Безопасная работа из дома: решения и подход «Лаборатории Касперского»

Игорь Басов
Менеджер по работе с партнерами в ПФО

Программа вебинара

Тысячи компаний по всему миру перевели сотрудников на удаленную работу (включая Microsoft, Google и «Лабораторию Касперского»).

На вебинаре мы разберем:

- Особенности удаленной работы и риски IT-безопасности.
- Простые правила, которые снизят риски
- Решения «Лаборатории Касперского» для безопасной удаленной работы

Главные риски при переходе на удаленку

1. Подключение большого количества потенциально зараженных устройств к инфраструктуре компании.
2. Рост числа удаленных соединений с офисом, часто через небезопасные сети Wi-Fi.
3. Увеличение объема трафика, который необходимо шифровать.

В чем опасность работы из дома?

Незащищенные сети Wi-Fi и 4G

- Шифровальщики
- Вредоносное ПО
- Корпоративный шпионаж

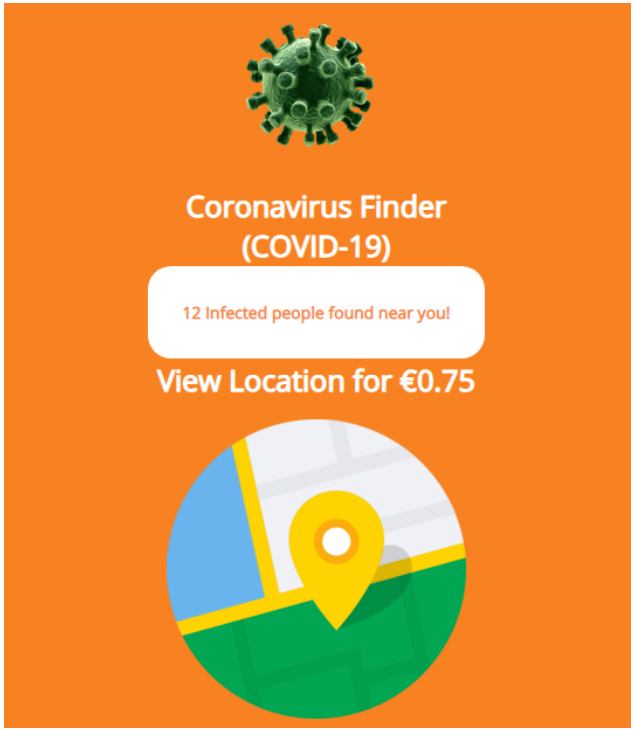
Персональные устройства (BYOD)

- Фишинг
- Децентрализованный IT-контроль
- Инвентаризация, контроль и защита мобильных устройств
- Низкопроизводительное оборудование с устаревшим ПО

Киберпреступники активизировались

Банковский троян Ginp по команде открывает веб-страницу под названием Coronavirus Finder (локатор коронавируса). На сайте предлагается узнать количество инфицированных коронавирусом рядом с вами.

Как только жертва трояна вводит платежные данные, они отправляются к мошеннику, деньги не списываются.



В период карантина перед злоумышленниками открываются дополнительные возможности, в том числе для корпоративного шпионажа, поэтому мы рекомендуем компаниям принять максимальное количество мер для того, чтобы удалённая работа была не только удобной, но и безопасной.

Дмитрий Галов, антивирусный эксперт «Лаборатории Касперского»

Как минимизировать риски

- Поставить пароли для входа в устройства
- На всех устройствах установить антивирусное ПО и включить фаервол
- Настроить VPN-доступ с двухфакторной аутентификацией
- Обновить все программы и IT-оборудование
- Зашифровать ноутбуки и смартфоны
- Сделать резервные копии ключевых данных
- Ввести ограничения по скачиванию сторонних приложений
- Проверить права доступа сотрудников и актуализировать их при необходимости
- Установить на устройства сотрудников программы, позволяющих искать эту технику в случае утери, таких как FindMyiPhone или Анти-Вор для Android
- Провести тренинг по цифровой безопасности

Защита рабочих мест

Адаптивная защита

ГИБКАЯ КОНСОЛЬ 7 В 1 ОДНА ЛИЦЕНЗИЯ –

НЕСКОЛЬКО ПРИЛОЖЕНИЙ


Kaspersky Security for Windows Server


Kaspersky Security for Mobile


Kaspersky Endpoint Security for Linux


Kaspersky Vulnerability & Patch Management


Kaspersky Endpoint Security for Windows


Kaspersky Endpoint Security for Mac


Kaspersky Security Center

И МНОГОЕ ДРУГОЕ...

ГОТОВОЕ РЕШЕНИЕ

ДЛЯ СМЕШАННЫХ СРЕД

Kaspersky Security для бизнеса

Линейка решений Kaspersky Security для бизнеса содержит несколько уровней с нарастающим функционалом. Для перехода на новый уровень не требуется переустановка защитного ПО, а для управления используется одна и та же консоль.

Total
Security для бизнеса

Расширенный
Endpoint Security для бизнеса

Стандартный
Endpoint Security для бизнеса

Защита и контроль каждого рабочего места

Уникальная адаптивная система безопасности

Включает все возможности Kaspersky Endpoint Security для бизнеса Стандартный

Максимальная защита каждого аспекта вашего бизнеса

Включает все возможности Kaspersky Endpoint Security для бизнеса Расширенный

Сравнение возможностей

Стандартный
Endpoint Security для бизнеса


Контроль программ для компьютеров


Контроль веб и устройств


Защита от угроз для мобильных устройств


Защита от программ-вымогателей


Аналитика на основе облака


Единая консоль управления


Защита для Windows, Linux и Mac


Защита серверов


Базовая поддержка SIEM (Syslog)


Управление доступом на основе ролей (базовое)

Расширенный
Endpoint Security для бизнеса


Развертывание ОС и стороннего ПО


Поиск уязвимостей и установка патчей


Расширенная поддержка SIEM (проприетарная технология)


Управление шифрованием


Адаптивный контроль аномалий


Управление доступом на основе ролей (расширенное)

Total
Security для бизнеса


Защита интернет-шлюзов


Защита почтовых серверов


Управление доступом на основе ролей (расширенное)

Контроль и защита рабочих мест

Защита

- Защита от почтовых, файловых и веб-угроз блокирует известное, неизвестное и сложное вредоносное ПО
- Защита от шифровальщиков и эксплойтов выявляет уязвимые приложения
- Восстановление системы позволяет отменить вредоносные действия шифровальщиков
- Сетевой экран блокирует неавторизованные сетевые соединения
- Анализ уязвимостей с рекомендациями по установке исправлений

Контроль и управление

- Веб-Контроль
- Контроль устройств
- Управление установкой исправлений
- Управление шифрованием

Безопасность мобильных устройств

- Мобильный антивирус
- Менеджер паролей
- Веб-Контроль и контроль функций
- Анти-Вор

Безопасность и контроль мобильных устройств сотрудников

Мобильный антивирус и защита от веб-угроз

- Защита в режиме реального времени от вирусов, вредоносных приложений и других угроз
- Блокирование фишинга и вредоносных веб-сайтов

Менеджер паролей

- Защита устройства паролем
- Поддержка Face ID и Touch ID

Анти-Вор позволяет удаленно

- Найти на карте / блокировать устройство
- Включить сирену
- Стереть данные

Ограничение активности, не связанной с работой

- Контроль программ для Android
- Контроль функций

Контроль устройств iOS

- Веб-Контроль
- Настройки прокси
- Ограничение функций (до 40 функций)

Облачные средства управления безопасностью

Kaspersky Endpoint Security Cloud

Самый простой способ защитить ваш бизнес без дополнительной нагрузки на ваши IT-ресурсы, время и финансы

Защита всех устройств

- Компьютеры и ноутбуки Windows и Mac
- Файловые серверы Windows
- Смартфоны и планшеты Android и iOS

Не нужно развертывать решение в офисе

- Облачное решение, всегда доступное на cloud.kaspersky.com
- Интуитивная консоль управления через веб-браузер

Экономия средств

- Доступна месячная подписка
- Два уровня решения на выбор:
  - Kaspersky Endpoint Security Cloud
  - Kaspersky Endpoint Security Cloud Plus

Преимущества Kaspersky Endpoint Security Cloud

- Мгновенная защита
- Отсутствие затрат на сервер администрирования
- Не требует установки обновлений
- Высвобождает ресурсы
- Экономит время для решения важных бизнес-задач

Что мы предлагаем

Надежная защита конечных устройств

- Технологии для обеспечения безопасности рабочих мест от ведущего производителя защитных решений

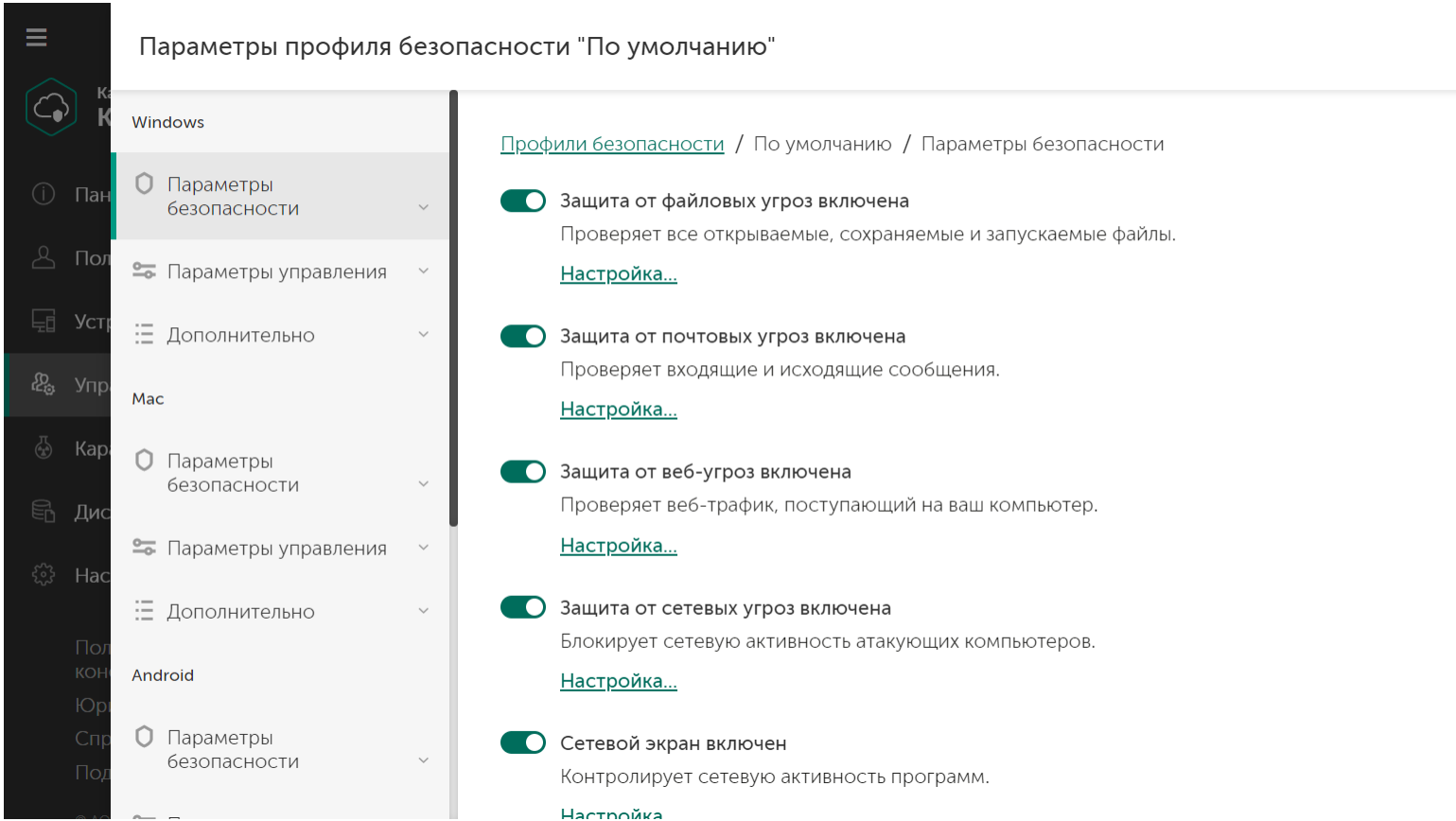
Автоматизированное решение для экономии бюджета и высвобождения ресурсов

- Не требует приобретения аппаратного или программного обеспечения. Просто зарегистрируйтесь на cloud.kaspersky.com
- Мгновенная защита и оптимальные предустановленные политики безопасности, разработанные экспертами «Лаборатории Касперского»

Безопасность удаленных сотрудников независимо от их местоположения

- Защита и контроль удаленных пользователей с помощью облачной консоли и дистанционного применения политик
- Бесплатная защита двух мобильных устройств для каждой лицензии

Дружелюбный и интуитивно понятный интерфейс



Два уровня решения на ваш выбор

	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security Cloud Plus
Безопасность		
Защита от почтовых, файловых и веб-угроз	✓	✓
Сетевой экран	✓	✓
Защита от сетевых атак	✓	✓
Защита от шифровальщиков и эксплойтов	✓	✓
Анализ уязвимостей	✓	✓
Контроль и управление		
Веб-Контроль		✓
Контроль устройств		✓
Управление шифрованием		✓
Управление установкой исправлений		✓

Уровень Plus включает важные для защиты удаленных сотрудников функции:

- Контроль устройств
  - » Контроль доступа к внешним и съемным устройствам, подключенным к компьютеру
- Веб-Контроль
  - » Контроль доступа к веб-сайтам в зависимости от их содержания и расположения
- Управление установкой исправлений
  - » Удаленное управление установкой обновлений и исправлений на корпоративных устройствах
- Управление шифрованием
  - » Удаленное шифрование устройств сотрудников с помощью встроенного шифрования Windows (BitLocker) и Mac OS (FileVault)

Готовое к работе решение

Попробуйте бесплатную 30-дневную пробную версию прямо сейчас

Создайте учетную запись на cloud.kaspersky.com

Добавьте устройства, требующие защиты

Обслуживание занимает ~15 мин. в неделю

Создайте рабочую область и разверните ПО для защиты рабочих мест

К каждому подключенному устройству автоматически применяется политика по умолчанию

И это всё! Пользователи защищены

~15 мин. в неделю на обслуживание

Повышение киберграмотности сотрудников

Сотрудники – самое уязвимое звено в корпоративной кибербезопасности

52% компаний считают, что сотрудники – это самая большая угроза кибербезопасности*

60% сотрудников хранят конфиденциальные данные на корпоративных устройствах (в том числе финансовую информацию и пр.)**

30% сотрудников признают, что сообщают коллегам учетные данные своего рабочего компьютера**

23% организаций не имеют правил или политик безопасности хранения корпоративных данных**

** По данным исследования The Cost of a Data Breach («Ущерб от утечки данных»), проведенного «Лабораторией Касперского» весной 2018 г.*
*** Sorting Out Digital Clutter In Business («Наводим порядок в цифровом пространстве»), «Лаборатория Касперского», 2019 г.*

Примеры фишинга

Чт 07.02.2019 16:28

Zhdanov <comunicazione@mediatecatoscana.it>

заказ [redacted]

Кому [redacted]

Добрый день!
Отправляю подробности заказа. Документ во вложении и тут: https://www [redacted]/documents/docs/

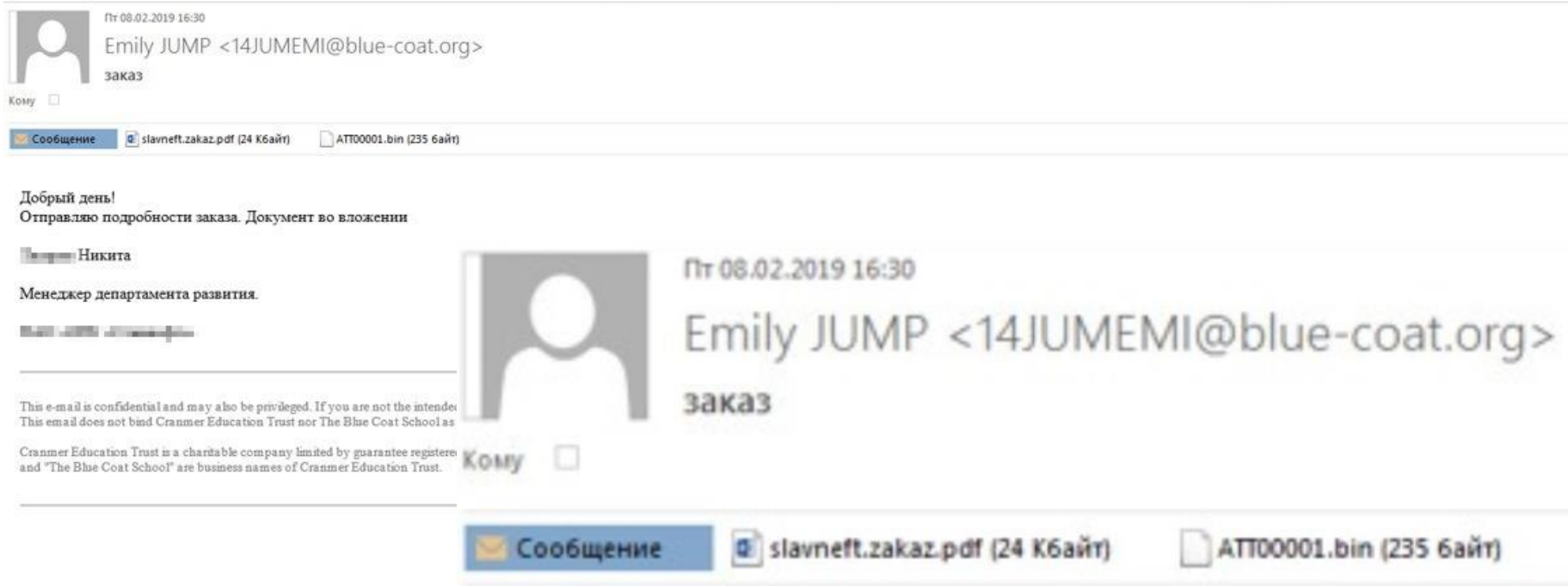
[redacted] Юрий Рудольфович

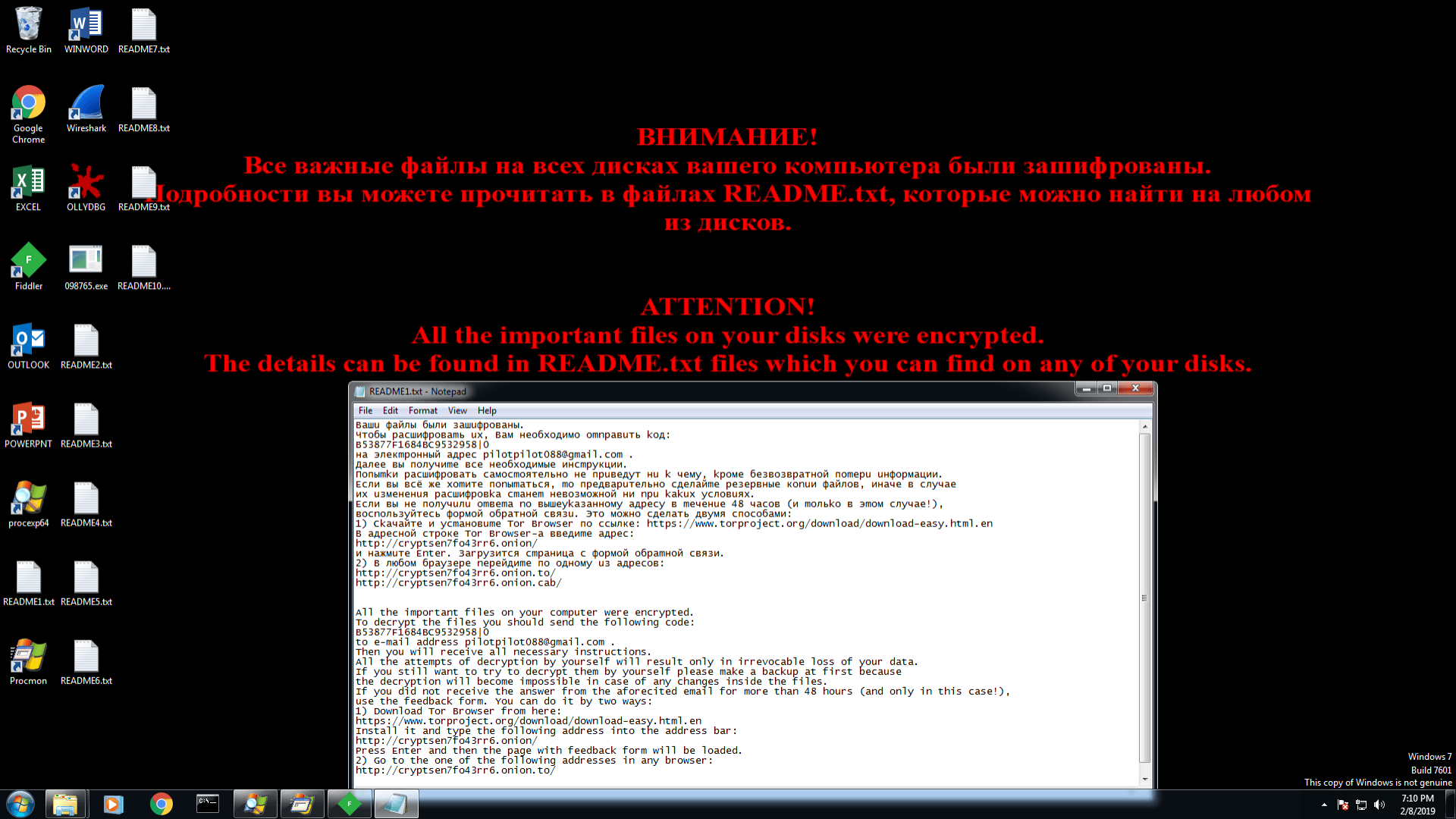
Менеджер Департамента по организационному развитию и работе с предприятиями.

ООО [redacted]

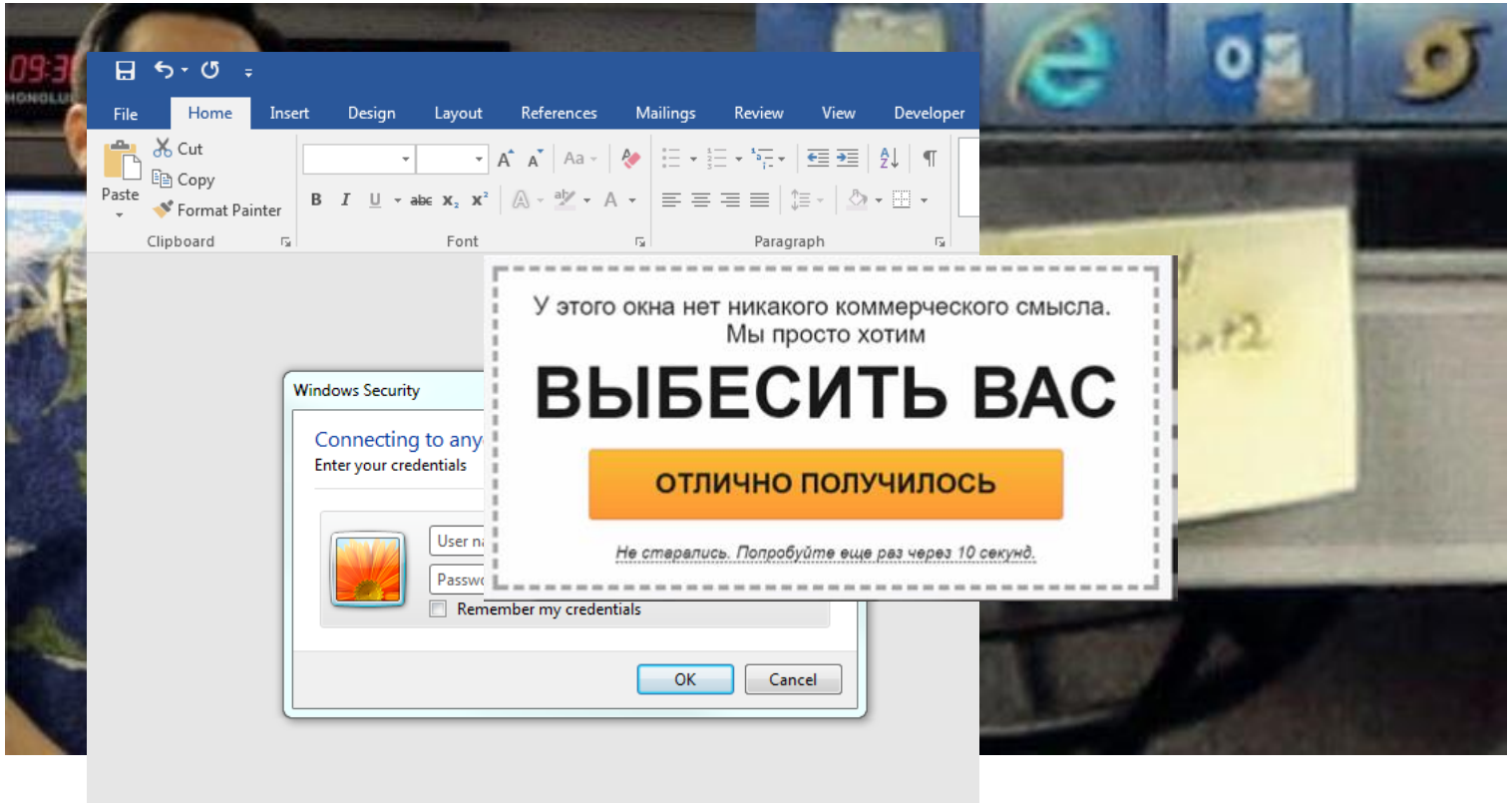
**********Проверено Kaspersky Mail Checker **********

Примеры фишинга




ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.
ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.
README1.txt - Notepad
File Edit Format View Help
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
B53877F1684BC9532958|0
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/
All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
B53877F1684BC9532958|0
to e-mail address pilotpilot088@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
Windows 7
Build 7601
This copy of Windows is not genuine
7:10 PM
2/8/2019

А что помимо фишинга?

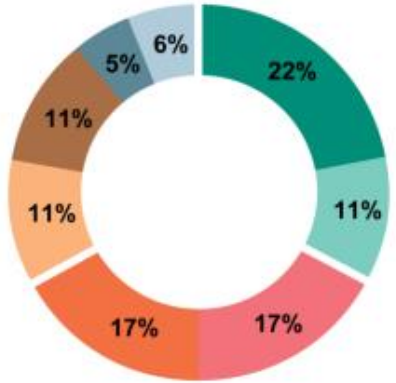


Векторы первичной компрометации

В трети инцидентов для начальной компрометации системы использовалась служба удаленного управления RDP. В большинстве

33% атак произошли вследствие небезопасных действий со стороны работников компании. Сотрудник загружал из недоверенных источников вредоносный файл и запускал его, в результате чего злоумышленники получали контроль над рабочей станцией. Следует отметить, что невозможно полностью исключить влияние человеческого фактора, однако регулярное обучение персонала основам компьютерной безопасности позволяет значительно уменьшить вероятность успешной атаки с использованием методов социальной инженерии.

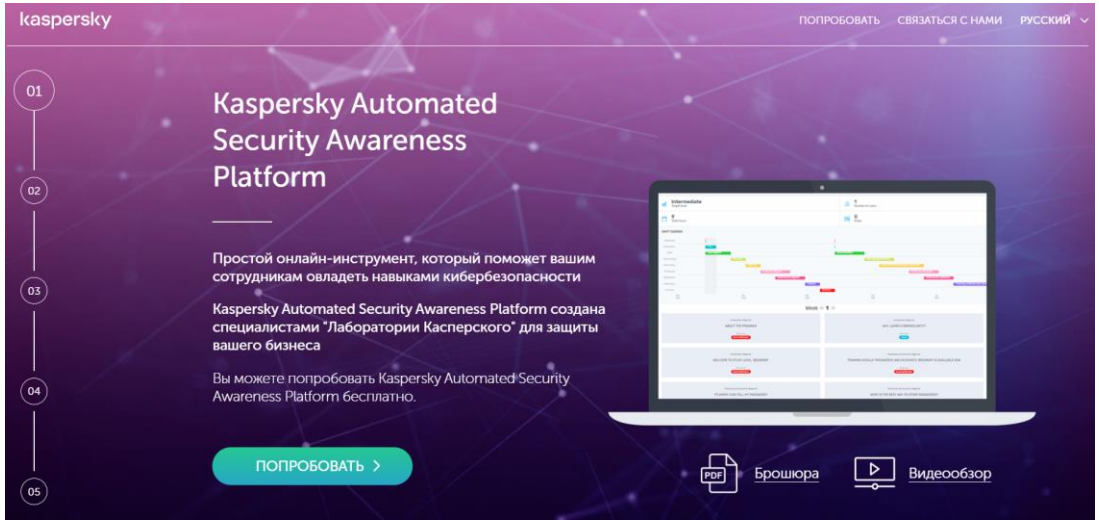
Распространённые векторы атак[5]



- Атака на RDP методом перебора
- Знание легальной учетной записи RDP
- Загрузка файла с зараженного сайта
- Загрузка вредоносного файла по ссылке в письме
- Атака на почтовый сервер методом перебора
- Эксплуатация ошибки конфигурации
- Эксплуатация уязвимости ПО
- Зараженный физический носитель

* Kaspersky Incident Response Analytics Report 2018

Kaspersky Automated Security Awareness Platform



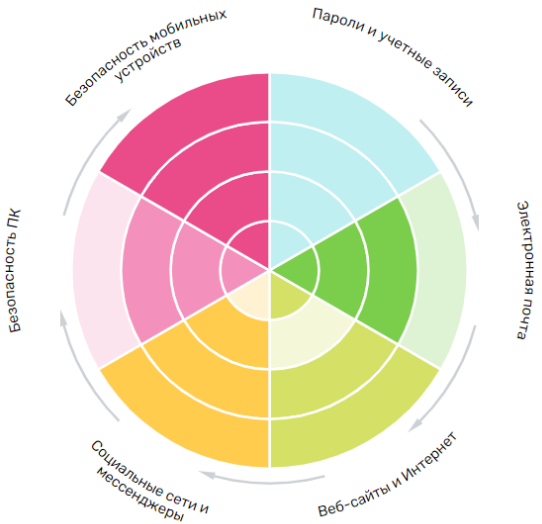
Решение, сочетающее в себе эффективность обучения и простоту управления

www.k-asap.com/ru

Содержание: только нужная информация и навыки, применимые на практике

Сотни конкретных навыков

Универсальный многоуровневый учебный план



1 занятие = не менее 1 нового навыка

- Что может угрожать моей электронной почте?
- Кому можно сообщать свой пароль от почты?
- Что делать, если вашу электронную почту взломали?
- Какие пароли следует использовать для своих почтовых сервисов?
- Почему для корпоративной и личной электронной почты нужно использовать разные пароли?
- Какие данные не стоит отправлять по электронной почте?
- На что обращать внимание, если вас просят ввести пароль от почтового аккаунта?
- Опасны ли ссылки, состоящие только из цифр?
- Все ли вложения в электронные письма стоит открывать?
- Что стоит сделать в отношении своих почтовых аккаунтов уже сегодня?

Четкая структура

Благодаря четкой структуре программы процесс обучения понятен, логичен и сбалансирован

- **Тесты перед занятиями**

для подтверждения необходимого уровня знаний и навыков

- **Интерактивные занятия**

Программа состоит из удобных коротких занятий (2–10 минут).

- **Закрепление знаний**

Напоминания не дают забыть полученные знания

- **Примеры из реальной жизни и проверочные вопросы**

помогают в обучении, позволяют закрепить знания и в целом улучшить полученные навыки

- **Имитация фишинговых атак**

для проверки изменений в поведении, а не просто усвоения знаний

План занятий

Модульный контент

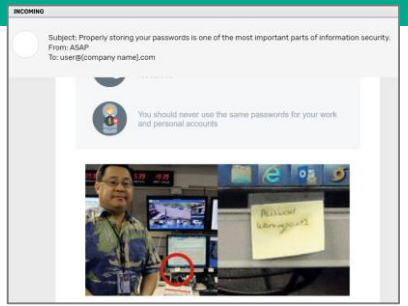
Разные элементы обучения дополняют друг друга и формируют навык

Мульти-модальный контент

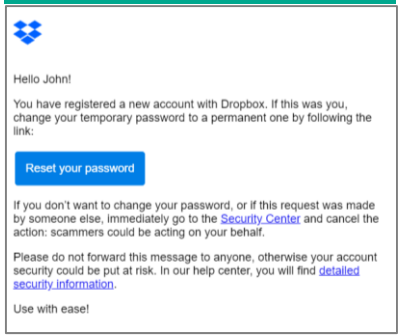
Интерактивные Занятия

Закрепление знаний

Тесты



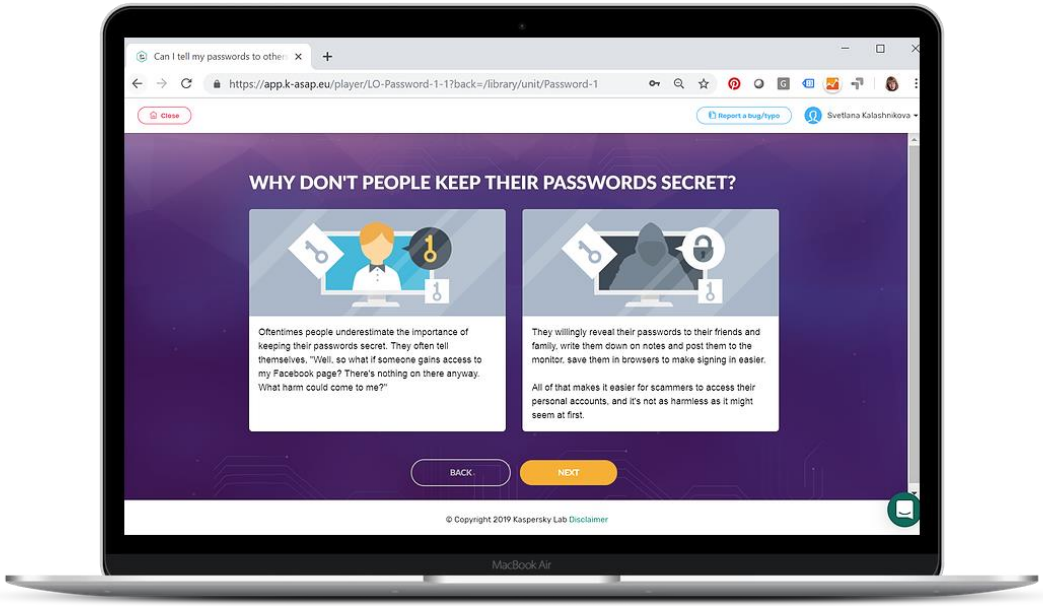
Имитация фишинговых атак

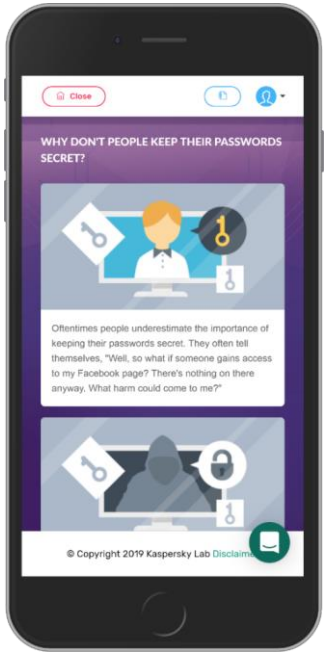


Обучение в офисе – или за его пределами на мобильных устройствах

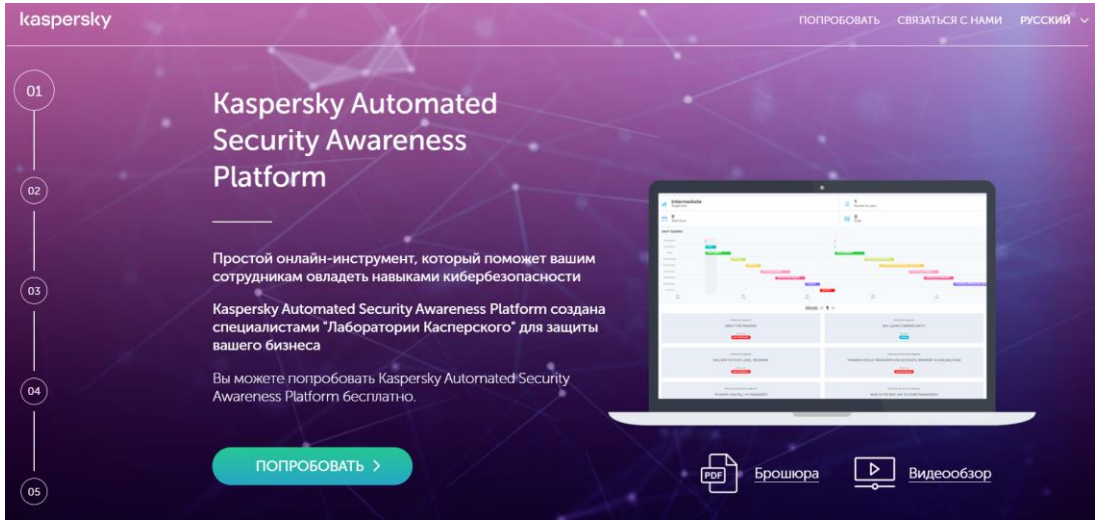
Адаптация для мобильных устройств

Адаптивный контент позволяет учиться в любое удобное время и на любом устройстве на работе или дома.





Kaspersky Automated Security Awareness Platform



Попробуйте бесплатно в течение 2 месяцев

www.k-asap.com/ru

Предложения «Лаборатории Касперского»

Предложения «Лаборатории Касперского»

- Бесплатная защита для медицинских организаций на 180 дней

http://kas.pr/SOS

Сроки проведения: 23.03.2020-23.06.2020

- Защита дополнительных узлов при продлении

Подробности у компаний-партнеров:
https://partnersearch.kaspersky.com/?b2b&locale=ru

Сроки проведения: 23.03.2020-30.04.2020

- Бесплатная пробная версия Kaspersky Security для MS Office 365 на 180 дней

https://cloud.kaspersky.com

kaspersky

Бесплатная защита для медицинских учреждений

«Лаборатория Касперского» бесплатно предоставит медицинским учреждениям по всему миру защиту сроком на 180 дней.

Отправить заявку

Медицинские учреждения сегодня мобилизуют все силы, во многих странах нагрузка на систему здравоохранения серьёзно возросла. В такое время вопросы обеспечения стабильности работы медицинского оборудования и бесперебойного доступа к информации, а также защиты персональных данных пациентов становятся особенно критичными.

«Лаборатория Касперского» бесплатно предоставит медицинским учреждениям по всему миру лицензии на 180 дней. Речь идёт о корпоративных продуктах для защиты конечных устройств и облачных инфраструктур:

- Kaspersky Endpoint Security для бизнеса Расширенный
- Kaspersky Security для виртуальных и облачных сред
- Kaspersky Endpoint Security Cloud Plus
- Kaspersky Security для Microsoft Office 365

Остались вопросы?

Igor.basov@kaspersky.com

kaspersky