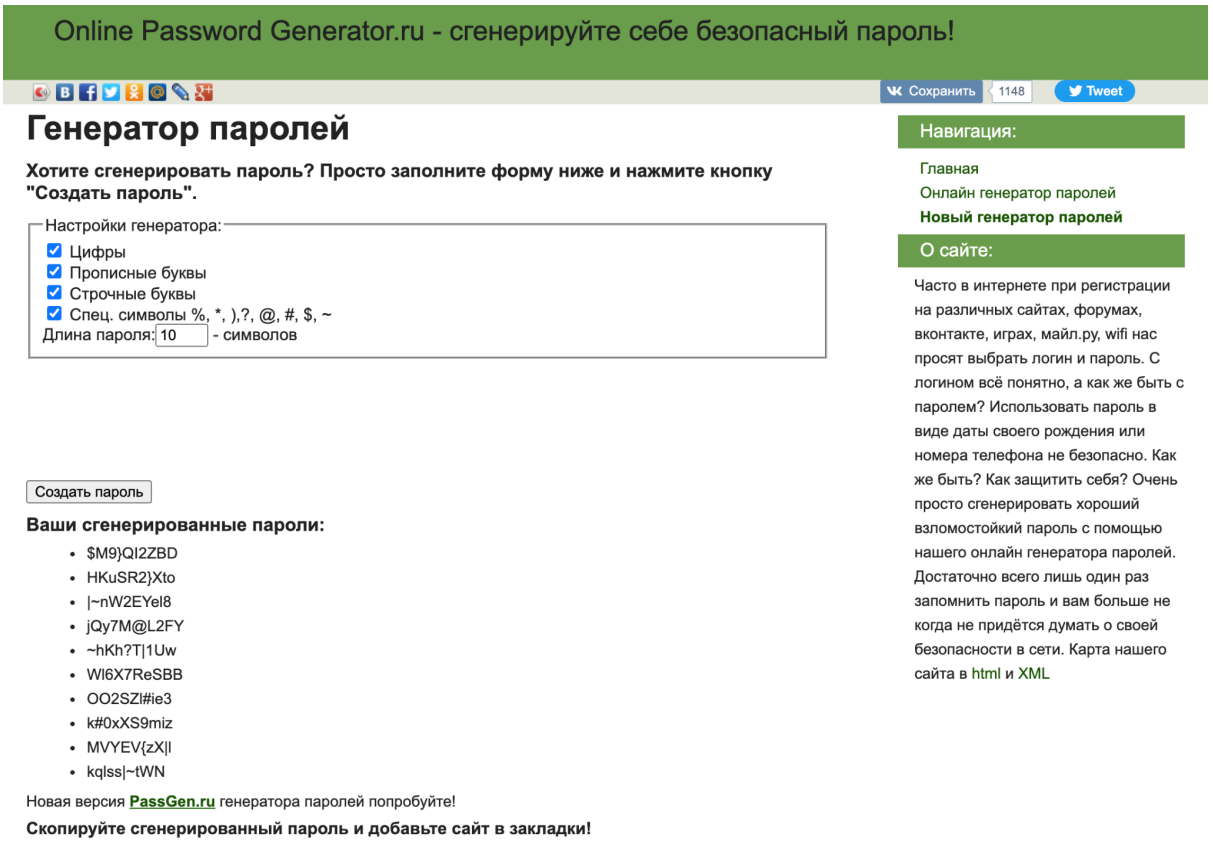
Есть лайфхак — можно взять стихотворение, которое вы помните наизусть, или запомнившуюся фразу и зашифровать их: заменить буквы на понятные символы.

Я помню чудное мгновенье → I_p0Mny|_4ydn0e_Mg№0veniE

Фраза остаётся читаемой, и запомнить такой пароль легко.

Другой способ придумывать надёжные пароли — сервис для их генерации. Таких программ в интернете много, вы можете выбрать ту, которая вас устраивает.

Для примера я взяла сервис Online Password Generator. Здесь можно выбрать, символы, которые мы хотим видеть в пароле: цифры, прописные и строчные буквы, спецсимволы. А также задать его длину — например, 10 символов. Когда заполнили данные, нажимаем кнопку «Создать пароль» и получаем целый список сгенерированных вариантов.



Всё достаточно просто и не приходится ломать голову над тем, как сделать пароль сложным.

[00.07.00]

Как запомнить пароль?

Мы уже обговорили, что пароли должны быть разными для разных сайтов. Как же запомнить, где какой используется? Можно создать сложный пароль и добавить к нему зашифрованное название ресурса. Например, взять первые буквы названия сайта: Ya для Yandex и так далее. Шифр с названием сервиса можно добавить к основному паролю через спецсимвол, точку, тире — как удобнее.

Чтобы не запутаться в паролях, нужно определиться с порядком цифр и букв, с их размером (когда заглавные, а когда строчные). То есть нужно придумать систему шифрования и никому о ней не рассказывать.

[00.08.41]

Где хранить пароли?

Если паролей много, и они сложные, хранить их в голове не получится — можно забыть. Есть два других варианта:

1. **Записать в блокноте** — не самый безопасный вариант, если блокнот хранится на видном месте. Придётся убирать его в закрытый ящик или сейф, чтобы защитить от посторонних.
2. **Менеджер паролей** — это программа для хранения паролей. Доступ к ним можно получить только введя мастер-пароль — пароль от всех паролей.

Менеджеров паролей много, один из самых популярных — Kaspersky Password Manager. Но есть и другие программы. Выберите удобный для вас инструмент, но лучше избегайте зарубежных сервисов и менеджеров паролей в браузерах.

Ещё одна рекомендация — уберите автозаполнение форм (когда браузер запоминает информацию и подставляет её), чтобы ваши данные не хранились в браузере.

Выводы:

- Не храните информацию о паролях и логинах на зарубежных сайтах.
- Не храните пароли на бумаге. Или убирайте блокнот с паролями в надёжное место.
- Отключите автозаполнение форм.
- Проверьте параметры восстановления пароля. Например, если вашу почту взломают, у вас должна быть возможность восстановить пароль с помощью мобильного или резервной почты. Иначе доступ можно потерять безвозвратно.
- Используйте двухфакторную авторизацию, то есть двойную систему защиты: сперва вводите пароль, затем код подтверждения, который приходит на телефон, указанный при регистрации. С двухфакторной авторизацией взломать аккаунт гораздо сложнее.
- Регулярно менять пароли. В мире всё ненадёжно: базы вскрываются, серверы сливают информацию, происходят утечки данных. Следите за информацией в СМИ, чтобы вовремя узнать об утечке данных, и раз в 3 месяца меняйте пароли. Чтобы не запутаться, в пароле можно зашифровать дату смены по принципу названий сайтов.

[00.15.15]

Вирусы и антивирусы

Вирусы не попадают на смартфоны или компьютеры воздушно-капельным путём. Любой вирус запускает сам пользователь. Например, когда загружает бесплатную программу вместе с вирусом, использует заражённую флешку или переходит по ссылке из письма со спамом. Windows особенно подвержен атакам, поэтому будьте внимательны. Чтобы обезопасить свой

компьютер, не открывайте письма от неизвестных отправителей, не скачивайте из них файлы и не переходите по ссылкам.

Иногда мошенники маскируются под известные сайты: например, приходит письмо от reg.ru о том, что нужно продлить доменное имя. Письмо выглядит так же, как и другие, которые присылала компания. Но ссылка ведёт не на страницу оплаты домена, а на пополнение электронного кошелька мошенников.

Перепроверяйте информацию, прежде чем совершить какое-нибудь действие.

[00.17.44]

Меры предосторожности в сети

Залог безопасного исследования сети — сочетание здравого смысла и программы-антивируса.

Не передавайте свои персональные данные незнакомым. Иногда мошенники запрашивают сканы документов, а потом продают их или используют против пользователей. Проверяйте, от кого приходит просьба предоставить персональную информацию. Если есть возможность, позвоните или напишите официальной службе поддержки сервиса или сайта.

Внимательно относитесь к ссылкам и игнорируйте спам. Если вам пришло письмо об умершем в Африке дядюшке, который оставил вам наследство, это мошенническая схема. Будьте внимательны.

[00.19.37]

Как определить, что компьютер заражён?

Есть явные и неявные признаки. Пример явного — на экране появляется баннер, который не даёт ничего сделать. На нём написано, куда отправить деньги, чтобы разблокировать систему. Иногда в таких случаях спасает только полное форматирование диска.

Но вирусы не всегда явно видны. Компьютер может начать подвисать, могут появиться проблемы с доступом к папкам, клавиши могут менять свои роли, а сайты — не открываться (в первую очередь вирусы блокируют сайты компаний, которые продают антивирусное ПО).

Всё это — звоночки, что с вашим компьютером что-то не то.

[00.21.19]

Антивирусные программы

Антивирус — программа для борьбы с вредоносным ПО: уничтожает вирусы и помогает восстановить повреждённые файлы. Известные антивирусы — Kaspersky, ESET, Dr.Web.

На что обратить внимание при выборе антивируса?

- **Регулярное обновление антивирусной базы** — время от времени появляются новые вирусы, ваш компьютер должен быть от них защищён.
- **Восстановление файлов** — пригодится, если важные документы повреждены вредоносным ПО.

Обычно у антивирусов есть бесплатная версия, если её функционала хватает, платную можно не покупать.

Для примера рассмотрим функционал антивируса Dr.Web:

- **Обновление вирусной базы** — если она актуальна, программа подскажет, что обновление не требуется.
- **Режимы проверки**: быстрая и полная.
- **Фоновый режим** — антивирус отслеживает любые действия на устройстве. Если вы сохраняете файл, программа сканирует его на лету: если есть вирус, вы получите уведомление.

[00.24.08]

VPN

VPN (Virtual Private Network) — виртуальная частная сеть. Задача технологии — защитить персональные данные (сайты не смогут их собирать) и обходить блокировки. Например, в Китае запрещены сервисы Google: просто так не получится открыть ни YouTube, ни Google Документы. А с VPN — получится.

Ещё одно преимущество технологии — защита от доступа третьих лиц в общественных сетях. Например, подключаясь к бесплатному Wi-Fi в метро или кафе, мы становимся более уязвимы: через такое соединение хакер может получить доступ к переписками, данным карт или другой информации. VPN шифрует данные и значительно усложняет задачу.

Как же работает VPN?

- Когда мы выходим в сеть без VPN, компьютер обращается к интернет-провайдеру, и через него мы получаем доступ в интернет. Сайты, на которые мы переходим, получают данные о местонахождении и других характеристиках: например, поле и возрасте. Они могут использовать их для навязчивой рекламы.
- VPN-клиенты шифруют данные. Можно стать другой личностью в сети, чтобы узнать о настоящих характеристиках было невозможно.

[00.28.08]

Какой VPN выбрать?

VPN можно установить на телефон, компьютер или как расширение для браузера. Чтобы выбрать подходящий, обратите внимание на параметры:

- **Удобство использования**, чтобы не пришлось разбираться в функциях и настройках. Принцип хорошего VPN — включил и работает.

- **Скорость работы**. Некоторые VPN замедляют скорость интернета, из-за этого страницы открываются подолгу.

- **Безопасность.** VPN-сервисы, даже бесплатные, её гарантируют — личные данные не будут передаваться сайтам.

- **Стоимость.** Есть бесплатные сервисы, а есть платные с дополнительными бонусами. Цены начинаются от $5.

- **Универсальность.** Если вы часто путешествуете, важно, чтобы VPN работал во всех странах без потери качества.

- **Есть служба поддержки.** Если вы платите за сервис, а он сбоит, здорово иметь возможность быстро получить ответ и решение от поддержки.

Важный вопрос — законно ли использовать VPN? Да, законодательство этого не запрещает.

У платных и бесплатных VPN есть свои плюсы и минусы:

- **У платных** высокая скорость, нет навязчивой рекламы, усиленная защита персональных данных, помощь техподдержки. Недостаток — придётся платить.
- **У бесплатных** есть лимиты по скорости, из-за которых VPN придётся включать и отключать, когда он не нужен. Есть реклама.

Но бесплатные сервисы не так уж плохи. Один из них — Kaspersky Secure Connection. Его можно установить на разные операционные системы, как на смартфон, так и на компьютер. А можно зайти на официальный сайт и купить версию для 5 устройств за 1790 рублей в год.

Для компьютеров на Windows ищите и скачивайте VPN только на официальных сайтах. Для смартфонов на iOS и компьютеров на MacOS — в App Store, для смартфонов на Android — в Play Market. Набирайте в поиске «VPN», смотрите на оценки, читайте отзывы и нажимайте «Загрузить», когда нашли подходящий сервис.

[00.36.56]

Итоги

Сегодня мы коснулись трёх важных тем:

- пароли — как их придумывать и хранить;
- вирусы и как от них защититься;
- VPN — что это, и зачем пригодится в жизни.

Надеюсь, этот урок для вас был полезным. До новых встреч в эфире!