

ПОВЫШЕНИЕ КИБЕРГРАМОТНОСТИ СОТРУДНИКОВ ПРОМЫШЛЕННОЙ КОМПАНИИ «ДАУ ИЗОЛАН»



Данила Гончаров

Начальник отдела ИТ
компании «Дау Изолан»

«Повышение уровня осведомленности в вопросах кибербезопасности – это важная часть ИБ-стратегии нашей компании. Мы понимаем необходимость регулярного обновления знаний по ИБ и формирования у сотрудников навыков, которые помогут правильно вести себя в случае реальной кибератаки. Ранее мы самостоятельно проводили обучение по кибербезопасности, но это было ресурсозатратно, – поэтому мы решили приобрести автоматизированный сервис, в рамках которого уже есть шаблоны, можно настроить рассылку на разные группы сотрудников, назначать пользователям подходящий теоретический курс и оценить результативность обучения»

Профиль организации

«Дау Изолан»

Крупнейший производитель полиуретановых систем в России и СНГ

[Узнать подробнее](#)

Отрасль: химическая промышленность

Размер: завод, офис, 4 складских корпуса, распределенных географически

Данные о проекте

Security Awareness (SA)

Сервис управления навыками кибербезопасности

[Узнать о сервисе](#)

Тип: облачный сервис

Описание: комплексное обучение сотрудников киберграмоте с экспертной поддержкой

Цель

Повысить уровень осведомленности сотрудников о киберугрозах в соответствии с ИБ-стратегией компании

Задача

- Познакомить с информацией об актуальном ландшафте цифровых угроз с приведением конкретных примеров
- Рассказать о правилах работы с компьютерной техникой и необходимости соблюдения парольной политики
- Оценить полученные знания

Решение

- Провести обучение по материалам, содержащим актуальную информацию о современных киберугрозах, новых векторах атак и тактиках злоумышленников
- Сформировать отчет с результатами обучения и список «уязвимых» сотрудников

Результат

- Организован обучающий курс по повышению киберграмотности сотрудников, в который включены теоретические материалы, описывающие признаки фишинга, уловки хакеров и возможные последствия атак
- 80% сотрудников успешно прошли первый обучающий курс, адаптированный под особенности компании и специфику отрасли
- По итогам первого обучающего курса количество пользователей, которые совершают потенциально опасные действия, сократилось на 30%

Цель

На практических примерах научить сотрудников грамотно реагировать на фишинговые атаки

Задача

- Проверить, насколько сотрудники компании квалифицированы в распознавании вредоносных писем
- Научить сотрудников распознавать фишинговые рассылки и адекватно на них реагировать

Решение

- Реализованы имитированные фишинговые атаки: произведена рассылка тестовых писем сотрудникам
- Назначены соответствующие курсы сотрудникам, прошедшим проверку
- Для тестовой рассылки подготовлено 5 шаблонов фишинговых писем, сформированных исходя из внутренних особенностей компании, внешних инфоповодов и актуальных векторов атак

Результат

- После прохождения обучения число сотрудников, совершающих небезопасные действия с фишинговыми письмами, сократилось на 24%
- По результатам рассылки фишинговых писем сформированы отчеты, позволяющие оценить уровень киберграмотности сотрудников компании
- Сотрудники научились распознавать фишинговые атаки, даже не открывая писем

