Если безопасность – то всесторонняя

Тренинги Kaspersky Security Awareness – универсальный ответ на многообразие киберугроз.

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Security Awareness Training

В 90%[1] случаев именно человеческая ошибка становится причиной инцидента безопасности. Как снизить эту цифру?

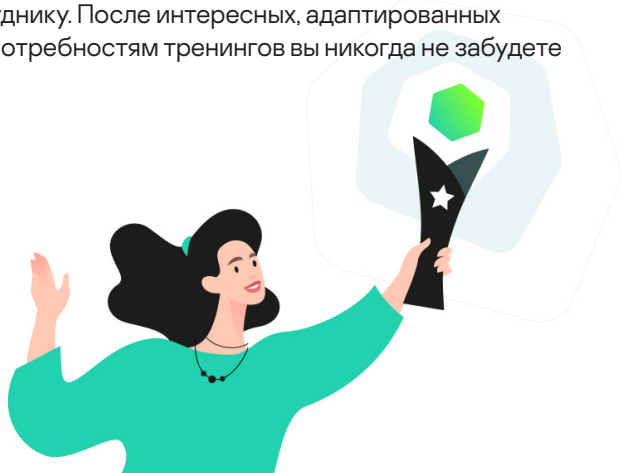
Все сотрудники обладают разными навыками и рабочими привычками, но любой может стать слабым звеном в системе защиты вашей организации.

Даже базовые навыки в сфере кибербезопасности помогут вашим сотрудникам защитить компанию от кибератак. Злоумышленникам намного проще использовать неосведомленность сотрудников об угрозах, чем писать сложный код для взлома систем кибербезопасности. К 17 января 2021 года компания Google обнаружила 2 145 013[2] фишинговых сайтов, эксплуатирующих человеческий фактор. А если учесть, что средний финансовый ущерб от утечки данных для крупного предприятия составляет 1 195 000 долларов США[3], потребность в тренингах по кибербезопасности становится очевидной.

Несмотря на это, лишь около 60%[4] организаций проводят для сотрудников обязательные тренинги для повышения осведомленности о киберугрозах. А в 10%[4] такие тренинги не являются обязательными.

Мы в «Лаборатории Касперского» считаем, что проблема заключается в отсутствии подходящей технологии обучения. Изменить поведение сотрудников непросто. Большинство очных или дистанционных тренингов однобоки и не имеют долгосрочного эффекта.

Тренинги по информационной безопасности Kaspersky Security Awareness решают эти проблемы. Мы предлагаем широкий спектр решений, которые охватывают все потребности организаций, связанные с безопасностью. Используя новейшие методы и технологии, мы обеспечиваем развитие навыков, необходимых каждому сотруднику. После интересных, адаптированных к конкретным потребностям тренингов вы никогда не забудете изученное.



[1] Sorting out a Digital Clutter («Наводим порядок в цифровом пространстве»), «Лаборатория Касперского», 2019 г.

[2] Статистика фишинговых атак, Tessian, 2020 г.

[3] Данные «Лаборатории Касперского», 2019 г.

[4] Статистика тренингов по информационной безопасности, Mimecast, 2018 г.

Одно гибкое решение для всех

52%[5] компаний

считают, что действия сотрудников представляют самую большую угрозу кибербезопасности

60%[6] сотрудников

хранят конфиденциальные данные на корпоративных устройствах (в том числе финансовую информацию, электронную почту и пр.)

Наши тренинги помогают сделать рабочую среду в вашей организации безопаснее.

Мы предлагаем тренинги для сотрудников любого уровня, от высшего руководства и IT-специалистов до рядовых работников. Тренинги адаптируются к потребностям конкретной организации и отдельных участников в области кибербезопасности. В них используются различные методы вовлечения, от построения учебных занятий аналогично работе с живым преподавателем до игрового подхода, который задействует естественное желание узнавать новое, совершенствоваться и соревноваться с коллегами. Это лучший способ мотивировать сотрудников повысить осведомленность в области кибербезопасности.

И так как тренинги Kaspersky Security Awareness проводит «Лаборатория Касперского», которая знает о безопасности все, вы можете быть уверены, что получите именно те навыки, в которых нуждаетесь. Мы поможем вам изменить поведение сотрудников и создать безопасную рабочую среду без лишних ограничений.

[5] Исследование The Cost of a Data Breach («Ущерб от утечки данных»), «Лаборатория Касперского», весна 2018 г.

[6] Sorting out a Digital Clutter («Наводим порядок в цифровом пространстве»), «Лаборатория Касперского», 2019 г.

Для высшего руководства

58%[8] руководителей высшего звена

считают, что обеспечивать IT-безопасность слишком сложно

42%[9] заявляют,

что для них IT-безопасность имеет низкий приоритет

60%[10] IT-директоров

считают, что высшее руководство – наиболее вероятная цель для кибератаки

76%[11] генеральных директоров

признают, что обходили протоколы безопасности, чтобы быстрее выполнить задачу

28%[12] руководителей высшего звена

просили IT-службы сделать для них исключение в протоколах безопасности своей организации

Командные игры и тренировки с имитацией атак меняют отношение к кибербезопасности

Если вы организуете тренинги по кибербезопасности для сотни сотрудников, но забываете о руководителях высшего звена, экспертах по бизнес-системам и IT-специалистах, то это не принесет большой пользы.

Именно руководители компании выделяют средства на тренинги для сотрудников, которые помогут получить навыки для защиты организации. В различных организациях доля сотрудников, защищенных программами кибербезопасности, колеблется от 85% до всего 56%[7].

Понимать, какой финансовый и репутационный ущерб могут нанести различные нарушения безопасности – от использования общих паролей до фишинговых атак, – должны люди на всех уровнях организации, начиная с высшего руководства.

Мотивирующие и эффективные тренинги

«Лаборатория Касперского» поможет вашему руководству лучше понять связь между кибербезопасностью и эффективностью бизнеса. Например, **курс для руководителей высшего звена** помогает главам и топ-менеджерам компаний усвоить основы кибербезопасности под руководством инструктора. В результате они начинают лучше разбираться в киберугрозах и способах защиты от них.

Вместе с **тренингом для руководителей высшего звена** (а также отдельно от него) мы предлагаем интерактивные игры для коллектива, например симулятор защиты **Kaspersky Interactive Protection Simulation (KIPS),** которые помогают применить полученные знания на практике. Симулятор разработан специально для лиц, принимающих решения. Это интерактивная командная игра, которая меняет отношение к кибербезопасности и помогает наладить взаимодействие между сотрудниками на разных уровнях организации.

[7] Отчет о кибербезопасности, Accenture, 2020 г.

[8] Исследование Trouble at the Top («Проблемы кибербезопасности на высшем уровне руководства»), MobileIron

[9, 10, 11] Cybersecurity's Greatest Insider Threat Is In The C-Suite («Главная внутренняя угроза кибербезопасности исходит от высшего руководства»), Forbes, 2020 год.

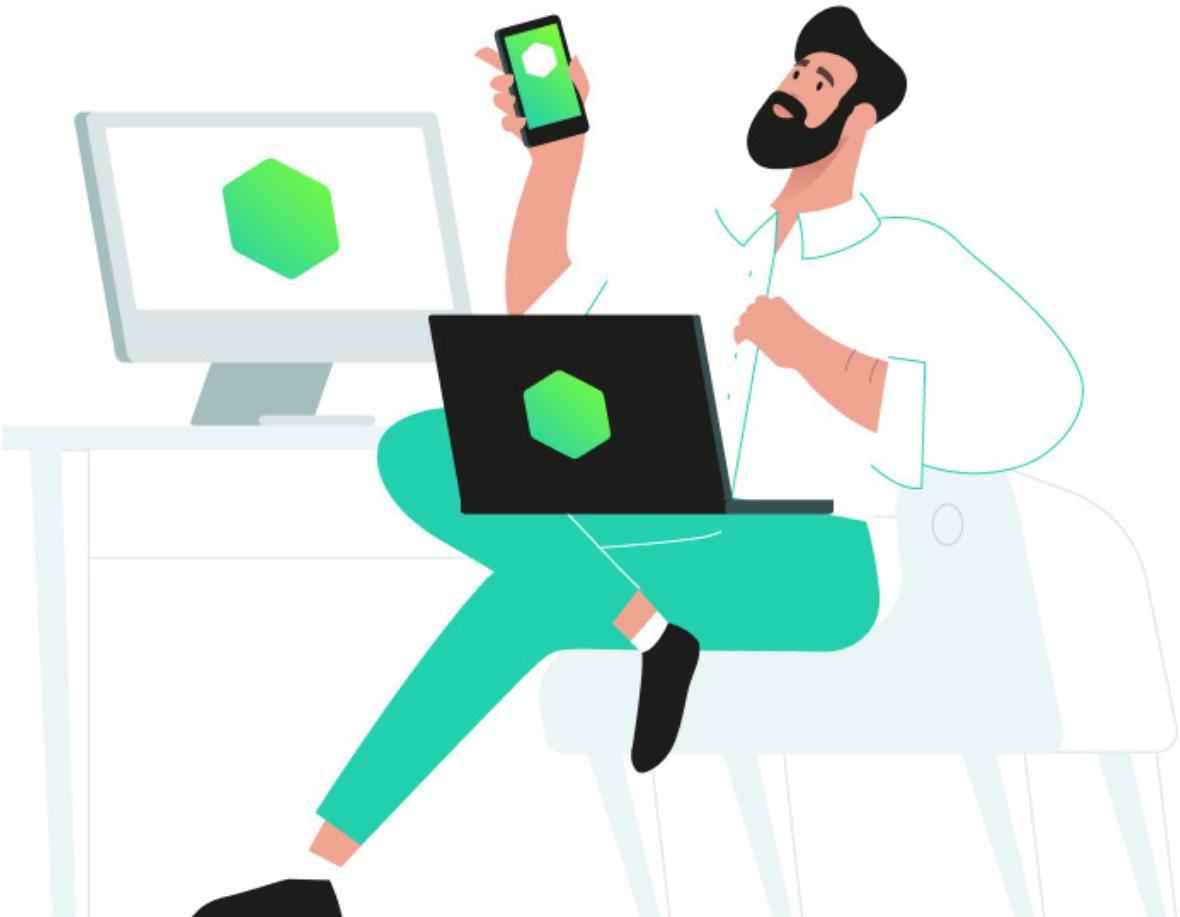
[12] Исследование Trouble at the Top («Проблемы кибербезопасности на высшем уровне руководства»), MobileIron

Во время этого тренинга руководители должны предугадывать последствия атаки, реагировать в установленных временных и бюджетных рамках и адаптироваться к сценариям, разработанным «Лабораторией Касперского» для различных отраслей: от банковского и промышленного сектора до транспорта и коммунального хозяйства.

В дополнение к Kaspersky Interactive Protection Simulation мы предлагаем **игровые тренинги** для линейных менеджеров и руководителей среднего звена, которые помогают им осознать важность кибербезопасности для принятия повседневных решений, придерживаться ее правил самим и требовать этого от других.

Наши уникальные методики позволят руководству вашей компании полностью погрузиться в процесс.

Тренинг Kaspersky Interactive Protection Simulation: снимок экрана. Электростанция в виртуальной реальности.

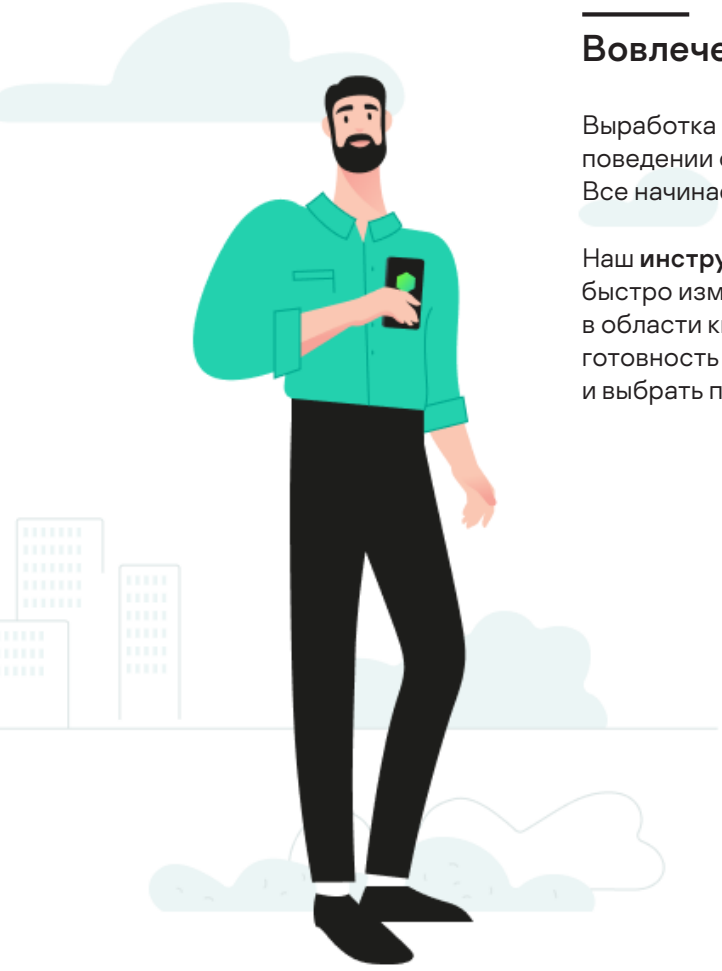


Для всех сотрудников

42%[13]
респондентов
из компаний со штатом свыше 1000 человек отметили, что большинство тренингов, которые они проходили, оказались бесполезными и неинтересными

В 75 странах
применяются наши тренинги по кибербезопасности

Более 500 000
сотрудников,
прошедших тренинги Kaspersky Security Awareness, помогают обеспечивать безопасность своих организаций, используя полученные навыки



Персонализированные тренинги и закрепление навыков

Организации заинтересованы в развитии и закреплении у большинства сотрудников навыков, которые они смогут рефлекторно применять в случае потенциальной угрозы кибербезопасности.

Однако существует два препятствия для этого: люди, как правило, не хотят менять свои привычки, а большая часть тренингов не может увлечь участников и, как следствие, развить их навыки.

«Лаборатория Касперского» устраняет эти препятствия и проводит более эффективные, интересные и простые в организации тренинги, опираясь на более чем 20-летний опыт в области кибербезопасности и знание передовых методик.

Вовлечение с начала тренинга

Выработка устойчивых изменений в кибербезопасном поведении сотрудников требует времени.
Все начинается с определения потребностей персонала.

Наш **инструмент оценки в игровом формате** помогает быстро измерить текущий уровень навыков сотрудников в области кибербезопасности. Вы можете определить готовность вашей компании противостоять киберугрозам и выбрать подходящий тренинг «Лаборатории Касперского».

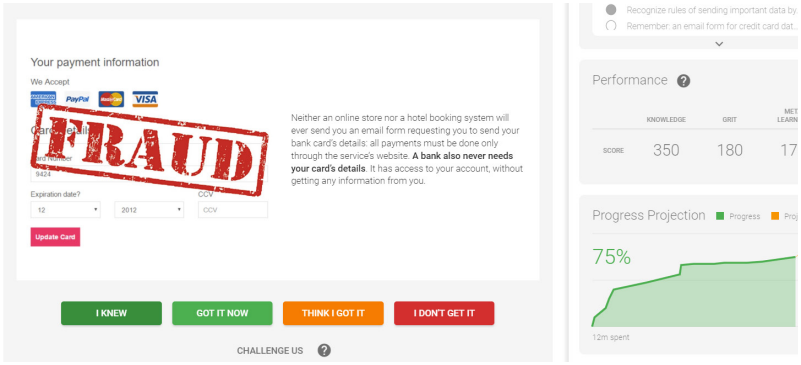
[13] The Digital Talent Gap («Нехватка специалистов по работе с цифровыми технологиями»), Capgemini

Адаптивные тренинги

В курсе Kaspersky Adaptive Online Training (KAOT) для подбора материалов к каждому занятию и для каждого пользователя используется адаптивный подход.

Kaspersky Adaptive Online Training – уникальный тренинг для развития более 300 навыков в сфере кибербезопасности. В нем используется научный подход, гарантирующий закрепление привычек безопасного поведения в рабочей среде.

В процессе тренинга отслеживается прогресс учащихся – содержание тренинга формируется в зависимости от того, на какие вопросы участник отвечает правильно, и его уверенности в приобретенных знаниях.



Тренинг Kaspersky Adaptive Online Training: снимок экрана

Для IT-специалистов широкого профиля

Тренинг полностью онлайн:

участникам нужно лишь подключение к интернету

4 модуля

с кратким обзором теории и практическими рекомендациями

4–10 упражнений

для закрепления конкретных навыков и использования защитных инструментов и ПО

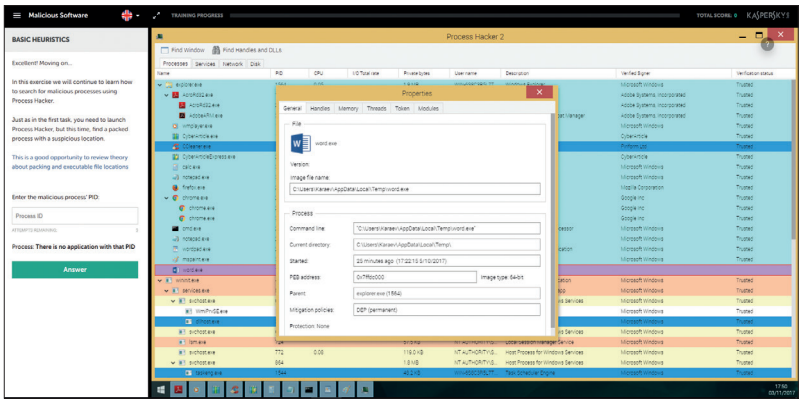
Развитие навыков реагирования на инциденты базового уровня

Для сотрудников IT-служб, техподдержки и других отделов, не обладающих экспертными знаниями по информационной безопасности, но вынужденных реагировать на инциденты, часто сложно выбрать подходящий тренинг. Базовые тренинги по кибербезопасности не принесут им пользы – эти знания у них уже имеются. Однако им требуются специальные навыки, так как зачастую именно они находятся на первой линии обороны от кибератак.

Чтобы решить эту проблему, «Лаборатория Касперского» разработала **онлайн-курс по кибербезопасности для IT-специалистов (CITO)**. IT-специалисты широкого профиля учатся распознавать вероятные сценарии атак, признаками которых являются кажущиеся безвредными инциденты с компьютером.

Тренинг также обеспечивает базовые знания о расследовании угроз и использовании защитных инструментов и программ. IT-специалисты приобретают теоретические знания и практические навыки, закрепляя их упражнениями. Они также учатся собирать данные инцидентов безопасности и передавать их сотрудникам службы информационной безопасности.

Этот тренинг – отличный способ усилить защиту организации от инцидентов без затрат на курсы для экспертного уровня.



Тренинг по кибербезопасности для IT-специалистов: снимок экрана

Кроме того, тренинг по кибербезопасности для IT-специалистов мотивирует их искать признаки кибератак и помогает понять, что они должны делать на первой линии кибероборонь.

Для специалистов по информационной безопасности и корпоративным коммуникациям

Развитие навыков кризисных коммуникаций

Знают ли сотрудники вашего отдела корпоративных коммуникаций, как реагировать на кибератаку? Этому редко обучают, однако в случае внешней или внутренней кибератаки или обнаружения комплексной целевой угрозы (APT) нужно уметь правильно рассказать о случившемся ответственным лицам.

Вашим сотрудникам необходимо знать, как правильно оповещать заинтересованных лиц внутри компании и вне ее при киберинцидентах, а для этого требуются навыки информационного контроля и кризисных коммуникаций.

Тренинг Kaspersky Incident Communications (KIC) помогает повысить квалификацию сотрудников отдела корпоративных коммуникаций и научить их правильному поведению при обнаружении киберугрозы – для этого в ходе тренинга проводится имитация атаки. Кроме того, сотрудники учатся эффективно согласовывать действия со службой информационной безопасности, в том числе разрабатывать и применять средства для минимизации репутационного и финансового ущерба.

Все эти ценные знания можно включить в руководство по кризисным коммуникациям, направленное на развитие навыков, помогающих обеспечить непрерывность бизнеса.

Имитация кибератак на тренингах Kaspersky Incident Communication позволяет кризисной команде лучше разбираться в том, каким киберугрозам может подвергнуться компания.

Для специалистов по информационной безопасности и корпоративным коммуникациям

Реальные ситуации

Материалы разработаны на основе опубликованных данных о реальных целевых атаках.

Профессиональный подход

Тренинг разработан всемирно известными экспертами и профессионалами в области связей с общественностью.

Готовность к атакам

По итогам тренинга ваша организация создаст или обновит план кризисных коммуникаций в случае кибератаки, которому может следовать группа реагирования на инциденты.

Заключение

Киберугрозы могут быть самыми различными, однако они все чаще нацелены на сотрудников организаций – самое слабое звено в цепи кибербезопасности.

Вам необходимо сформировать безопасную рабочую среду на каждом уровне организации, от руководства до рядовых сотрудников – и универсального сценария здесь не существует.

Мы предлагаем тренинги по информационной безопасности Kaspersky Security Awareness, которые адаптируются для различных ролей, помогая быстро развить нужные навыки. Kaspersky Security Awareness – единое гибкое решение, которое быстро и эффективно меняет поведение ваших сотрудников, делая его безопаснее.

Обратитесь к нашим экспертам или партнерам, чтобы узнать, как использовать решения Kaspersky Security Awareness для укрепления корпоративной стратегии безопасности.

Пробная версия Kaspersky ASAP: k-asap.com/ru
Kaspersky Security Awareness: www.kaspersky.ru/awareness
Связаться с нами: Awareness@kaspersky.com

www.kaspersky.ru