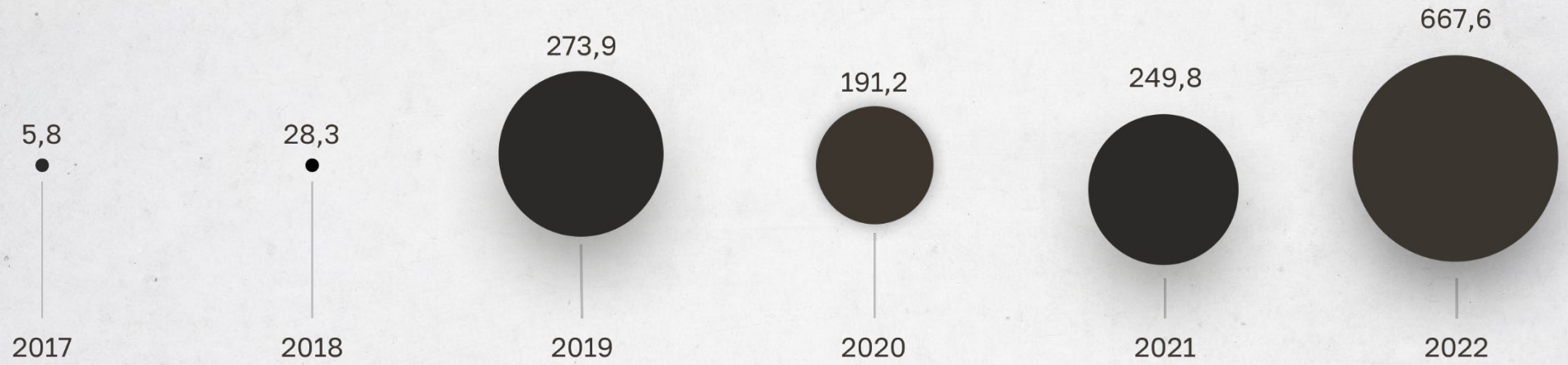
Статистика

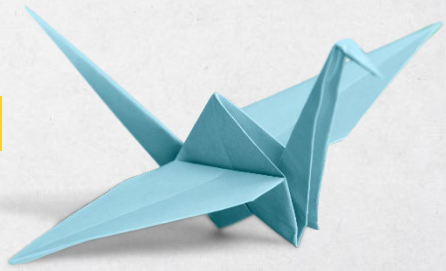
92 %
компаний стали жертвами фишинговых атак в 2022 году.

93 %
утечек данных произошли из-за фишинговых атак



количество утекших записей ПДн и платежной информации. Млн записей, 2017–2022 гг.

Источники:
https://www.computerweekly.com/news/365532100/Nine-in-10-enterprises-fell-victim-to-successful-phishing-in-2022
InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя



Последствия

Кейс

Компания

Крупный бельгийский банк

Происшествие

Сотрудникам были разосланы письма якобы от высокопоставленных руководителей

Результат

Банк потерял 70 миллионов евро

Как защититься

Регулярное обучение

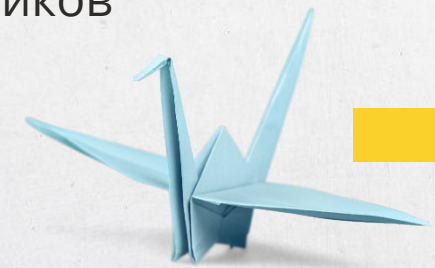
Повышение осведомленности сотрудников в области ИБ

Контроль знаний

Определение уровня усвоения материала

Имитированные атаки

Проверка сотрудников, как они реагируют на потенциальную угрозу со стороны мошенников



Как обучать

Тренинги

+

Погружение

Очные тренинги обычно более глубоко погружают в материал

Персонализация

Программа обучения может быть построена на основе уровня знаний и потребностей участников

Обратная связь

Участники могут задавать вопросы по ходу обучения

—

Затраты

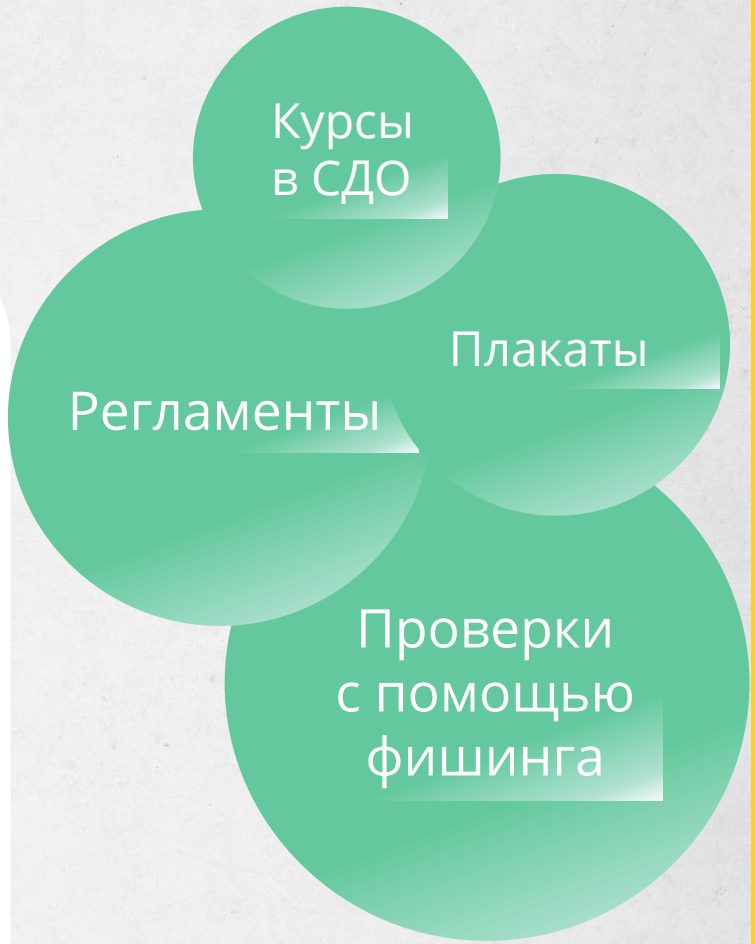
Большие финансовые затраты на организацию и проведение

Время

Ограниченное время на посещение тренинга

Доступность

На рынке сложно найти квалифицированных инструкторов



Как обучать

Курсы в СДО

+

Гибкость

Пользователи могут пройти обучение в любое время

Доступность

Большое количество курсов можно найти в интернете без дополнительной платы

Разнообразие

Разные форматы подачи материала, включая видео, интерактив и прочее

—

Затраты

Большие финансовые затраты на интеграцию СДО

Самодисциплина

Не все пользователи способны эффективно управлять временем

Обратная связь

Не всегда есть возможность получить обратную связь от экспертов курса

Регламенты

Плакаты

Проверки с помощью фишинга

Как обучать

Плакаты

+

Стоимость

Небольшие финансовые затраты на размещение в офисе

Доступность

Большое количество плакатов можно найти в интернете

Повторение

Постоянно привлекают внимание сотрудников в офисе, что служит напоминанием о важных аспектах

—

Не вся информация

Плакаты ограничены по размеру и объёму информации

Неинтерактивность

Нет возможности проверить усвоение материала

Обновление

Нет возможности часто актуализировать информацию

Регламенты

Проверки с помощью фишинга

Как обучать

Проверки с помощью фишинга

\+

Реалистичность

Создание максимально приближенных ситуаций

Практический опыт

Помогает развивать навыки распознавания подозрительных сообщений и действий

Сознательность

Пользователи могут стать более осторожными и бдительными

Регламенты

—

Доступность

Контракт с подрядчиками (большие финансовые затраты) или бесплатные версии (GoPhish)

Как обучать

Регламенты

+

Законодательство

Могут помочь организации соблюдать требования законодательства

Установка стандартов

Стандарты и правила для обеспечения ИБ в организации

Управление рисками

Идентификация и управление рисками, связанными с ИБ

—

Бюрократия

Повышение административной нагрузки в организации

Соблюдение актуальности

Нет возможности проверить усвоение материала

Затраты

Финансовые и временные ресурсы на разработку, внедрение и поддержку

Как обучать


План-график обучения
Регламенты
Тренинги
Плакаты
Курсы
в СДО
Проверки
с помощью
фишинга

Аналитика по сегменту

3 млрд

фишинговых писем ежедневно злоумышленники отправляют Компаниям*

85%

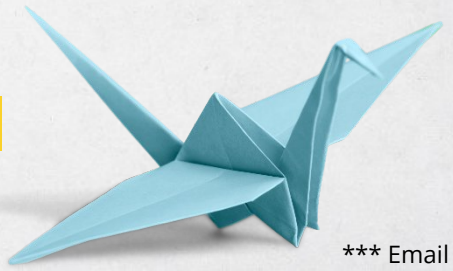
утечек данных происходят из-за «человеческого фактора»**

$4,24 млн

составляет средняя стоимость утечки данных в 2022 году***

Решение →

SECURE-T



* 2021 Data Breach Investigation Report

** Cost of a Data Breach Report 2021, Ponemon Institute и IBM Security)

*** Email Fraud Landscape: Spring 2021

Решение

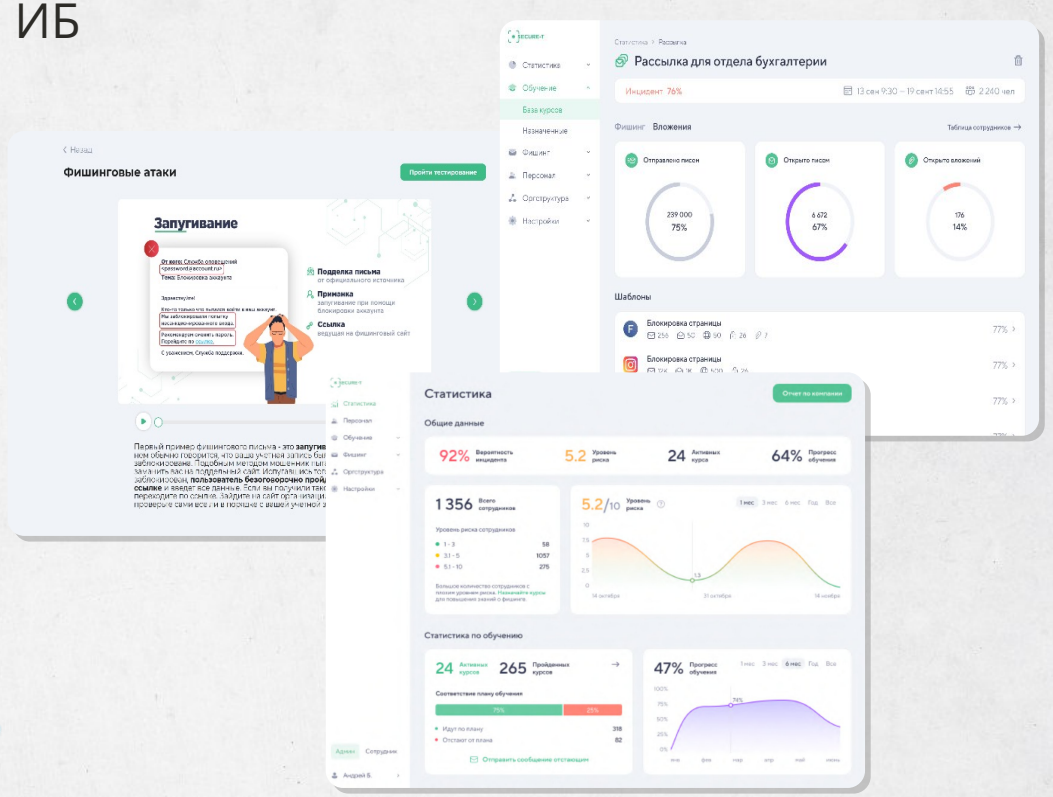
Secure-T Awareness Platform

Secure-T уже четвертый год занимается повышением осведомленности сотрудников в области ИБ

Теория
Обучающие курсы и тесты

Практика
Имитация фишинга и вирусные вложения

Аналитика
Подробная статистика
и выявление уязвимых сотрудников



Все возможности

Secure-T Awareness Platform

Курсы

Объем обучающих курсов
не менее 40 модулей

Фишинг

Персонализированные
письма, а также вложения

Конструктор

Создание поддельных писем
и лэндингов

Интеграция

Интеграция через API

СДО

Возможность загружать
свои собственные курсы

Логирование

Фиксирование всех действий
пользователей

Редактор курсов

Возможность вносить
изменения в наши курсы

Онбординг

Автоматическое
назначение по группам

Настройка тестов

Гибкая настройка
тестовых вопросов

Внедрение системы приносит ощутимые результаты

Кейс

Дано

Поставщик инженерных услуг
(150 пользователей)

Проблема

При проверке сотрудников было выявлено, что только 27% персонала- не подвержены фишинговым атакам

Снижение количества сотрудников, подверженных фишингу*

68%

*После годового использования Secure-T Awareness Platform