KASPERSKY lab

Kaspersky Security Awareness (Программа повышения осведомленности)

Игрофицированная программа обучения для всех категорий сотрудников

www.kaspersky.ru

#ИстиннаяБезопасность

Эффективный метод укрепления корпоративной культуры интернет-безопасности

Более 80% всех киберинцидентов связаны с человеческим фактором. Предприятия тратят огромные средства на восстановление ресурсов после инцидентов безопасности, вызванных действиями сотрудников. Однако традиционные программы обучения, призванные предотвращать такие нарушения, недостаточно эффективны. Они информируют, но не мотивируют. Программы повышения осведомленности «Лаборатории Касперского» не только дают знания, но и формируют правильное поведение.

Непреднамеренные действия сотрудников – причина большинства корпоративных инцидентов кибербезопасности.

- В 2015 г. компания IBM сообщила, что процент внутренних нарушений безопасности, вызванных ошибками сотрудников, превысил 95%[1].
- В 2015 г. 75% крупных организаций и 31% небольших компаний Великобритании пострадали от атак, связанных с человеческим фактором[2].
- В среднем финансовый ущерб от одного инцидента, связанного с небрежностью пользователей, составляет для крупного бизнеса 1,2 млн долл. США[3].
- Средний ущерб от фишинговой атаки может достигать 400 долл. на сотрудника в год (без учета прочих типов кибератак)[4].

Как показывают исследования и опросы, большинство существующих программ повышения грамотности в сфере ИБ недостаточно эффективны. Причин такого положения дел несколько:

- Пользователям скучно читать описания политик и техническую документацию, термины не всегда понятны, а описания атак вызывают скепсис. Упор делается на запреты, а не на примеры того, как нужно поступать.
- У сотрудников отсутствует мотивация к обучению (они не допускают, что могут стать мишенями злоумышленников).
- Пользователи видят в отделе ИБ помеху в работе, а не защитников, и постоянно пытаются обойти установленные меры безопасности.
- Кроме того, сложно оценить результат тренинга по осведомленности. Обычно учитывается только число пользователей, прошедших обучение.

Преимущества программы

«Лаборатория Касперского» предлагает тренинги по информационной безопасности для сотрудников всех уровней.

Kaspersky Security Awareness адаптируется в соответствии с потребностями любой организации.

- **Наши курсы не только дают знания, но и закладывают основы безопасного поведения:** при обучении используются игровой подход, практические занятия, имитация атак и т. д. Это позволяет формировать устойчивые привычки и укреплять кибербезопасность в долгосрочной перспективе.

- Для разных категорий сотрудников **формируются разные навыки**. Высшее руководство, линейные руководители/менеджеры среднего звена, IT-специалисты и рядовые специалисты — все эти группы сотрудников обучаются разным навыкам с учетом их должностных обязанностей.
- Большинство курсов проходят в онлайн-формате, поэтому формат позволяет и отделу ИБ, и отделу кадров **легко отслеживать успеваемость пользователей и контролировать ход обучения**.
- В основе курсов – **богатый опыт «Лаборатории Касперского» в области кибербезопасности и разработки защитных решений**.

KIPS – игра, которая закладывает понимание стратегии ИБ

Игра Kaspersky Interactive Protection Simulation (KIPS) предназначена для руководителей компаний, корпоративных экспертов по кибербезопасности и сотрудников IT-отделов. Цель тренинга: повысить осведомленность о рисках и проблемах безопасности, связанных с использованием современных компьютерных систем, а также продемонстрировать влияние киберугроз на результаты бизнеса.

На время игры участники погружаются в симулированную среду, где им предстоит справиться с рядом неожиданных киберугроз. При этом им необходимо не только отражать атаки, но также увеличивать прибыль компании и сохранять ее репутацию. Для этого им нужно, совместно с другими участниками команды, выстроить оптимальную стратегию кибербезопасности, которая эффективна и против существующих, и против будущих угроз.

В ответ на происходящие события команда-участник выбирает действия, которые определяют дальнейшее развитие сценария, а в конечном итоге — размер прибыли, которую получит или не получит «предприятие». Действуя в условиях меняющейся обстановки и неполной информации, участники учатся расставлять приоритеты, принимать решения и учитывать разные точки зрения. Таким образом, создается приближенная к жизни ситуация: в основе каждого сценария лежат события, которые вполне могут произойти в реальности.

Преимущества KIPS:

- Интересная, увлекательная и динамичная игра (2 часа).
- Способствует обучению командной работе.
- Состязательность способствует проявлению инициативы и развитию аналитических навыков.
- Формат игры упрощает понимание принципов IT-безопасности.

«KIPS помогает понять, насколько сильно в случае будущих инцидентов безопасности вы будете благодарны самим себе за некоторые простейшие, базовые стратегические решения – например, проведение аудита безопасности, обучение сотрудников, смену паролей или установку патчей».

Марк Дженкинс – Совет Катара по информационно-коммуникационным технологиям (ICT Qatar)

Доступные сценарии (онлайн и офлайн)

Корпорация	Защита предприятия от программ-вымогателей, целевых атак и нарушений безопасности автоматизации.
Банк	Защита финансовых учреждений от специализированных целевых атак, направленных на банкоматы, управляющие серверы и бизнес-системы.
Электронные госуслуги	Защита государственных электронных ресурсов от атак и эксплойтов.
Промышленная компания	Защита АСУ ТП и критически важной инфраструктуры. Существует два варианта сценария – «Электростанция» и «Станция водоочистки».
Транспорт	Защита логистической компании от серии кибератак, включая целевую атаку, проникновение инсайдера, ошибку Heartbleed.

Каждый сценарий построен вокруг наиболее актуальных для данной отрасли векторов угроз. Это позволяет выявлять и анализировать типичные ошибки в отношении стратегии кибербезопасности и реагирования на инциденты.

Игровые тренинги Kaspersky Cybersafety Management Games

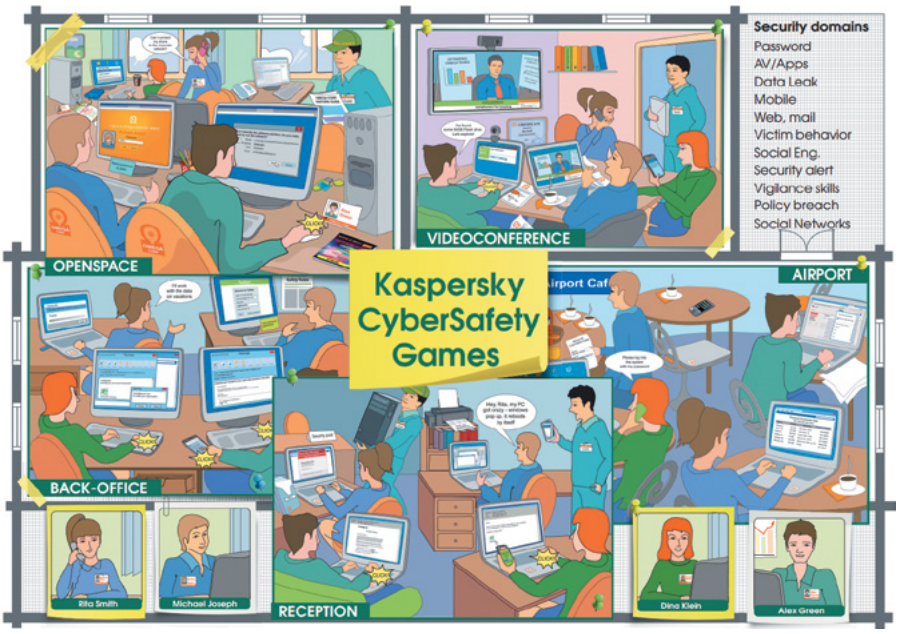
Kaspersky CyberSafety Games – это интерактивный мастер-класс, который включает компьютерные занятия и уроки под руководством инструктора. Тренинг показывает линейным руководителям всю важность кибербезопасности на их уровне ответственности. Помимо создания необходимых знаний и компетенций, игровой курс помогает выработать правильное отношение к поддержанию безопасной рабочей среды во всем подразделении.

Все больше организаций принимают меры по защите от киберугроз, внедряя системы IT-безопасности и обучая сотрудников правильному поведению. Но достаточно ли этого?

- Действительно ли знания, полученные в процессе обучения, делают поведение пользователей более обдуманным? Или на сотрудников влияет что-то другое?
- Обязательно ли жертвовать эффективностью работы ради поддержания должного уровня безопасности?
- Всегда ли специалисты отдела ИБ ощущают, что у них достаточно ресурсов для обучения многочисленных сотрудников основам правильного поведения в Сети?

Без помощи руководства подразделений невозможно разрешить эти вопросы и обеспечить кибербезопасность организации, сохранив высокую эффективность ее работы. Ведь именно линейные руководители, а не сотрудники отдела ИБ, ежедневно взаимодействуют с рядовыми сотрудниками и принимают важные для бизнеса решения. Чтобы построить надежную систему защиты, необходимо сделать соображения кибербезопасности неотъемлемым элементом принятия повседневных решений.

Игровые тренинги CyberSafety Management Games для руководителей дают необходимые знания, а также развивают нужные компетенции и правильное отношение к кибербезопасности, без которых невозможно обеспечить безопасную работу их подразделений.



Что получают менеджеры по итогам тренинга:

- **Понимание.** Внутреннее принятие методов кибербезопасности как важного и одновременно не слишком сложного набора действий.
- **Новое отношение к кибербезопасности.** Взгляд на повседневные рабочие процессы через призму кибербезопасности.
- **Принятие решений с учетом кибербезопасности.** Отношение к кибербезопасности как к неотъемлемой составляющей бизнес-процессов.
- **Мотивация к применению полученных знаний.** Умение влиять на сотрудников, отвечать на их вопросы по ИБ и давать полезные советы.

Этот игровой тренинг также можно лицензировать как программу для корпоративных обучающих центров – в таком случае компания сможет проводить неограниченное число тренингов силами внутренних тренеров. Ключевые преимущества корпоративной лицензии:

- Простота подачи материала – тренерам не обязательно быть экспертами в области кибербезопасности.
- Простота планирования занятий – для коротких модулей найдет время даже самый занятой сотрудник, а компании не нужно составлять график обучения ориентируясь на доступность тренеров «Лаборатории Касперского».
- Возможность кастомизации тренинга под политики компании и ее процессы.

Платформа обучения навыкам закладывает основы общекорпоративной кибергигиены

Для обеспечения кибербезопасности важно не только расширять знания сотрудников, но и формировать у них нужные навыки. Именно поэтому онлайн-платформа обучения навыкам – ключевой компонент программы повышения осведомленности. Она помогает пользователям освоить разные сценарии и ситуации, получить больше знаний и понять, как определять и реагировать на распространенные киберугрозы. Онлайн-обучение позволяет практиковаться и учиться на интерактивном портале.

Интерактивные обучающие модули

- Короткие и увлекательные
- Упражнения с немедленной обратной связью
- Закрепление навыков с помощью автоматической корректировки процесса обучения в соответствии с результатами выполнения предыдущих заданий
- Более 25 модулей, охватывающих все области IT-безопасности

Оценка знаний

- Включает выбранные заранее или случайные тесты, причем сам заказчик может назначать тематику вопросов и длину теста
- Охватывает разные сферы IT-безопасности
- Обширная библиотека вопросов и механизм рандомизации исключают списывание

Имитация фишинговых атак

- Три типа фишинговых атак разной сложности, основанные на реальных событиях
- При каждом открытии «фишингового» сообщения игрок получает возможность обучиться новым навыкам и закрепить их
- Настраиваемые шаблоны
- Автоматическое назначение обучающих модулей для тех, кто не справился с имитированной атакой

На июнь 2017 г. платформа доступна на 30 языках.

С помощью платформы онлайн-обучения и «Практического руководства» от «Лаборатории Касперского» клиенты смогут создать и внедрить эффективный, долгосрочный и контролируемый план обучения в области ИБ с постепенным переходом от более простых задач к более сложным. Широкий тематический охват курса позволяет обучать пользователей в соответствии с ландшафтом угроз и их исходными навыками.

Интерактивная демонстрация находится по адресу http://www.kaspersky.ru/enterprise-security/cybersecurity-awareness/demo/ (на англ. языке).

Отчеты и анализ

- Платформа предоставляет статистику для всей организации сразу, а также для каждого подразделения, должности и сотрудника индивидуально
- Платформа контролирует навыки и скорость обучения каждого сотрудника
- Кроме того, она поддерживает экспорт данных в разных форматах, а также может интегрироваться в систему дистанционного обучения (LMS) клиента

Всесторонняя оценка

При оценке культура безопасности рассматривается с разных точек зрения.

- Организационный уровень (уровень руководства)
- Персональный уровень (уровень сотрудников)
- Знания в области ИБ
- Система кибербезопасности как непрерывно действующий процесс

Формат обучения

Обучение проходит онлайн: нужны только доступ в интернет или к корпоративной СДО (LMS) и браузер Chrome. Все модули состоят из короткой теоретической части, практических советов и 7–10 упражнений: каждое позволяет отработать определенный практический навык и учит использовать инструменты и защитное ПО в повседневной работе.

Рекомендуемый темп: модуль в неделю, то есть около 45 минут. Таким образом, курс будет успешно завершен через 1,5 месяца, причем каждый сотрудник потратит на него 4–5 часов.

Мы рекомендуем обучение всем IT-специалистам в организации, в первую очередь работникам службы IT-поддержки и системным администраторам, но также он будет полезен и специалистам других отделов – в частности, всем, кто имеет права локального администратора на своей рабочей станции.

Обучение IT-специалистов навыкам поддержания кибербезопасности (Cybersecurity for IT Online)

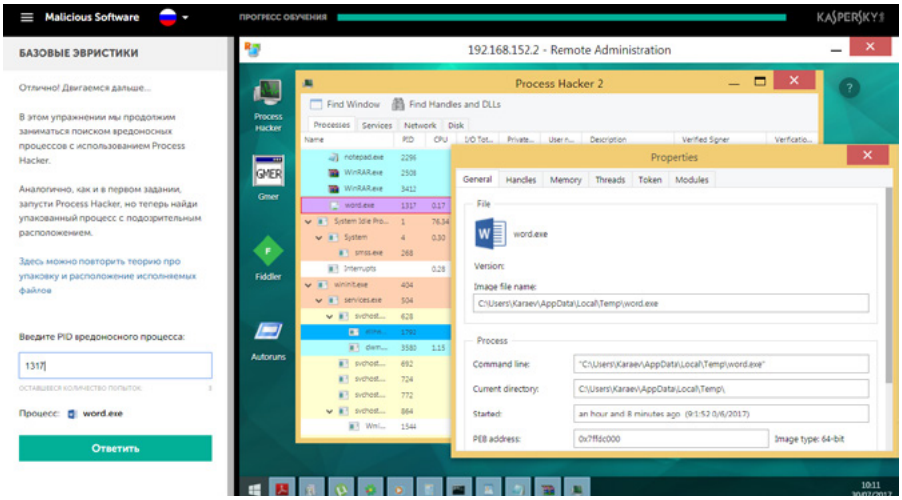
Стандартные программы повышения осведомленности не затрагивают IT-профессионалов, службу IT-поддержки и других технических сотрудников. Базовых программ осведомленности для них недостаточно, однако делать из технических специалистов полноценных экспертов по кибербезопасности за корпоративный счет слишком дорого, долго, рискованно – другими словами, не нужно.

«Лаборатория Касперского» представляет программу обучения, предназначенную специально для IT-специалистов, которая учитывает их высокий уровень технической осведомленности и специфику их рабочих обязанностей.

Первая линия кибероборонs

«Лаборатория Касперского» выпустила онлайн-курс для обучения корпоративных IT-специалистов общего направления. Курс состоит из шести модулей:

- Основные практические сведения о киберугрозах
- Вредоносное программное обеспечение
- Потенциально нежелательные программы и файлы



- Основы расследования инцидентов
- Реагирование на фишинг и разведка в открытых источниках
- Корпоративная безопасность: контроль уязвимостей и защита серверов

Этот курс дает IT-специалистам практические навыки по распознаванию возможной атаки при изучении безобидного на первый взгляд инцидента, а также навыки по сбору данных для передачи службе IT-безопасности. Также обучение мотивирует IT-специалистов искать и находить признаки кибератаки и помогает понять их задачи в качестве первой линии кибероборонны.

Оценка культуры кибербезопасности

В ходе оценки мы анализируем поведение сотрудников всех уровней с точки зрения разных аспектов кибербезопасности и показываем их отношение к этим аспектам.

Полученный отчет поможет отделу ИБ обратить внимание на проблемные области и правильно расставить приоритеты во внутренней и внешней деятельности отдела. Такими областями могут быть культура и обучение, внутренний PR и обмен информацией, а также другие вопросы сотрудничества при работе в компании.

Корпоративная культура безопасности включает и области, которые могут оцениваться только для всей компании одновременно. По результатам оценки можно предметно обсудить роль и место кибербезопасности в обеспечении эффективной работы организации.

- Ответственное отношение к кибербезопасности (восприятие безопасности и политик).
- Управление рисками (руководство, обратная связь, улучшения).
- Следование принципам кибербезопасности (отношение к мерам безопасности и соответствующее поведение).
- Влияние на бизнес (баланс между безопасностью и эффективностью работы компании).

Обратите внимание, что оценка культуры кибербезопасности не равнозначна оценке уровня защищенности компании (не является аудитом IT-безопасности) и ничего не говорит об эффективности работы отдела ИБ.

Отчет о культуре кибербезопасности показывает, как обычный сотрудник воспринимает кибербезопасность; что он думает о культуре, привычках, ежедневных процедурах и других аспектах, связанных с кибербезопасностью; каковы его индивидуальные взгляды на те или иные принципы защиты компании от киберугроз. Такое восприятие формируется на основе всей совокупности практик, принятых в компании, а не только в результате работы отдела информационной безопасности или отдела управления рисками.

Оценка проводится в виде онлайн-опроса на базе облачной платформы. Опрос одного сотрудника занимает около 15 минут; обычно для анкетирования всей организации требуется около 2 недель.

Клиент получает обобщающий отчет по результатам опроса.

Формирование культуры кибербезопасности

Таким образом, для развития культуры кибербезопасности в компаниях разработана серия тренингов, формирующих осведомленность при помощи игровых технологий на всех уровнях организационной структуры под руководством отделов безопасности и работы с персоналом.

Комплексный подход, простая и понятная подача материала

- Широкий круг проблем безопасности
- Отработка действий в повседневной обстановке
- Интересный процесс обучения
- Практические упражнения
- Язык, понятный не только IT-специалистам
- Подробные инструкции и методологическая поддержка

Преимущества для бизнеса

93%
Вероятность применения полученных знаний в повседневной работе

10
Сокращение количества инцидентов до 10 раз

50-60%
Снижение рисков кибербезопас-ности в денежном выражении

30
Более чем 30-кратная окупаемость вложений в повышение осведомленности

1 IBM 2015 Cyber Security Intelligence Index (Аналитический обзор киберугроз за 2015 г. компании IBM).

2 2015 Information Security Breaches Survey (Исследование инцидентов безопасности за 2015 г.), правительство Великобритании совместно с компаниями InfoSecurity Europe и PwC.

3 Humans Factor in IT security: How Employees are Making Businesses Vulnerable from Within, «Лаборатория Касперского» и B2B International, 2017 г.

4 Расчеты сделаны на основе исследования Ponemon Institute, «Cost of Phishing and Value of Employee Training» (Ущерб от фишинга и значимость обучения сотрудников), август 2015.

Решения для крупного бизнеса: http://www.kaspersky.ru/enterprise-security/
Kaspersky Security Awareness: **http://www.kaspersky.ru/enterprise-security/cybersecurity-awareness/**

www.kaspersky.ru
#ИстиннаяБезопасность