



ЮБИЛЕЙНЫЙ ГОД
Благотворительного Фонда

«Цифровая безопасность»

Проект реализуется при поддержке Благотворительного фонда «Дорога к дому» компании «Северсталь»



Фролов Александр Альбертович



Руководитель проекта «Цифровая безопасность»

Фонд поддержки социальных проектов и инициатив «Добрый город»



2020 г.



Что для Вас цифровая безопасность?

Цифровой след - уникальный набор данных, оставленный человеком в интернете.

Цифровые следы бывают:

- **Активные**
- **Пассивные**



- Конституция РФ
- Федеральный закон «Об информации, информационных технологиях и о защите информации»
- Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»
- Федеральный закон «О персональных данных»
- Гражданский кодекс РФ
- Уголовный кодекс РФ
- Кодекс РФ об административных правонарушениях

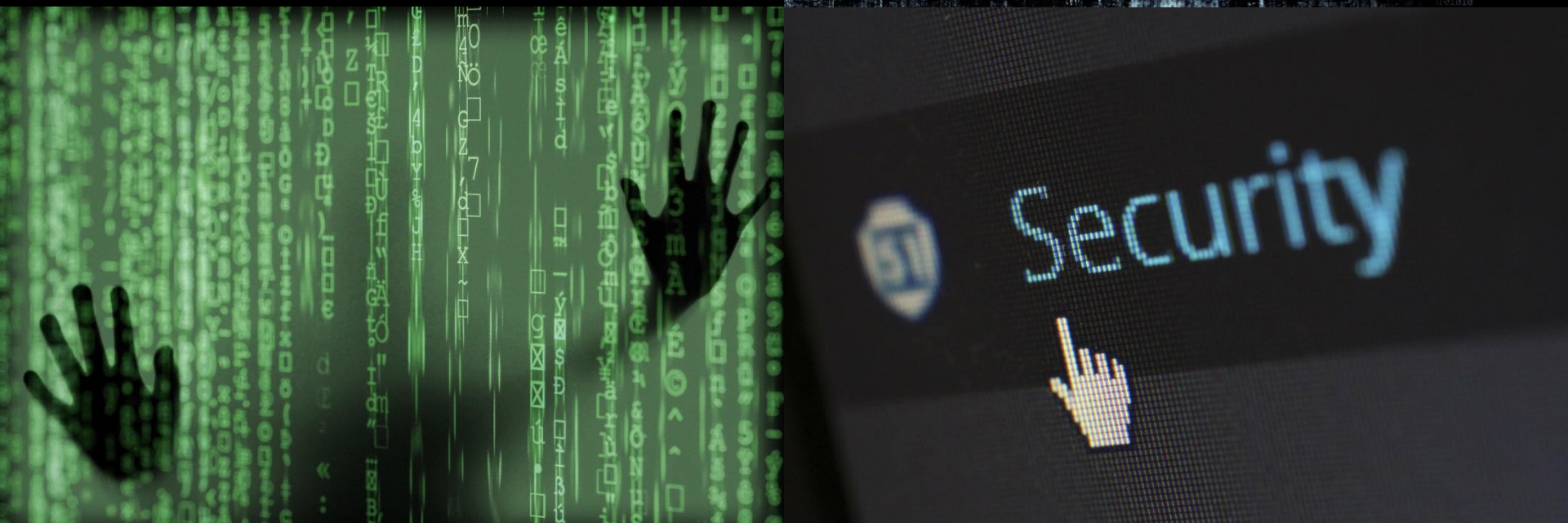
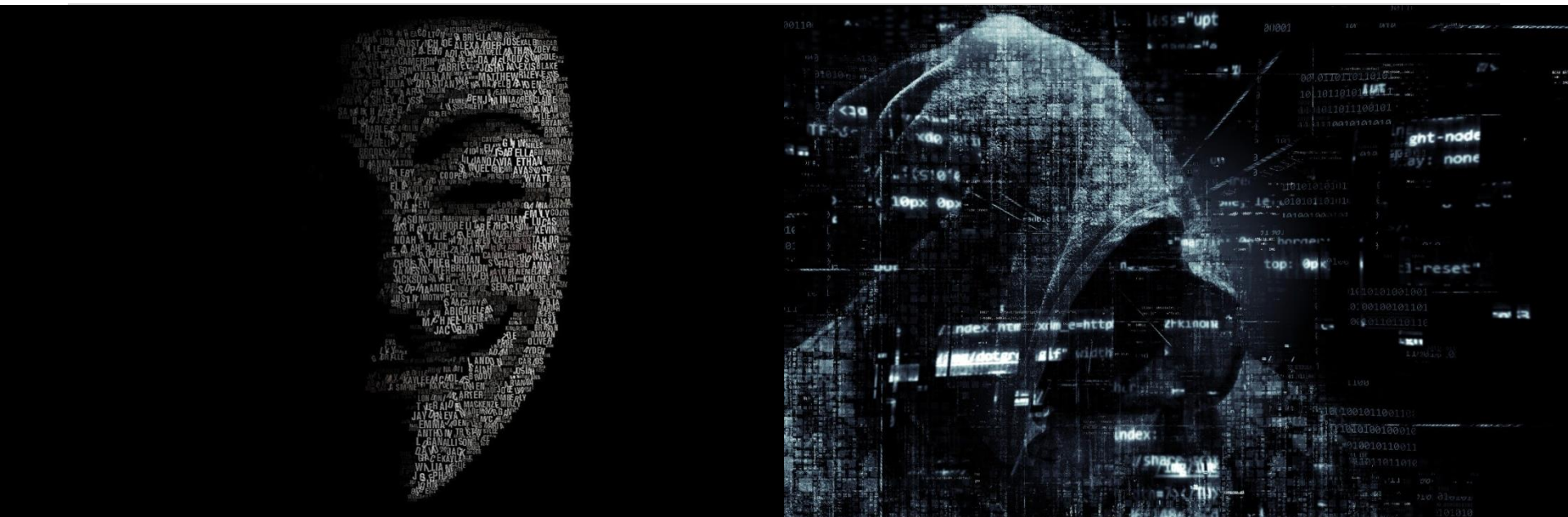
- Запрещено распространять информацию, направленную на пропаганду войны, разжигание расовой, национальной или религиозной ненависти и вражды
- Не допускается распространение информации в неприличной форме, оскорбляющей человеческое достоинство и общественную нравственность, выражающую явное неуважение к обществу, государству, официальным государственным символам, Конституции или органам власти

- Запрещено призывать к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка
- Не допускается распространение недостоверной общественно значимой информации под видом достоверных сообщений
- Запрещается нарушать авторские права и права субъектов персональных данных.

- 1. Ваши личные данные и информация, в том числе, составляющая банковскую тайну**
- 2. Номера телефонов и электронная почта для спам сообщений и звонков**
- 3. Ваши страницы в социальных сетях для обмана от вашего лица других людей**
- 4. Ваши пароли, Cookie-файлы, ответы на секретные вопросы и другая информация, которая может помочь получить доступ к вашим аккаунтам**

- 1. Мошенничество в интернете (в т.ч. в интернет-магазинах)**
- 2. Небезопасные сети, цифровые носители, сайты и файлы**
- 3. Фейк-страницы в социальных сетях**
- 4. Фишинг (совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль)**
- 5. Компьютерные вирусы**

Вирусы в интернете



- Stealer
- Keylogger
- Вирусы-шифровальщики
- Скрытые майнеры
- RAT
- BotNet



Stealer / Keylogger

Stealer - вирус, функционал которого состоит из воровства сохранённых паролей, файлов с рабочего стола, Cookie-файлов, криптовалютных кошельков и других данных, которые могут быть интересны хакеру.

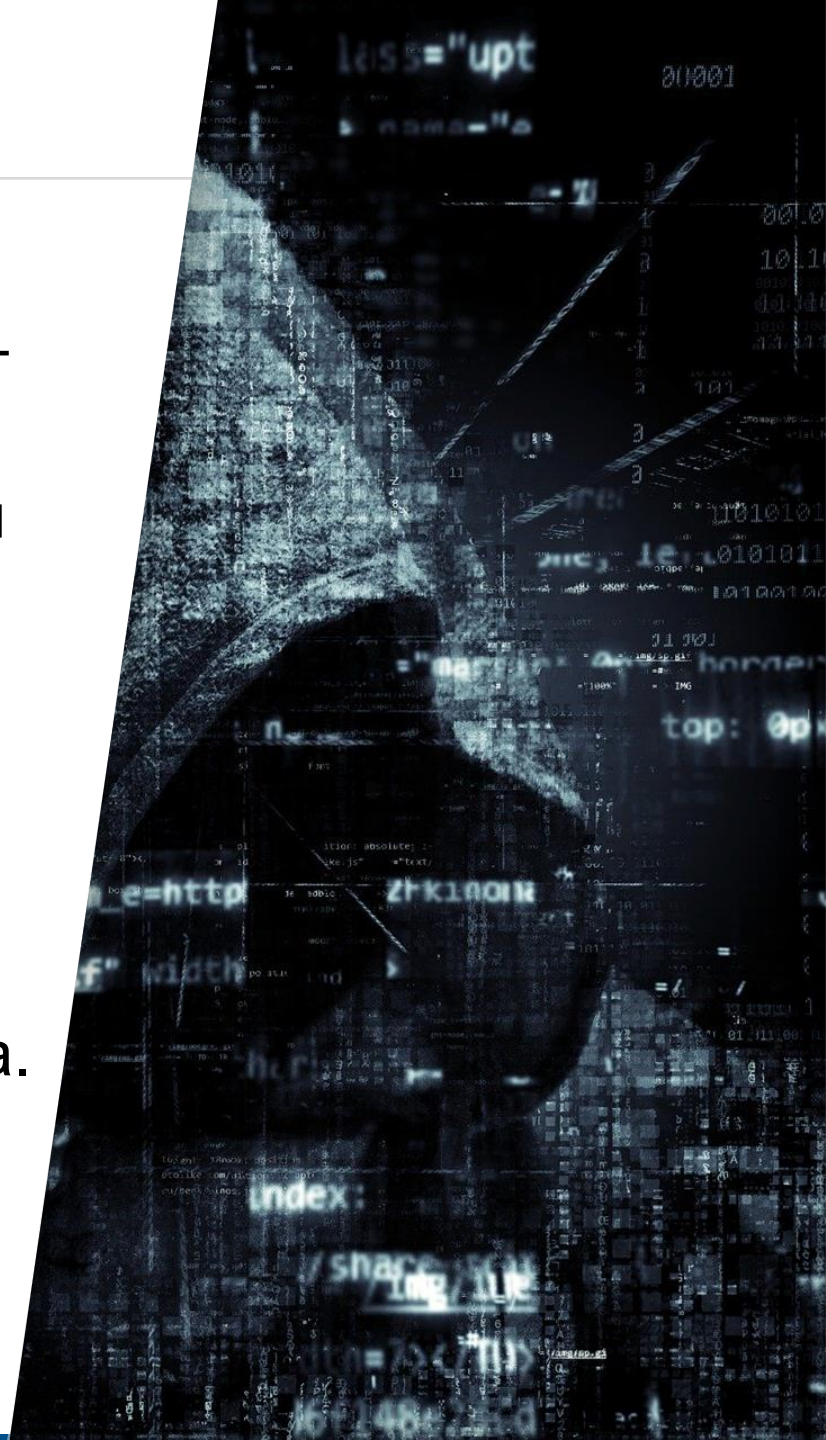
Keylogger - вирус, который запоминает и передаёт хакеру нажатые на клавиатуре компьютера клавиши.



Шифровальщики / Скрытый майнер

Шифровальщики - вирусы шифровальщики зашифровывают всю информацию на компьютере жертвы, а потом вымогают деньги за расшифровку

Скрытый майнер - вирус, который устанавливается на компьютере жертвы и использует ресурсы этого компьютера для майнинга криптовалют для хакера.



RAT / BotNet

RAT (Remote Administration Tool) - средство удалённого доступа к системе. Программа, которая предоставляет удалённый доступ к компьютеру.

BotNet - вирус, который используется для массового заражения компьютеров и включению их в сеть подконтрольных хакеру ботов. После заражения хакер может использовать ресурсы заражённого компьютера для совершения незаконных действий (рассылка спама, DDOS-атаки) или майнинга криптовалюты



- Установить и регулярно обновлять антивирус
- Регулярно обновлять другие программы и операционную систему
- Не запускать подозрительные программы
- Не хранить пароли в браузере или в текстовом файле на рабочем столе

Предупреждения антивируса

**TrojWare.Win32.PSW.OnLineGames.NFE@89114**

Location: C:\Users\tester\Desktop\vi...\patra.exe

More information: Unavailable

**Clean (Recommended)**
Quarantines the file

**Ignore**
Ignores the alert and allows the file operation 

[Show Activities](#)

Перегрев компьютера, громкий шум куллеров



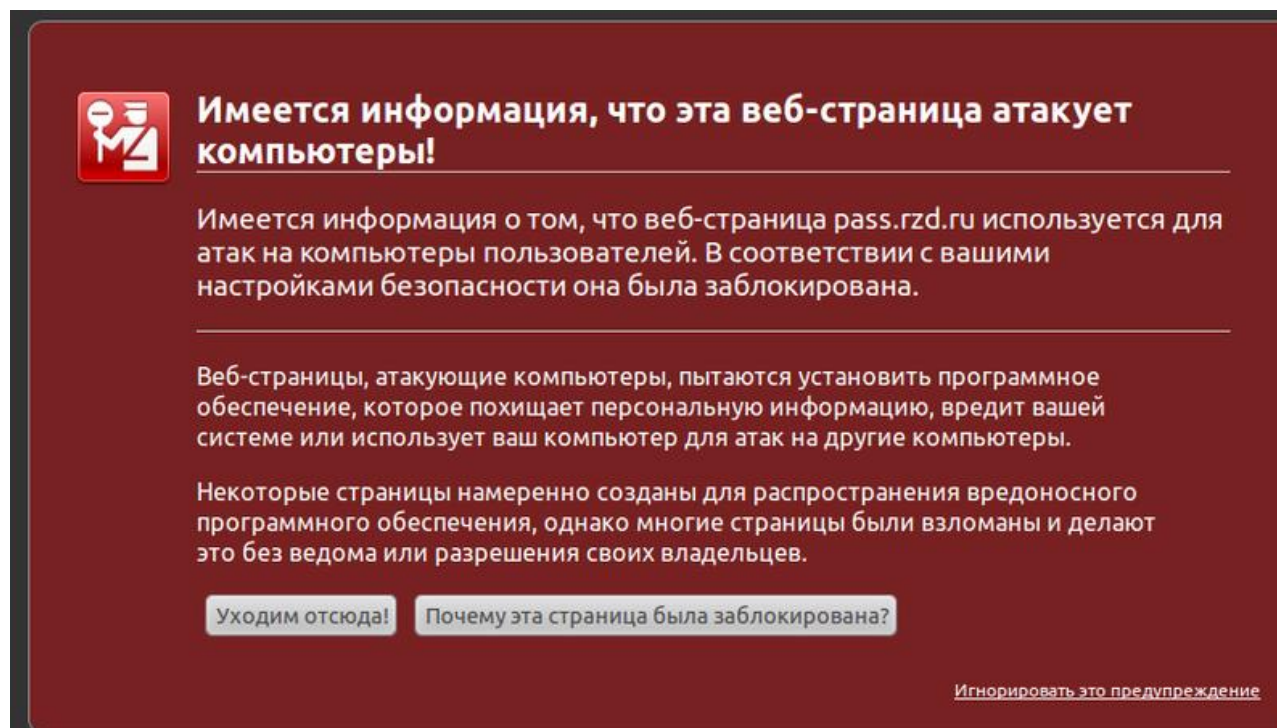
Процесс использует слишком много мощностей процессора

Подозрительные процессы

Имя	Состояние	99% ЦП	74% Память	0% Диск	0% Сеть
Приложения (10)					
▷		0,1%	231,8 МБ	0 МБ/с	0 Мбит/с
▷		71,8%	386,3 МБ	0 МБ/с	0 Мбит/с
▷		0%	3,3 МБ	0 МБ/с	0 Мбит/с
▷		0%	8,4 МБ	0 МБ/с	0 Мбит/с

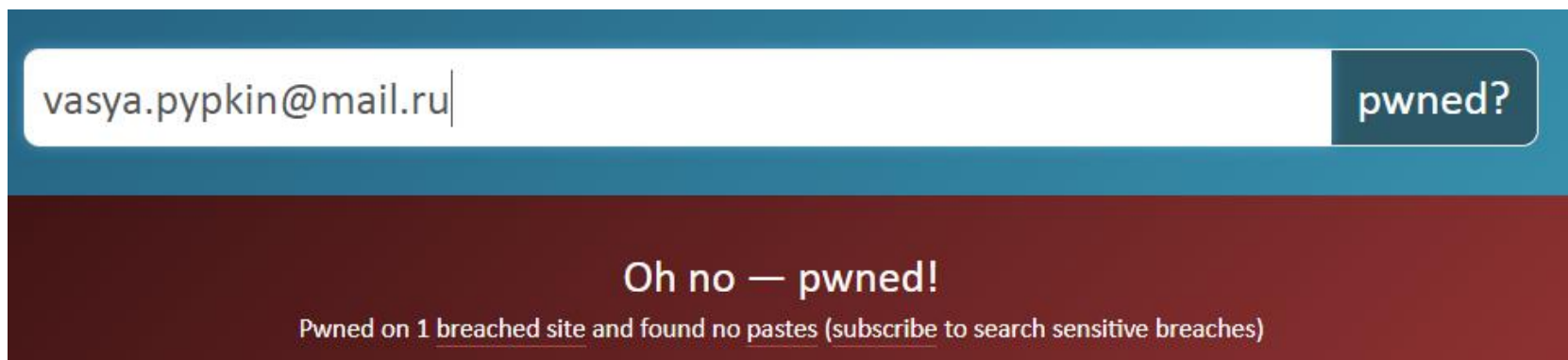
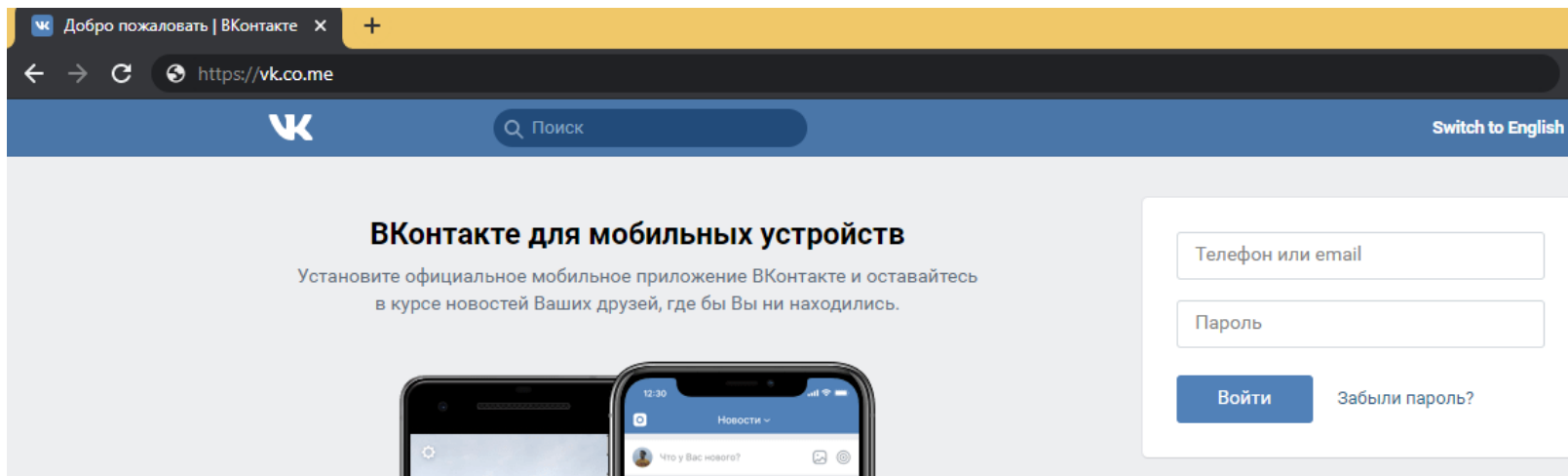
Узел службы: локальная систе...	C:\Windows\system32\svchost.exe -...	0%	19,3 МБ	0 МБ/с	0 Мбит/с
Узел службы: локальная систе...	C:\Windows\System32\svchost.exe -...	0%	83,4 МБ	0 МБ/с	0 Мбит/с
Узел службы: локальная служ...	C:\Windows\system32\svchost.exe -...	0%	6,7 МБ	0 МБ/с	0 Мбит/с
Узел службы: локальная служ...	C:\Users\User\Pictures\svchost.exe -...	0%	2,4 МБ	0 МБ/с	0 Мбит/с
Узел службы: локальная служ...	C:\Windows\system32\svchost.exe -...	0%	12,8 МБ	0 МБ/с	0 Мбит/с
Узел службы: локальная служ...	C:\Windows\System32\svchost.exe -...	0%	10,7 МБ	0 МБ/с	0 Мбит/с
Узел службы: модуль запуска ...	C:\Windows\system32\svchost.exe -...	0%	3,2 МБ	0 МБ/с	0 Мбит/с
Узел службы: сетевая служба ...	C:\Windows\system32\svchost.exe -...	0,2%	8,8 МБ	0 МБ/с	0 Мбит/с
Узел службы: служба загрузки...	C:\Windows\system32\svchost.exe -...	0%	1,4 МБ	0 МБ/с	0 Мбит/с
Узел службы: удаленный вызо...	C:\Windows\system32\svchost.exe -...	0,2%	4,2 МБ	0 МБ/с	0 Мбит/с

JavaScript - язык программирования, который используют веб-страницы для взаимодействия с пользователем. Браузер выполняет любой JavaScript код при заходе на страницу. Злоумышленник может встроить опасный JavaScript код на своём сайте или взломав чужой. В результате выполнения таких скриптов вас может перекинуть на другой сайт, у вас могут украсть Cookie-файлы или ваш компьютер может использоваться для майнинга криптовалюты.



Фишинговые сайты

Утечки баз данных с сайтов



- Никому не передавать свои пароли и денежные средства
- Без необходимости не регистрироваться на сайте со своими персональными данными. Использовать временную электронную почту
- Не использовать один пароль для нескольких сайтов. Использовать случайно генерируемые пароли
- По возможности использовать двухфакторную аутентификацию или другие меры безопасности
- Проверять URL перед совершением каких-либо действий на сайте

- Не указывать в социальных сетях номер телефона, электронную почту, паспортные данные, адрес и другую информацию о себе
- Отключить JavaScript полностью или заблокировать некоторые виды опасных скриптов
- Заблокировать интернет рекламу
- Не скачивать подозрительные файлы
- Регулярно проверять компьютер на предмет безопасности
- Проверять с кем Вы общаетесь в сети

Кейс № 1

На концерте, приуроченном ко Дню защиты детей, ученица 9 класса Мария вела съёмку происходящего на фото и видеокамеру. Помимо самой Марии, в кадр попал зритель Сидоров.

Мария поделилась фото и видеозаписью в социальных сетях. Спустя некоторое время Сидоров обнаружил в Интернете пост Марии, на котором было запечатлено его изображение. Крайне возмущившись увиденным, Сидоров потребовал у Марии удалить все опубликованные материалы с его участием. Мария отказалась, сославшись на то, что это ее фотографии и видео. Оцените ситуацию.

Кейс № 2

Морозов зашел на сайт интернет-магазина, который уведомил его об использовании файлов cookie. Морозову было предложено либо согласиться с данным условием работы с сайтом, либо покинуть его без возможности дальнейшего использования интернет-магазина. Форма согласия была сформирована автоматически, с автоматическим проставлением галочки в графе «согласен». Полагая, что действия сайта противоречат действующему законодательству, Морозов обратился за юридической консультацией. Оцените ситуацию.

Кейс № 3

К вам приехал погостить дальний родственник. Он попросил вас попользоваться вашим компьютером, когда вы решили сходить в магазин. Пока вас нет, родственник захотел скачать через торрент музыку для телефона. Вернувшись вы увидели, что он, ругаясь, что ничего не работает, закрывает предупреждение антивируса и запускает явно вирусную программу. Что вам надо сделать, что бы минимизировать ущерб от действия этого вируса?

Наши контакты

Партнеры проекта



Фонд поддержки социальных проектов и инициатив «Добрый город»



(4852) 73-11-08



a.a.froloff@gmail.com



дорога-к-дому.рф



vk.com/dorogakdomu



facebook.com/dorogakdomu35

instagram.com/dorogakdomy

Клуб цифрового права «Digital Femida» ЯрГУ им. П.Г. Демидова



Аппарат Уполномоченного по правам человека в ЯО



АНО «Ресурсный центр поддержки НКО и гражданских инициатив»

