



ЯКласс

КИБЕРБЕЗОПАСНОСТЬ: ЧТО НУЖНО ЗНАТЬ УЧЕНИКАМ И УЧИТЕЛЯМ?

Нафикова Роза Альбертовна
региональный представитель «Якласс»
в Московской области

Грекова Виктория Александровна
заместитель директора МОУ СОШ №8, г. Подольск

www.yaclass.ru

Цифровой мир



Больше половины населения Земли пользуется интернетом.

В России доступ к глобальной сети имеет **81%** населения.
7 место по вовлеченности людей в цифровую экономику
5 место по числу пользователей смартфонов

Каждый из нас находится онлайн в среднем **7 часов в день!**

Мы общаемся, совершаем покупки, учимся и управляем финансами, не выходя из дома.



Факт

90 % взрослых используют гаджеты для развития и обучение ребенка. Так ответили родители детей **3-6 лет**

В начальной школе почти у **86 %** детей есть свой смартфон или планшет, а к **11-14 годам** - у **99 %**.

В прошлом году этот показатель составлял **97 %**.

У **40 %** детей в младшей школе уже есть страница в социальных сетях. Среди старшеклассников этот показатель возрастает до **92 %**.



ЯКласс
2021

Кибератаки



5,5 раз

рост количества атак на образовательные сервисы и электронные дневники по [данным](#) Ростелеком

1 300

новых вредоносных и нежелательных программ, которые маскируются под популярные сервисы для видеоконференций по [данным](#) Kaspersky Lab

350 000

пользователей были атакованы через электронные учебники и готовые рефераты по [данным](#) Kaspersky Lab



ЯКласс
2021

ЯКласс



Каждую неделю

происходят атаки на сайты ЯКласс в разных странах



Май 2020

месяц с самым большим количеством атак. Сразу после попадания на 4 строчку самых популярных образовательных сайтов в мире по [данным](#) SimilarWeb

ЯКласс
2021

ЯКласс



softline[®]
We know we can



РОСКОМНАДЗОР



Что важно знать!

Цели злоумышленников:

- Обогащение за ваш счет
- За счет ваших друзей
- Политические активисты
- Вербовка криминала
- Поступки психически нездоровых людей

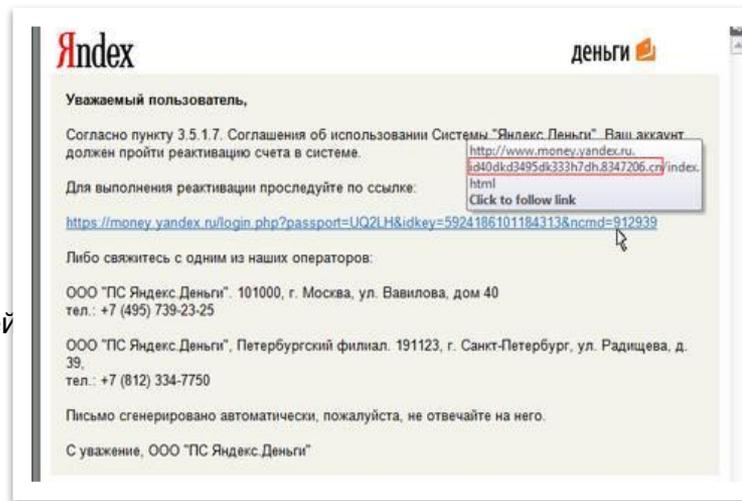
Как они действуют? взламывают или атакуют

ШИРОКОВЕЩАТЕЛЬНО

1. Фишинг
2. Социальная инженерия
3. Зловреды на сайтах
4. Утечки баз паролей

ПРИЦЕЛЬНО

1. Брутфорс эккаунтов
2. Зараженные флэшки
3. Взлом через ваших близких
4. Физический доступ к устройствам

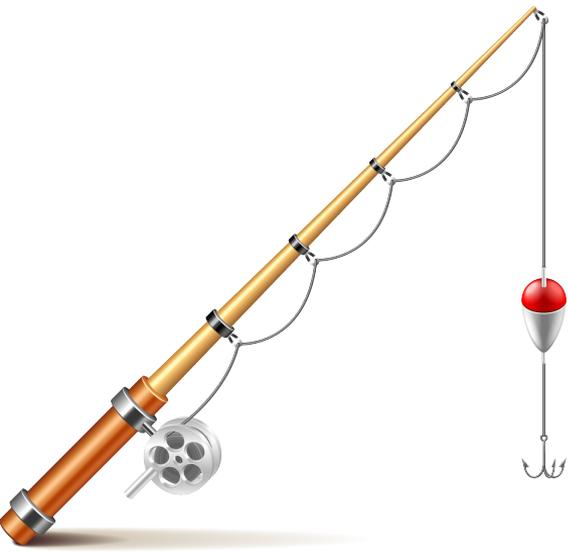


Фишинг
Что это такое?

Фишинг

(англ. fishing — рыбная ловля)

— вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.



Примеры фишинга «в черную»:



- Пользователю приходит письмо с информацией об акции на таком-то ресурсе
- Он кликает по абсолютной ссылке и переходит на поддельный сайт (идентичный оригинальному)
- Совершает покупки, производит оплату на поддельном (фишинговом) сайте



Найдите отличия:

lamoda.ru

Iamoda.ru

1amoda.ru

Фишинг

На что обращать
внимание?

- Адрес отправителя письма
- Ссылка или файл, которые есть в письме
- Адрес сайта, который находится по ссылке

Триггеры:

Почта не в домене yaklass:

Нормальный адрес: info@yaklass.ru

Подозрительный адрес: info@yaclasss.ru

Сокращенные ссылки, прим.: bit.ly/3dD8AR9,
vk.cc/4qZzHY, clck.ru/BBYw2, cutt.ly/jcY6h42

Домен сайта, который Вы видите впервые,
прим.: yaklass.ucoz.ru, yak1ass.su,
yaklassmail.bitreeks24.com, yaklass.bitrix244.net



Безопасная среда социальных сетей

«Одинок тот, кто всегда онлайн»

А. Полярный

- С кем дружить в цифровом мире?
- Какую информацию нельзя выкладывать в сети?
- Сетевой этикет
- Или кто твой цифровой друг?



Кибербуллинг (интернет-травля)

- это намеренные оскорбления, угрозы, с помощью современных средств коммуникации - чаще всего в социальных сетях, мессенджерах, онлайн-играх.



Кибербуллинг

Вот приходит жирный тролль...»
Как себя вести с троллями и другими неприятными субъектами.

Что делать? План действий

- Никогда не отвечайте на буллинг
- Если вам прислали сообщение, которое вы считаете оскорбительным для вас, обязательно сделайте его скриншот и сохраните на компьютере – это будет отличным доказательством в будущем.
- Блокируйте булли и сообщайте администрации ресурса
- Поговорите о проблеме с кем-нибудь
- Если в сети вам угрожает одноклассник, обязательно расскажите об этом учителю и администрации школы.
- Если кто-то угрожает вам и распространяет ваши персональные данные по всему интернету, сообщите об этом взрослым и в полицию.
- Скрывайте свои страницы в соцсетях
- Если в соцсети есть приватный режим, то рекомендуем вам применить его
- Проявите сочувствие Всегда помните, что счастливые и самодостаточные люди не травят других.

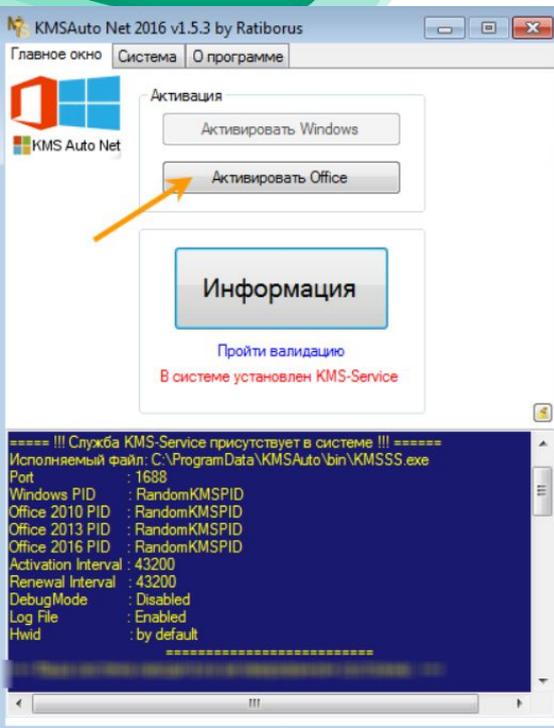


ЯКласс
2021

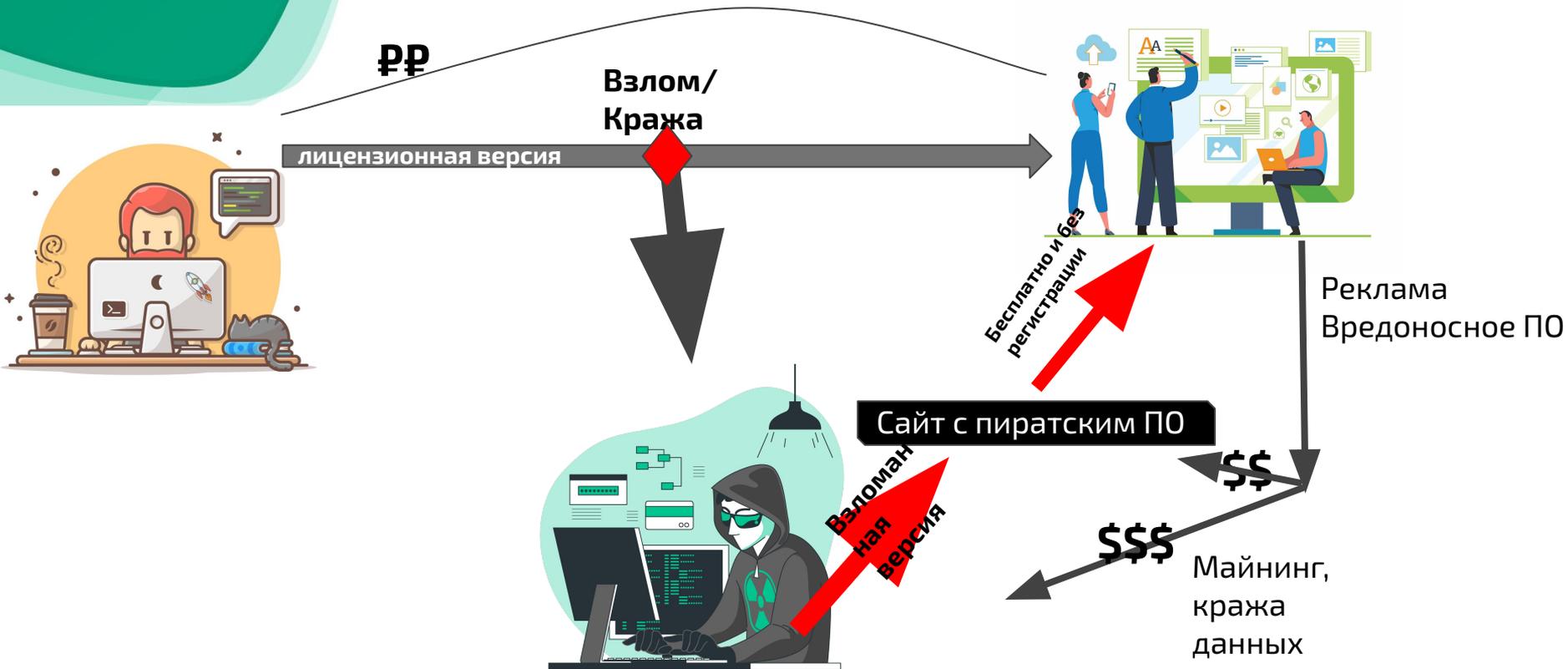
Пиратское программное обеспечение

– это контрафактное ПО, которое киберпреступники нелегально копируют и продают/распространяют бесплатно.

Чаще всего под “удар” от правоохранительных органов попадают не хакеры-взломщики, а те - кто использует нелицензированное ПО.



Как это работает?



Последствия от использования пиратского ПО

От создателей “кряка”(crack):

- Замедление компьютера
- Утечка данных с Вашего ПК
- Использование ресурсов вашего ПК для майнинга

От правоохранительных органов:

- Штрафы для физ. и юр. лиц ([ст. 7.12 КоАП РФ](#))
- Возмещение ущерба разработчику ПО
- Изъятие компьютера

Вас взломали? Вы “подхватили” вирус?

С вероятностью **90%**

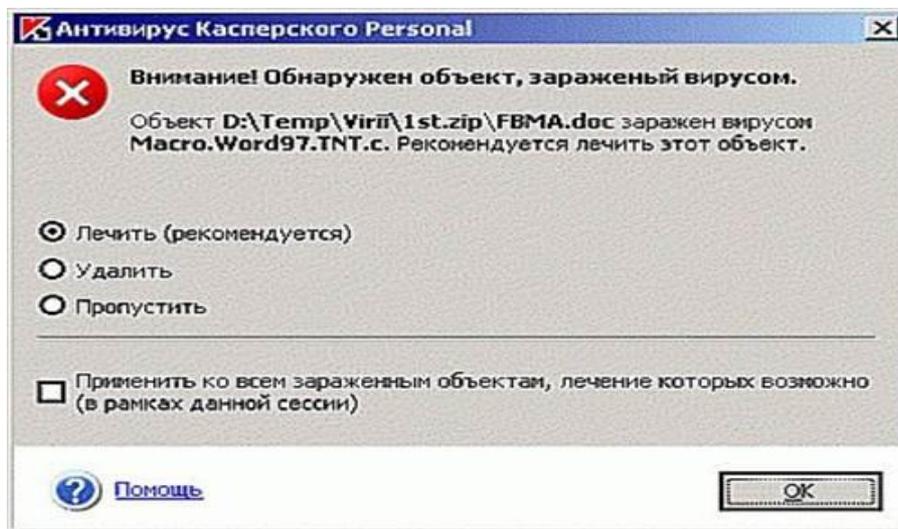
вы не узнаете, что вы взломаны!



Как узнать, что вы заражены?



1. Сообщения антивирусов
2. Правила переадресация почты, которые вы не ставили
3. Запросы подтверждения входов со странных адресов или устройств
4. Сообщения всему вашему контакт-листу от вашего имени



Как защититься от взлома?



Четыре простых правила:

1. Каждому аккаунту – свой пароль
2. Сложный пароль
3. Пароль часто меняемый
4. Меняемый с надежного устройства



12345678

Jxtyu ckj;ysq gfhjkm

7ftx3#

Требования к хорошему паролю

Хороший, надежный пароль должен состоять из не менее **8** символов и содержать в себе:

- прописные буквы английского алфавита от А до Z;
- строчные буквы английского алфавита от а до z;
- десятичные цифры (от 0 до 9);
- специальные символы (например: !, \$, #, %);

Примеры: XZAz0znt1sUGcfGa |)Hw1LJ^l| |
WRLeWah}#h}

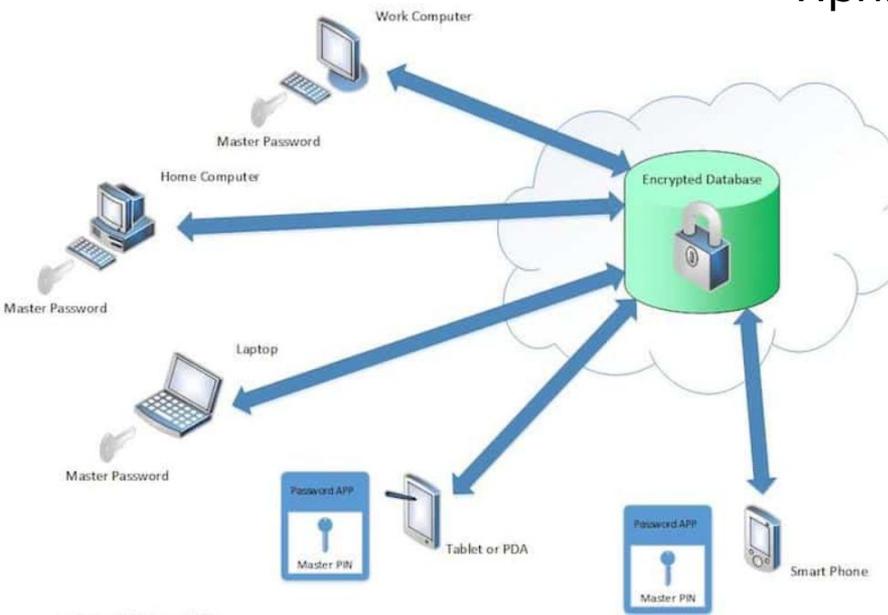


Пароли
Где хранить
пароли?

Менеджеры паролей

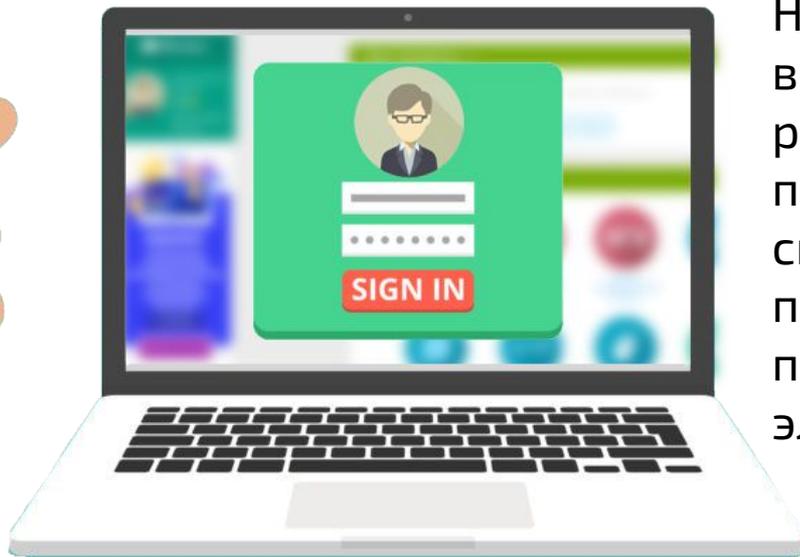
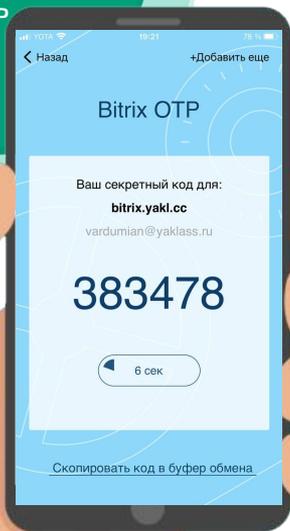
Это сервисы, которые созданы специально для надежного хранения паролей. Они содержат информацию в зашифрованном виде, что затрудняет взлом паролей кибермошенниками.

Примеры: Bitwarden, 1Password



Пароли
Надежная
надежность

Двухфакторная аутентификация



На практике это обычно выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS, в приложении или электронной почте

Кибергигиена



1. Не держите большие архивы «на всякий случай»
1. Используйте надежные пароли
2. Введите для себя понятие «чистого» устройства
3. Не ходите с чистого устройства на сомнительные сайты
4. Не устанавливайте непонятные программы
5. Забудьте про публичные wi-fi и автоподключения
6. Чужие флэшки и флэшки с конференций – угроза!
7. И не забудьте, что принцип «один раз не считается» в кибербезопасности не работает!!! ☺

ЯКласс
2021

Кибергигиена



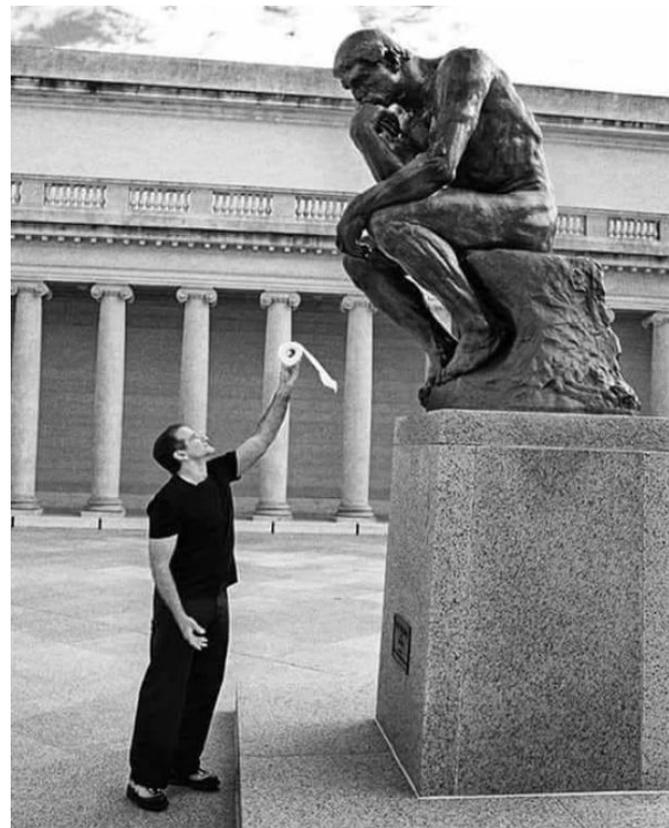
Нет смысла атаковать хорошо защищенных!

Это дорого!

Это долго!

Проще атаковать “цифрового бедняка”

из доверенной среды!



Куда бежать?



Управление «К» МВД России в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие

1. преступлений в сфере компьютерной информации:
2. преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности:
3. преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации.
4. преступлений, связанных с незаконным использованием объектов авторского права или смежных прав.



О кибербезопасности на ЯКласс

[Вебинар для учителей «Проводим классный час: буллинг и травля в школе»](#)

[Вебинар для родителей «Родителям на заметку: наши дети и соцсети».](#)

[Онлайн -урок «Соцсети под защитой»](#)

[Классный час. Кибербуллинг и буллинг \(11+\)](#)

[Онлайн-урок «Вокруг науки с "ЯКласс"»: Кибергигиена. Как безопасно пользоваться личными данными](#)

Минутки кибербезопасности

Вместе с нашим экспертом ребята:

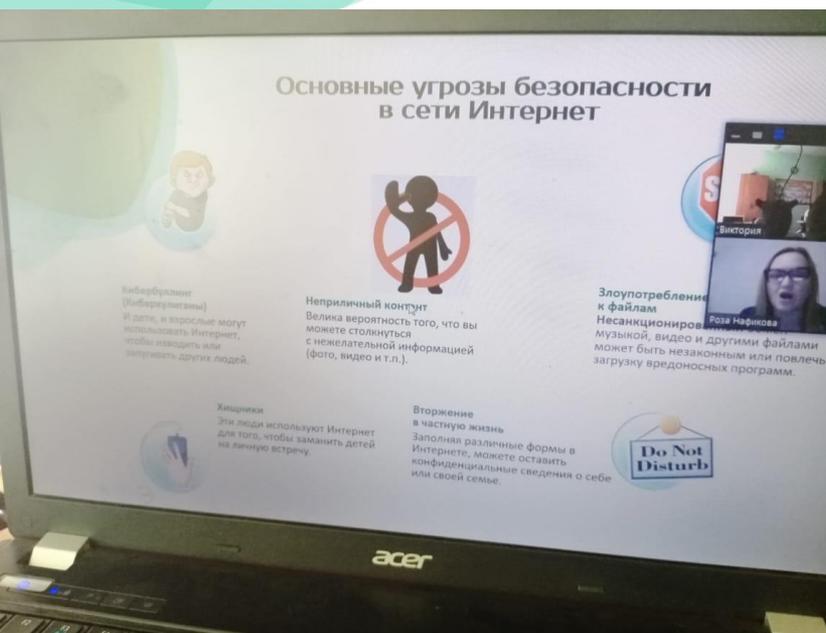
- узнают, **какие угрозы могут подстергать в Интернете;**
- познакомятся **с основными правилами безопасности,** которые надо соблюдать при работе в Сети;
- смогут пройти **увлекательную онлайн-викторину** и получить **сертификат, подтверждающий звание Знаатока кибербезопасности.**

Форма проведения — онлайн-подключение.

Продолжительность — 20 мин..

После мероприятия мы направим на почту учителя шаблоны сертификатов, которые можно будет вручить ученикам, успешно выполнившим онлайн-викторину на «ЯКласс».

Чтобы принять участие в мероприятии, все участники должны быть зарегистрированы на сайте «ЯКласс».



Минутки кибербезопасности. Выдача проверочной работы (викторины).

www.yaklass.ru

Результаты - Минутки кибербезопасности. викторина.

Отзывы

ЯКласс

Виктория Александровна Грекова
48
Мой профиль
Выйти

Начало
Справочный раздел
Мои классы
Вебинары
Новости
ТОПы
Учебные заведения
Предметы
Проверочные работы
Результаты учащихся
Обновления
Управление пользователями
Подписка Я+
ЯКлуб
Переменка
Поиск по сайту

Учащийся	Результат	Учащийся	Результат	Учащийся	Результат	Учащийся	Результат	Учащийся	Результат	Учащийся	Результат	Учащийся	Результат	Учащийся	Результат
Гаджикаева Элина	14 б. 100% 07:00	Гаджикаева Элина	14 б. 100% 08:02	Евдокимова Анастасия	11 б. 79% 07:36	Жукова Мария	13 б. 93% 13:37	Лаврова Мария	13 б. 93% 11:48	Мухоморова Мария	14 б. 100% 05:54	Петрова Мария	14 б. 100% 05:20	Сидорова Мария	14 б. 100% 06:22
Шишканова Маша	14 б. 100% 11:05	Шишканова Маша	14 б. 100% 06:19	Тимофеева Мария	14 б. 100% 09:50	Тимофеева Мария	14 б. 100% 07:32	Тимофеева Мария	14 б. 100% 08:32	Цыганова Мария	14 б. 100% 11:14	Шишканова Маша	14 б. 100% 11:05	Шишканова Маша	14 б. 100% 11:05

Задание 1 1 б.

1. Задание 1

Учащийся: Гаджикаева Элина
Баллы: 1 из 1

Когда можно доверять письму от неизвестного отправителя?



- Никогда нельзя доверять письму от неизвестного отправителя
- Отправитель ссылается на ваших друзей
- К вам обращаются по имени
- Отправитель использует логотип авторитетной компании

Исправить Распечатать Следующее

[Отправить отзыв в ЯКласс](#)

Просмотр результатов проверочной работы (викторины).

www.yklass.ru

Результаты - Меню по кибербезопасности. Викторина.

ЯКласс

Викторина
Александрова
Григорья
48
Мой профиль
Выход

- Начало
- Справочный раздел
- Мои классы
- Вебинары
- Новости
- ТОПы
- Учебные заведения
- Предметы
- Проверочные работы
- Результаты учащихся
- Обновление
- Управление пользователями
- Подписка Я+
- ЯКлуб
- Пермиссия
- Поиск по сайту

Результат	Учащийся	по 01	по 02	по 03	по 04	по 05	по 06	по 07	по 08	по 09	по 10
		1 б.	1 б.	1 б.	2 б.	1 б.	1 б.	3 б.	1 б.	2 б.	1 б.
14 б. 100%	07:00 Гаджигодова Элана	1	1	1	2	1	1	3	1	2	1
14 б. 100%	08:02 Голово Денил	1	1	1	2	1	1	3	1	2	1
11 б. 79%	07:36 Ермаков Назар	1	1	1	2	1	1	0	1	2	1
13 б. 93%	13:37 Жабина Иван	0	1	1	2	1	1	3	1	2	1
13 б. 92%	11:48 Лудякина Илона	1	0	1	2	1	1	3	1	2	1
14 б. 100%	05:54 Макарова Алена	1	1	1	2	1	1	3	1	2	1
14 б. 100%	05:20 Рожкова Елизавета	1	1	1	2	1	1	3	1	2	1
14 б. 100%	06:22 Сидорова Ислена	1	1	1	2	1	1	3	1	2	1
14 б. 100%	08:19 Сулейманов Никита	1	1	1	2	1	1	3	1	2	1
14 б. 100%	09:50 Тарасов Михаил	1	1	1	2	1	1	3	1	2	1
14 б. 100%	07:32 Тарбуков Алексей	1	1	1	2	1	1	3	1	2	1
14 б. 100%	08:32 Теплов Артем	1	1	1	2	1	1	3	1	2	1
14 б. 100%	11:14 Шариков Олег	1	1	1	2	1	1	3	1	2	1
14 б. 100%	11:05 Шихалиева Маши	1	1	1	2	1	1	3	1	2	1

Пройди онлайн-викторину
и получи сертификат
знатока
кибербезопасности





ЯКлассная памятка по кибербезопасности



1. **Не проходи по ссылкам, не открывай файлы присланные незнакомыми людьми.** Там может быть вирус, от которого и антивирус не спасет!
2. **Не добавляй "в друзья" - всех подряд!** Помни, в интернете незнакомые люди скрывают кто они на самом деле!
3. **Доверяй интуиции!** Если общение кажется тебе странным, прекрати его.
4. **Не сообщай другим людям и подозрительным сайтам информацию о себе** (телефон, адрес, № школы, пароли, паспортные данные родителей, номера банковских карт и т. д.)
5. **Не отвечай на спам** (спам - это ненужные адресату электронные послания, рекламные письма и т. п.). Так спамер поймет, что ты используешь эту электронную почту и будет высылать еще больше спама. Необходимо пометить данное письмо, как спам в своей почтовой программе.
6. **Создавай надежные пароли.** Если тебя "взломают" можно потерять время и деньги!
7. **Не переводи деньги незнакомым людям обещающим тебе приз,** как правило это мошенники. Также если твой знакомый написал тебе через соц. сети и просит перевести ему деньги, убедись, что это действительно он, а не мошенник взломавший его учетную запись.
8. **Спроси совета у взрослых.** Всегда спрашивай взрослых, если тебе что-то непонятно в Интернете: как зарегистрироваться, какие персональные данные можно указать, по какой ссылке можно перейти и др.
9. **Не используй незнакомые флешки.** Найди в школе или на улице флешку, не стоит её использовать, т.к. она может быть заражена компьютерным вирусом и специально оставлена в публичном месте.
10. **Не будь грубияном!** Помни за "нином" человек.



 ЯКласс
БЛАГОДАРНОСТЬ



**Уважаемый учитель,
Грекова Виктория Александровна!**

Благодарим Вас

за организацию и проведение мероприятия по кибербезопасности
совместно с образовательным ресурсом “ЯКласс”,
разработанным и поддерживаемым Фондом развития интернет-инициатив
при Президенте Российской Федерации и Инновационным центром “Сколково”.



Генеральный директор
“ООО ЯКласс”
Четвериков С.А.



ООО ЯКласс

город Москва
октябрь 2021



ЯКласс

Горячая линия

8 800 600 04 15

info@yaklass.ru

Нафикова Роза Альбертовна
региональный представитель
«Якласс»
в Московской области

nafikova@yaklass.ru