Почему в вашей организации никто не озабочен Security Awareness?

Бударин Евгений
Evgeny.Budarin@kaspersky.com

KASPERSKY lab

ОШИБКИ СОТРУДНИКОВ – КЛЮЧЕВАЯ УГРОЗА БЕЗОПАСНОСТИ КРУПНЫХ КОМПАНИЙ СЕГОДНЯ

более

95%

всех утечек данных случаются из-за человеческих ошибок

* IBM 2015 Cyber Security Intelligence Index

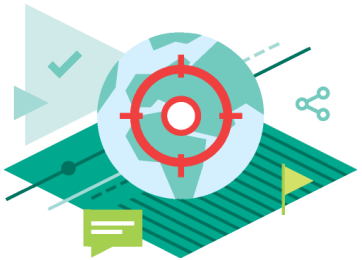
только

25%

страховых планов покрывают инциденты, произошедшие из-за человеческих ошибок и небрежности

* 2015 Global Cyber Impact Report. Ponemon Institute LLC.

УЩЕРБ ОТ ОШИБОК СОТРУДНИКОВ



$551,000

для крупных компаний

прямые расходы на восстановление от киберинцидента *

$38,000

для компаний среднего и малого бизнеса

прямые расходы на восстановление от киберинцидента *

до $400

на сотрудника в год

средний ущерб от фишинговых атак **

* “Damage Control: the Cost of Cybersecurity Breaches”, Kaspersky Lab and B2B International, October 2015.

** Calculations based on Ponemon Institute, “Cost of Phishing and Value of Employee Training”, August 2015.

КИБЕРУГРОЗЫ, НЕПОСРЕДСТВЕННО СВЯЗАННЫЕ С ОШИБКАМИ СОТРУДНИКОВ

- Фишинговые атаки
- Социальная инженерия
- Редко обновляемое ПО
- Слабые/ универсальные пароли
- Незаблокированные компьютеры и мобильные устройства
- Неблагонадежные приложения на корпоративных смартфонах
- Удаленная работа с незащищенных личных устройств
- Использование публичного Wi-Fi
- Кража устройств с незашифрованными данными (PC, смартфоны, флешки)

- Утечка данных
- Финансовое мошенничество
- Программы-вымогатели
- Ботнеты/ DDoS
- APT
- Атаки на промышленные объекты и сбои и работе критической инфраструктуры
- Электронный шпионаж
- Потери из-за простоя сотрудников и повреждения оборудования

ОСНОВНЫЕ ПРИЧИНЫ ОШИБОК СОТРУДНИКОВ

42%	Несоблюдение пользователями ИБ-политик и процедур
42%	Общая беспечность/ халатность
31%	Неосведомленность о новых типах угроз
29%	Недостаточное владение программами и навыками безопасного просмотра вебсайтов
26%	Несоблюдение ИБ-политик и процедур IT-специалистами

“Trends in IT Security”. CompTIA, 2015.

ПОЧЕМУ НЕЭФФЕКТИВНЫ СУЩЕСТВУЮЩИЕ ТРЕНИНГИ?

УРОВЕНЬ СОТРУДНИКА

- Занимают много времени
- Мешает исполнять основную работу
- Этим должны заниматься IT
- Кому я интересен?
- С сотрудниками ИБ сложно общаться
- Атаки же редко бывают
- Слишком сложные
- Слишком поверхностные
- Слишком технические
- Сложные и абстрактные
- Быстро забываются
- Оторваны от бизнеса
- С хакерами все равно ничего не сделаешь

- Скучно!

УРОВЕНЬ КОМПАНИИ

- Таким обучением сложно управлять
- Всех все равно не обучишь
- Это не приоритет
- Нет поддержки сверху
- Плохо поддаются оценке
- Тренинги проводятся формально, многие списывают
- Результаты обучения не проанализировать
- Дорого
- Быстро устаревают
- Начальник требует не тратить время на то, что не приносит прямого результата
- Никак не связаны с реальной работой
- Это разовое обучение (хотя даже им управлять сложно)

- Неэффективно!

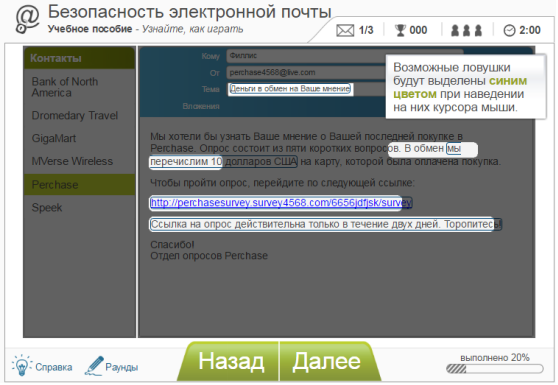
ПОДХОДЫ К ОБУЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Стандартный подход

Инструкции, ежегодные презентации, постеры, тренинги

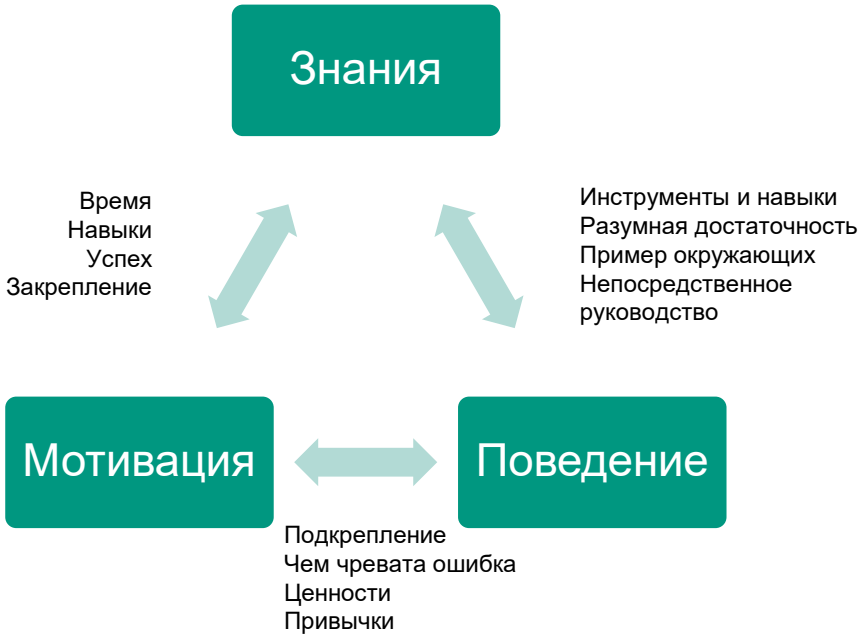
Низкая эффективность
Мало возможностей для измерения результата

Интерактивный подход + инструменты геймификации



- 93% – вероятность применения полученных знаний в повседневной работе
- 90% – сокращение числа ошибок
- 50-60% – снижение рисков кибербезопасности в денежном эквиваленте
- Более чем 30-кратная окупаемость вложений (ROI)

КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ: ПСИХОЛОГИЯ В ОСНОВЕ ВСЕГО



Большинство программ повышения осведомленности работают только со знаниями. Но люди устроены иначе: никто не руководствуется только теорией.

Поведение – вот с чем надо работать в ходе таких тренингов. А поведение всегда тесно связано с мотивацией и набором знаний.

Предлагаемый нами подход – создание и поддержание Культуры кибербезопасности – эффективен и измерим. На всех трех уровнях – знания, поведения, мотивации.

ТРЕНИНГИ KASPERSKY SECURITY AWARENESS

Навыки, а не только знания

Тренинги для **всех уровней и функций** организации

Компьютеризированные учебные программы – легко проводить, управлять обучением и измерять эффективность

Эффективность через **соревнование**, обучение на практике (**learning-by-doing**) и использование **реальных рабочих ситуаций**

Kaspersky Interactive Protection Simulation (KIPS)

- Увлекательный и вовлекающий формат
- Продолжительность – всего 2 часа
- Командная работа, помогающая создавать эффективное сотрудничество
- Атмосфера соревнования, способствующая проявлению инициативы и развитию навыков ситуационного анализа
- Сценарий разработан таким образом, чтобы способствовать лучшему пониманию мер информационной безопасности
- От участников не требуется глубокая экспертиза в области безопасности

CYBERSAFETY MANAGEMENT GAMES

Для менеджеров

ПОНИМАНИЕ ВАЖНОСТИ ИБ

Внедрение внутренних мер по кибербезопасности – серьезный процесс, однако в его основе лежит набор простых действий, не требующих больших временных затрат

УМЕНИЕ ПРИНИМАТЬ БИЗНЕС-РЕШЕНИЯ С УЧЕТОМ ПРИНЦИПОВ ИБ

Кибербезопасность как неотъемлемая часть бизнес-процессов

МОНИТОРИНГ

Взгляд на повседневные рабочие процессы с точки зрения кибербезопасности

УБЕЖДЕНИЕ И ВДОХНОВЕНИЕ

Вдумчивое руководство и полезные советы подчиненным

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ КИБЕРБЕЗОПАСНОСТИ

Для всех сотрудников

Комплексное решение: тестирование + атаки + обучение

30 языков. Cloud и On-premises

Обучающие модули

Короткие и забавные

Теория и упражнения с немедленным подкреплением

29 модулей на все аспекты ИБ (число модулей растет)

Auto-enrollement: автоматически назначаются после плохого прохождения соответствующего задания

Симулированные фишинговые атаки

3 типа атак разной сложности. Основаны на реальных случаях фишинга

Обучающая страница сразу после совершения пользователем опасных действий

Возможна кастомизация шаблонов

Оценка знаний (assessment)

Включает базовые предустановленные тесты, покрывающие разные темы кибербезопасности

Возможность создания тестов по внутренней политики безопасности

Авто-назначение обучения сотрудникам с низкими показателями ответов

Аналитика и отчетность

Позволяет отслеживать уровень обучающихся и динамику изменений

Анализ как в целом по организации, так и по подразделениям и на индивидуальном уровне

Экпорт в PDF, XLS, CSV

ОЦЕНКА КУЛЬТУРЫ КИБЕРБЕЗОПАНОСТИ

Для руководителей отделов ИБ

Позволяет проанализировать повседневное поведение сотрудников и их отношение к кибербезопасности

Онлайн-исследование на основе кратких кастомизированных опросников для сотрудников и менеджеров. Развитая система отчетов.

ТРЕНИНГИ, КОТОРЫЕ ДЕЙСТВИТЕЛЬНО РАБОТАЮТ

до

90%

Сокращение числа инцидентов

не менее

50%

Снижение ущерба в денежном выражении

до

93%

Вероятность применения навыков в повседневной работе

более чем

30x

Окупаемость вложений (ROI)

86%

Готовность рекомендовать программу

Вопросы?

Бударин Евгений
Evgeny.Budarin@kaspersky.com

KASPERSKY lab