



Человеческий firewall

**Преодоление человеческого
фактора в кибербезопасности**

KPMG

Декабрь 2021

Подход к программе осведомленности

2 основные цели:

1. Перевести осведомленность о безопасности из разряда выбора в **привычку**
2. Вовлекать людей на **эмоциональном уровне**:
 - Почему кибербезопасность важна?
 - Что в этом есть личного и индивидуального?

88

процентов зарегистрированных нарушений включают в себя элемент человеческой ошибки. Занятых сотрудников, чьи почтовые ящики ежедневно переполнены сообщениями, легко обмануть вредоносным письмом - и хакеры знают об этом. Поэтому компаниям крайне важно разработать и поддерживать комплексную стратегию кибербезопасности, в которой четко учитывается человеческий фактор.



Модель управления изменениями ADKAR

компания Prosci,
созданная
основателем
Джефффри
Хайаттом

ADKAR

- A Awareness** → Осознание необходимости перемен
Для повышения осведомленности на экранах рабочего стола сотрудников может отображаться напоминающее сообщение, например: «Сообщите о фишинге».
- D Desire** → Желание участвовать в изменениях и поддерживать их
Для стимулирования желания можно использовать серию сценариев «Что если?» с описанием потенциальных последствий и угроз, если не практиковать безопасное поведение.
- K Knowledge** → Знание о том, как измениться
Для повышения уровня знаний, использовать периодически интерактивные симуляции фишинга, включая мгновенную образовательную информацию для тех, кто стал жертвой.
- A Ability** → Способность реализовать требуемые навыки и поведение
Для развития навыков можно установить кнопку на панели инструментов электронной почты, чтобы сообщать о подозрительных сообщениях. команде кибербезопасности.
- R Reinforcement** → Подкрепление для поддержания изменений
Чтобы закрепить такое поведение, сотрудники, сообщающие о подозрительных сообщениях в электронной почте, могут получить ответ с благодарностью за бдительность и принятие мер. Если в сообщении обнаружит вредоносную деятельность, сотрудник может получить дополнительное признание своей помощи.

Сила брендинга И КОММУНИКАЦИЙ



Ежемесячные бюллетени, которые носят образовательный характер и посвящены своевременной или актуальной теме.



Уведомления информационного характера, например, о внедрении нового инструмента кибербезопасности.



Консультации позиционного характера, например, о надлежащем использовании сторонних программных приложений или о том, когда их не следует использовать.



Оповещения, которые могут быть использованы и являются частью плана реагирования на инциденты, чтобы привлечь сотрудников во время атаки или активного расследования и проинструктировать их о необходимости немедленных действий, например, смены паролей.



Количество участвующих в живых мероприятиях и презентациях



Количество сообщений о подозрительных электронных письмах



Показатель устойчивости к симулированным фишинговым атакам



Прохождение профессиональных учебных программ



Обратная связь через опросы сотрудников



Взаимодействие с командой по кибербезопасности через фирменный адрес электронной почты конкретного отдела

Измерение успеха

Как начать?



Установите цель

Владельцы программы - те, кто инициирует проектирование, разработку и реализацию программы и в итоге отвечают за ее успех - должны начать с проведения анализа пробелов для оценки понимания сотрудниками кибербезопасности и установления эталона для организации. Им необходимо будет взаимодействовать с руководством компании, чтобы помочь донести до них важность программы управления поведением, и им потребуется свобода, чтобы узнать о структуре компании, иерархии и культуре. Эти сведения помогут определить наиболее эффективные средства коммуникации, частоту сообщений, тон и подход.



Разработайте

Создание и реализация комплексной программы требует сотрудничества. Для начала владельцы программы должны быть профессионалами в области маркетинга, продаж и коммуникациями. Они должны обладать превосходными навыками письма и способностью переводить техническую информацию в понятные для обывателя термины. Анализ пробелов, первоначальные исследования и сравнительный анализ должны быть использованы для того, чтобы сформулировать всеобъемлющий стратегический план, в котором отражены цели, задачи, тактика и сроки реализации программы.



Создайте

В дополнение к владельцам программы, группы с различными навыками, экспертизой и опытом необходимы для полной разработки и реализации программы.

