«Безопасность в глобальной сети»

Корпорация «Российский учебник»

Галяев Владимир Сергеевич,
старший научный сотрудник Лаборатории математического моделирования и информационных технологий
Федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий»

О чем будем говорить?

В рамках вебинара будут рассмотрены следующие вопросы:

- **основные угрозы глобальной сети;**
- **наиболее распространенные уловки онлайн-мошенников;**
- **меры противодействия угрозам в глобальной сети;**
- **как нивелировать последствия реализации угрозы;**
- **некоторые программные средства, повышающие уровень защиты.**

Шеф, все пропало!

Аналитический центр Национального агентства финансовых исследований (НАФИ) на основании опроса представителей более 500 компаний в 2017 году приводит следующие данные:

- ✓ **Столкнулась с проблемами каждая 2-ая компания**
- ✓ **Серьезно пострадала каждая 5-ая компания**
- ✓ **Средняя сумма убытков – около 300 тыс. руб.**
- ✓ **Общая сумма убытков оценивается не менее 100 млрд. руб.**

Чаще всего это выражалось в заражении вирусами рабочих компьютеров сотрудников, в том числе с последующим вымогательством денег (20%), во взломе почтовых ящиков (12%), атаках на сайт компании (10%).

Кому я нужен, я же не бизнесмен и не политик

По оценкам экспертов более 40% проводимых сетевых атак приходятся на персональные компьютеры граждан.

Крупные вендоры в области информационной безопасности, например, антивирусные компании, в своих квартальных и ежегодных отчетах констатирует, что каждый персональный компьютер становится целью атаки не менее одного раза в год.

Если на предприятии существует уровень корпоративной защиты, но домашние компьютеры, зачастую, вообще не защищены.

Мобильные устройства – 98% находятся в частном пользовании, при этом более 78% пользователей никак не защищают их.

Сервисы и пользователи

- ✓ **Веб-серфинг (просмотр сайтов)**
- ✓ **Социальные сети**
- ✓ **Электронная почта**
- ✓ **Облачные хранилища**
- ✓ **Облачная работа с документами**
- ✓ **Мессенджеры**
- ✓ **Интернет-магазины**
- ✓ **Онлайн-банкинг**
- ✓ **Просмотр видео**

Что нам угрожает

Технические угрозы

- ✓ **Вредоносные программы (вирусы, трояны, черви, руткиты)**
- ✓ **Отказ в доступе к информации**

Информационные угрозы

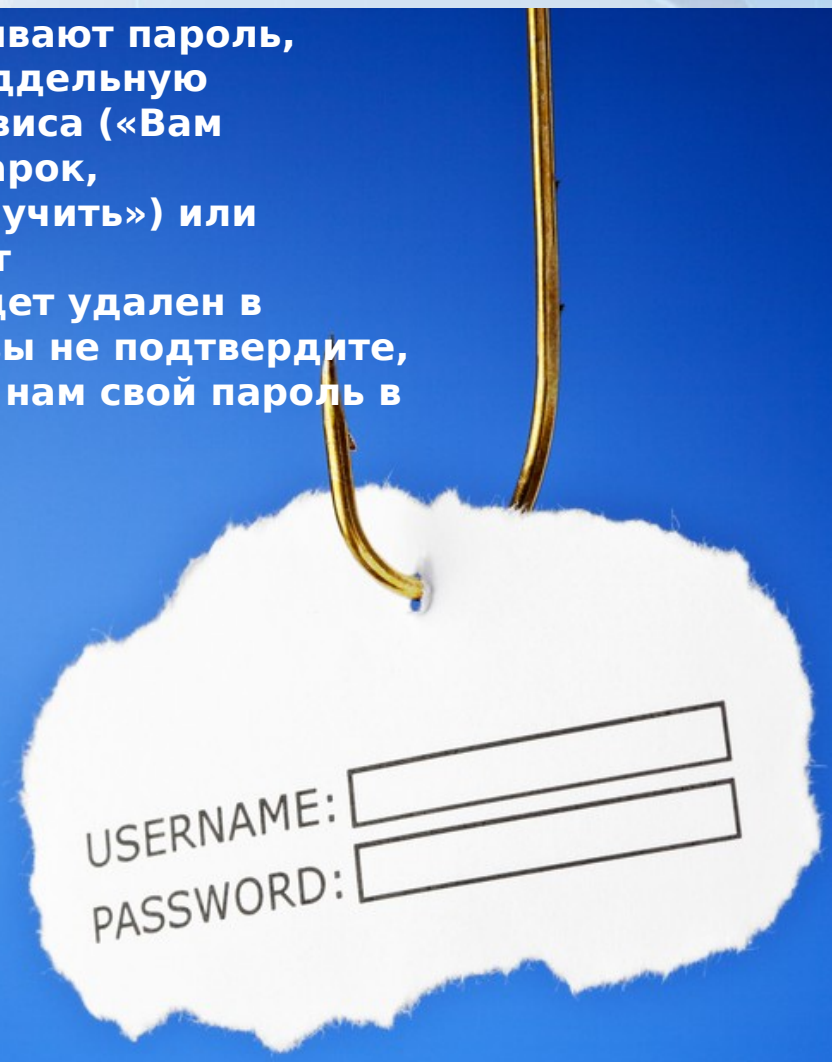
- ✓ **Хищение информации (в том числе, паролей от различных аккаунтов)**
- ✓ **Порча информации**
- ✓ **Кибермошеничество (в том числе, хищение денег, обман с товарами)**
- ✓ **Спам**

Коммуникационные

- ✓ **Кибербуллинг (угрозы, шантаж, запугивание)**
- ✓ **Противозаконный контент (в том числе, неэтичная или противозаконная информация)**

Фишинг

У пользователей выманивают пароль, перенаправляя их на поддельную страницу знакомого сервиса («Вам прислали открытку/подарок, залогиньтесь, чтобы получить») или запугивая («Ваш аккаунт скомпрометирован и будет удален в течение 24 часов, если вы не подтвердите, что вы — это вы, выслав нам свой пароль в ответном e-mail»).



Учетные записи могут быть перепроданы оптом

Чаще всего скупкой почтовых ящиков в больших объемах занимаются спамеры.

Взлом почты

Деньги можно извлечь из самого ящика...

Это могут быть, например, учетные записи соцсетей, хостингов, банков, электронных денег, игровые аккаунты. Если в ящике нет данных о самих паролях, атакующий может запросить восстановление пароля на ящик. Также атакующий обязательно проверит, не подходит ли почтовый пароль к учетным записям на других ресурсах.

...или получить от владельца аккаунта

Пользователь может стать жертвой шантажа — ему предложат выкупить шантажа может быть также личная информация кументов), которая содержится в ящике.

ованного лица

. Доступ может понадобиться вашему конкуренту руднику, ревнивому супругу. Сразу заметим, что от очень маленькую долю от общего объема.

Взлом социальных сетей

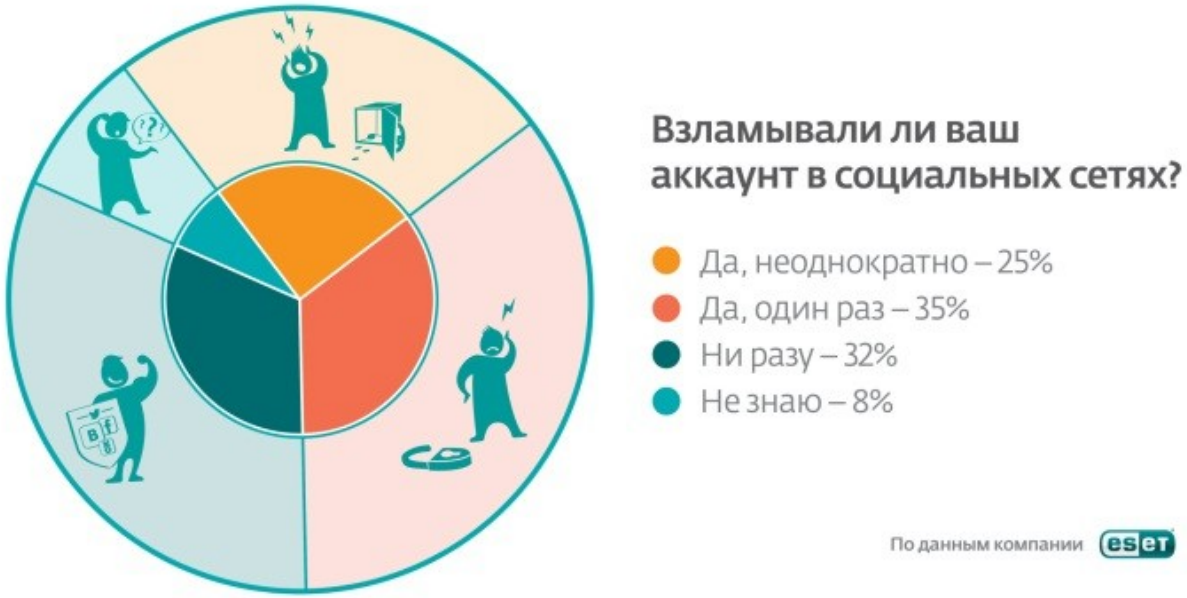
В 2017 году мошенники такими путями похитили у физлиц около миллиарда рублей.

Дискредитация пользователя

Выманивание денег у его друзей и подписчиков

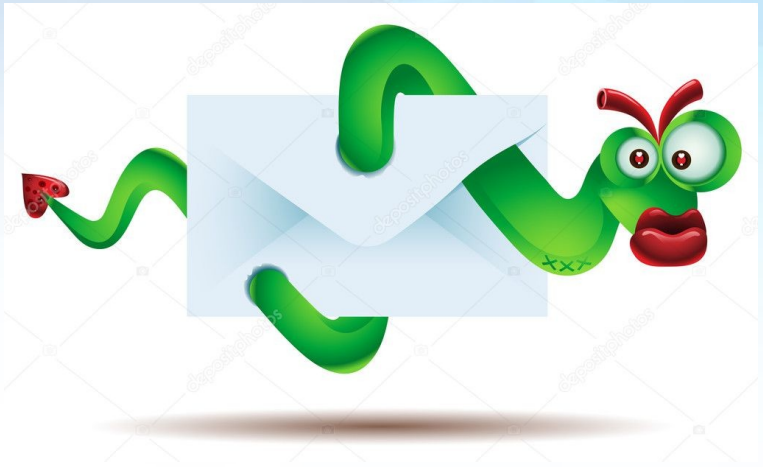
Незаконное распространение рекламы

Получение доступа к личной информации в том числе других пользо



Чем опасны трояны и черви

Компьютерные черви похожи на вирусы в том, что они копируют функциональные копии самих себя и могут вызвать тот же тип повреждений. В отличие от вирусов, которые требуют распространения зараженного файла-носителя, черви являются автономным программным обеспечением и не требует программы-хоста или помощи человека, чтобы размножаться.



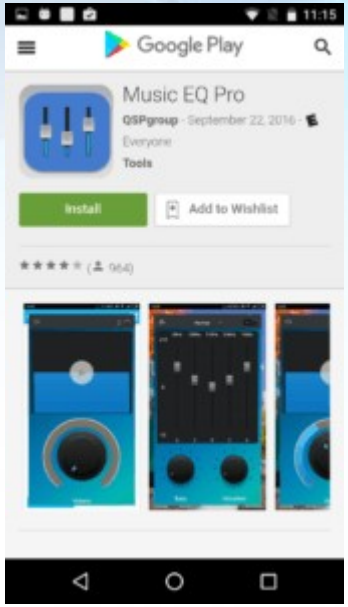
Троян (trojan) — тип вредоносного ПО, названный в честь деревянного коня, который греки использовали для проникновения в Трою. Это вредоносное ПО, которое выглядит законно. Пользователей, как правило, обманным путем заставляют загрузить и запустить его на своем компьютере.

Мобильные устройства – под прицелом

Особенности мобильных устройств:

- **Практически всегда в сети**
- **Пользователи не знают о возможностях защиты или не хотят ее использовать**
- **Содержат большое количество информации как в виде документов и файлов, так и внутри используемых программ**
- **Практически неконтролируемая установка и удаление программ**

Пример: Мобильного троянец вымогатель Trojan-Ransom.AndroidOS.Pletor.d распространялся через официальный магазин приложений Google Play. Троянец выдавал себя за приложение для обслуживания устройства, в задачи которого входили очистка от ненужных данных, ускорение работы устройства и даже антивирусная защита.



Trojan.AndroidOS.Ztorg.ad в официальном магазине приложений Google Play Store

Боты, они же «зомби»

«Бот» — производное от слова «робот» и представляет собой автоматизированный процесс, который взаимодействует с другими сетевыми службами. Боты часто автоматизируют задачи и предоставления информации и услуг, которые могли бы производиться человеком. Вредоносный бот распространяет вредоносное ПО, которое заражает компьютеры и подключает их через бэкдоры к центральному серверу управления, который может управлять всей сетью взломанных устройств. Используя бот-нет злоумышленник может совершать DDOS-ата

Mirai — это вредоносная программа, которая запускает бот-сеть в интернете вещей. В прошлом году она нанесла серьезный урон в сети, остановив несколько крупных сервисов. Причиненный ею ущерб оценивается в 4 млрд. долларов.

Законодательство нам поможет!

УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

«Национальный координационный центр по компьютерным инцидентам (НКЦКИ) является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

Приказ Директора ФСБ России от 06.09.2018 № 52109)

Как вы считаете, способны ли сегодня российские правоохранительные органы успешно расследовать компьютерные преступления, находить и наказывать компьютерных злоумышленников?

Согласно статистике МВД России, в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое 20 преступление.

Раскрываемость данных преступлений составила 41,3%

Информация с сайта Генеральной прокуратуры РФ

Проблема - решение

1. **Вредоносное программное обеспечение**	**Установка и использование антивирусного программного обеспечения** **Обновление программного обеспечения, особенно операционной системы**
2. **Подбор пароля**	**Не использовать «слабые» пароли (свое имя, телефон, qwerty и т.п.** **Использовать разные пароли для разных ресурсов.** **Особенно важно иметь устойчивый пароль от почтового ящика, на который зарегистрированы важные ресурсы (онлайн-банк, например)**
3. **Взлом через «секретный вопрос»**	**Вводить собственный, уникальный секретный вопрос с нетривиальным ответом**

Проблема - решение

4. **Социальная инженерия, фишинг**

Не открывать ссылки (а лучше сами письма) от незнакомых людей с непонятными заголовками («Срочно проверьте договор. Нам нужно отправлять данные»)

Уделите внимание адресной строке в браузере. Похожая картинка, но разные адреса – верный признак мошенников

Не используйте чужие аккаунты ни под каким предлогом, и никому не передавайте свои аккаунты

Настройте двухфакторую авторизацию, если это возможно

5. **Доступ к личным данным**

Не храните личные данные в облачных хранилищах. Все действительно важные документы (а также фотографии и т.п.) лучше

Что делать, если уже …

1. **Взломали почту / социальную сеть**

Если Вам еще удается зайти (злоумышленник не сменил пароль), то смените пароль немедленно.

В социальной сети желательно сделать рассылку или вывесить пост, о том. что Вас взломали и сообщения в такой-то период не надо воспринимать

Взаимодействуйте со службой технической поддержки почтового сервиса или социальной сети. Помните: у них есть жесткие инструкции, чтобы не выдать информацию третьим лицам, - слушайте инструкции и отвечайте максимально нейтрально.

2. **Вы думаете, что взломали онлайн-банк или аналогичный сервис**

Звонок в службу поддержки клиентов для блокировки всех карт.

Физическое посещение банка, чтобы восстановить доступ

Что делать, если уже …

3. **Подцепили троянец-вымогатель, который заблокировал (зашифровал) данные**

Не лечите с помощью антивируса! Вы скорее всего уничтожите доступ к своим файлам.

Большинство крупных антивирусных компаний выпускает специальные «таблетки» под конкретные вирусы.

На форумах достаточно оперативно появляются подходящие коды к тому или иному вирусу. Попробуйте поискать. Если ничего не найдено и есть время в запасе – попробуйте выждать 1-2 дня и повторить поиск.

4. **Компьютер зомбировали (постоянно занята оперативная память, присутствует сетевой трафик, даже если не пользуетесь сетью)**

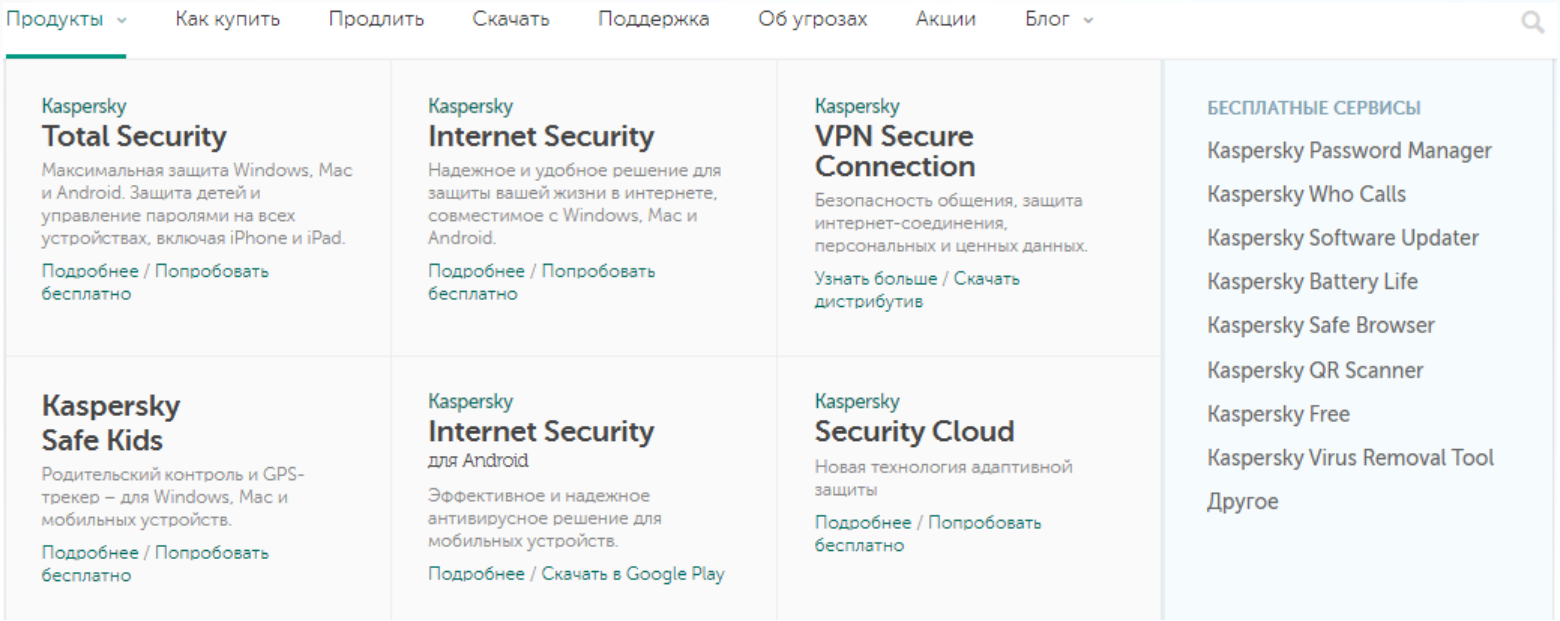
Запустить полную проверку диска антивирусом, которому доверяете

Некоторые особенности программного обеспечения

Антивирусы

Производители антивирусных программ выпускают целую линейку продуктов, которые отличаются по функционалу. При работе с сетью важно, чтобы были доступны функции безопасного соединения, поддержка проверки сайтов, а также контроль запускаемого программного обеспечения.

Важно помнить: НИ ОДИН антивирус не гарантирует 100% защиты от всех атак. Но «гулять» по сетевым ресурсам совсем без сетевого антивируса – это почти гарантированное заражение.



Некоторые особенности программного обеспечения

Браузеры

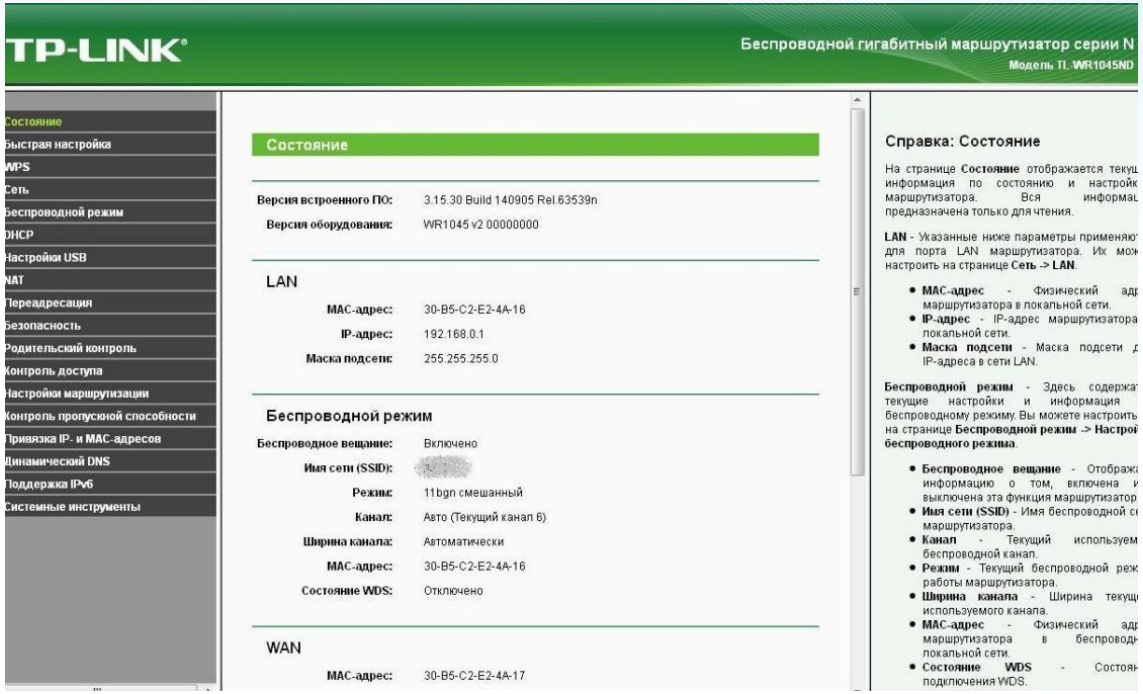
Пользуйтесь проверенным, распространенным браузером, который не навязывает Вам установку дополнительных компонент.

Если при установке есть различного рода дополнительные пункты (с проставленными по умолчанию галочками) на установку дополнительных компонент, то лучше поискать другой браузер.

Полезно, чтобы браузер поддерживал установку плагина от Вашего антивируса, который обеспечивает защищенное соединение.

И немного о технике

Домашние роутеры могут использоваться по принципу «включил и используй», но лучше их настроить. В частности, сменить пароль администратора и настроить контроль доступа



Спасибо