StopPhish

КИБЕРИММУНИТЕТ НА УДАЛЁНКЕ

Как вовлечь сотрудников в безопасность,
даже если они работают вне офиса

Эмилия Садыкова, ведущий эксперт по защите от социальной инженерии, StopPhish

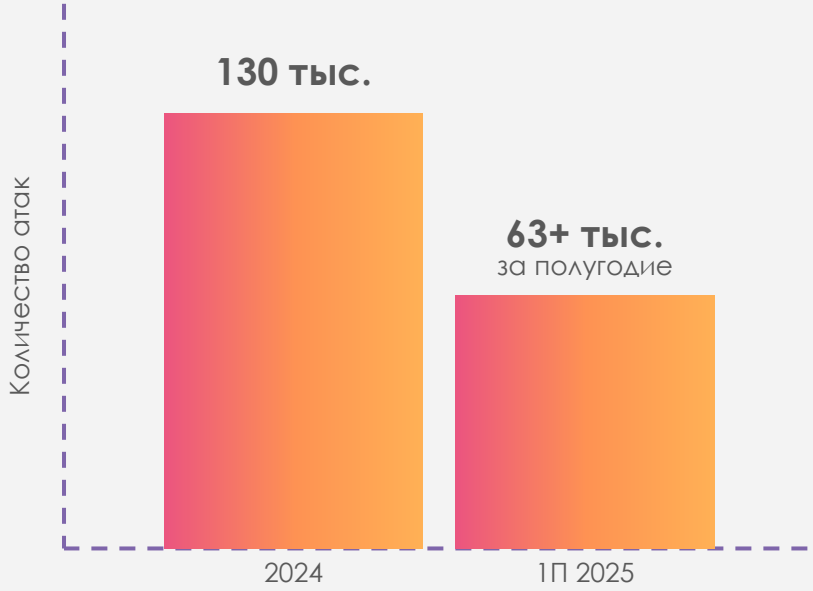
УДАЛЁННАЯ РАБОТА ПОД ОГНЁМ: ЦИФРЫ 2024–2025

+30%
рост кибератак через личные устройства сотрудников в 1П 2025. CNews.ru

+425%
рост фишинговых атак в РФ за 2024 год (заблокировано >22 тыс. фишинговых ресурсов). ТАСС

1,8 млрд
попыток кибератак в России в 2024 году (по данным Лаборатории Касперского). Forbes

95%
утечек связаны с человеческим фактором; 42% — неумышленные действия сотрудников. TAdviser



ТРИ КРИТИЧЕСКИХ ФАКТОРА РИСКА

- Множество каналов атак
- Изоляция сотрудника
- Ослабленный контроль ИБ-служб

ОФИСНАЯ ЭПИДЕМИЯ: ВИРУС ДОВЕРИЯ

+7644%

9 получателей писем

688 открытий письма

140 уникальных ip

Повышение ЗП с 1.10 с ссылкой на портал

От: [redacted]

Тема: Повышение заработной платы

Коллеги, добрый день.

Для нас важно, чтобы каждый сотрудник был уверен в завтрашнем дне, поэтому мы объявляем о повышении заработной платы для всех направлений, начиная с **01.10**.

Подпишите дополнительное соглашение и пришлите его в ответном письме.

Дополнительное соглашение мы загрузили на наш официальный портал:

С уважением, [redacted]

Помощник руководителя отдела по начислению заработной платы

ОТ ЗАЩИТЫ К ИММУНИТЕТУ

ТРАДИЦИОННАЯ ЗАЩИТА «РЕАКТИВНЫЙ ПОДХОД»

- Защитить технологиями
- Сотрудник = слабое звено

КИБЕРИММУНИТЕТ «ПРОАКТИВНЫЙ ПОДХОД»

- Защитить технологиями
- Сотрудник = активная линия обороны

4 ШАГА К ФОРМИРОВАНИЮ КИБЕРУСТОЙЧИВОСТИ СОТРУДНИКОВ

1	2	3	4
Обучение	Практика в безопасной среде	Культура без наказаний	Измеримость результатов

ПОДХОДЫ, КОТОРЫЕ РАБОТАЮТ НА УДАЛЁНКЕ

- Короткие видеовставки примеров атак
- Нарастающая сложность учебных фишинговых атак
- Позиционирование контента с точки зрения личного применения
- Микрообучение
- Тренажеры

МИКРООБУЧЕНИЕ

Вы попались на фишинговую атаку

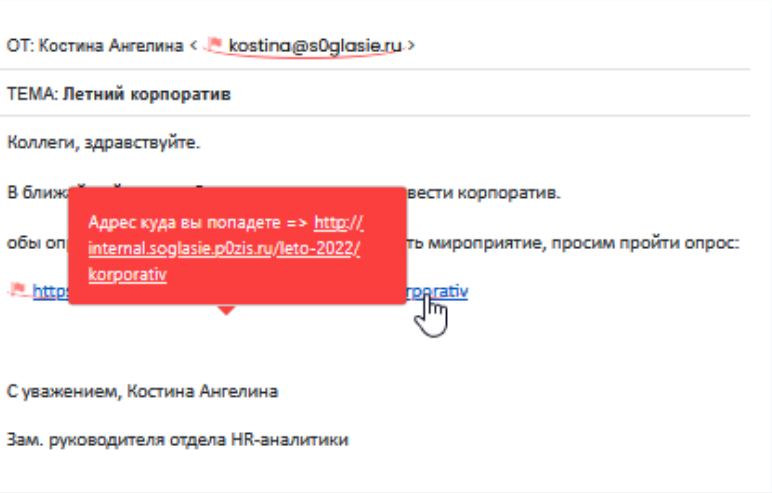
Вам повезло. Это сообщение – просто проверка знаний.

Данное письмо было потенциально опасным.

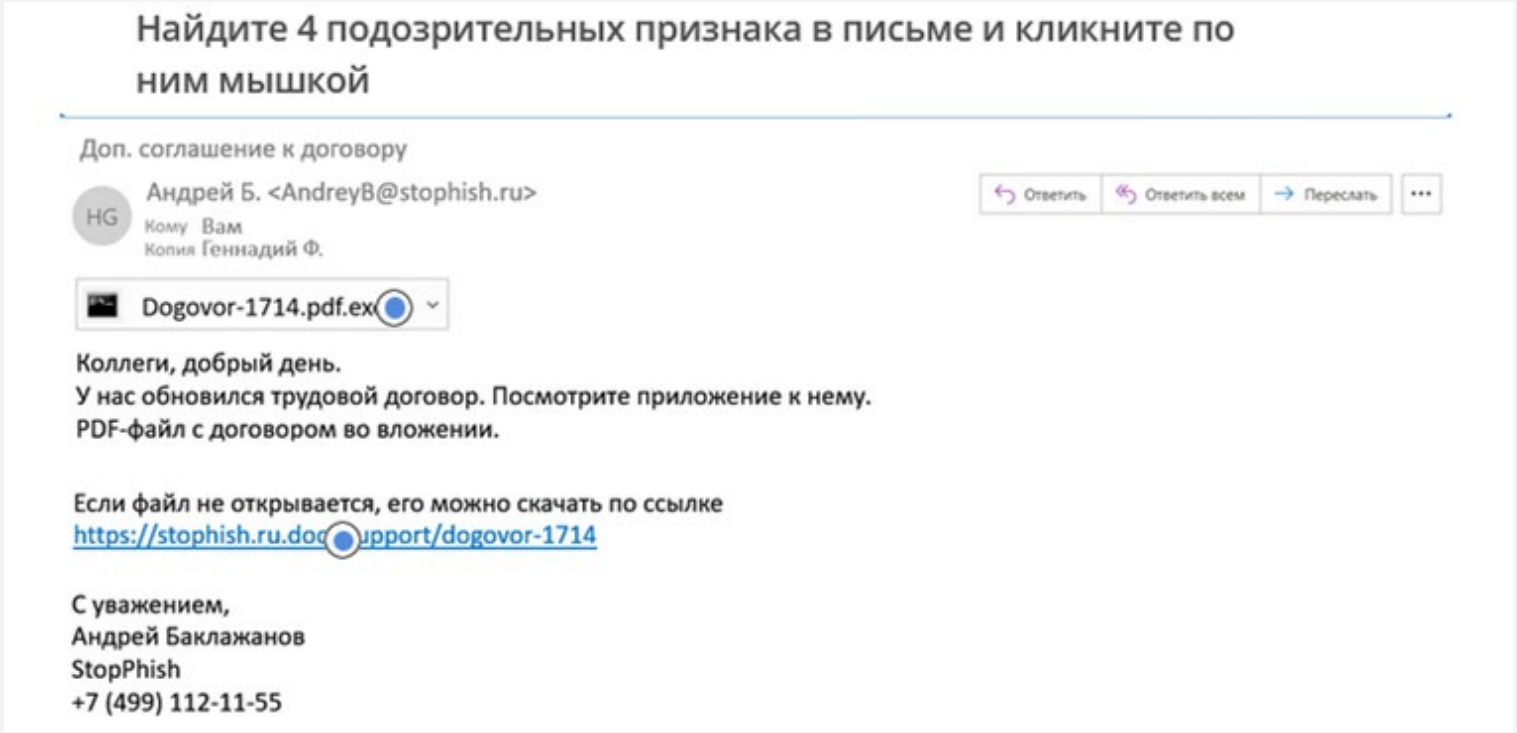
Обратите внимание на адрес отправителя письма.

Наведите курсор мышки на ссылку в письме и вы сможете увидеть настоящую ссылку.

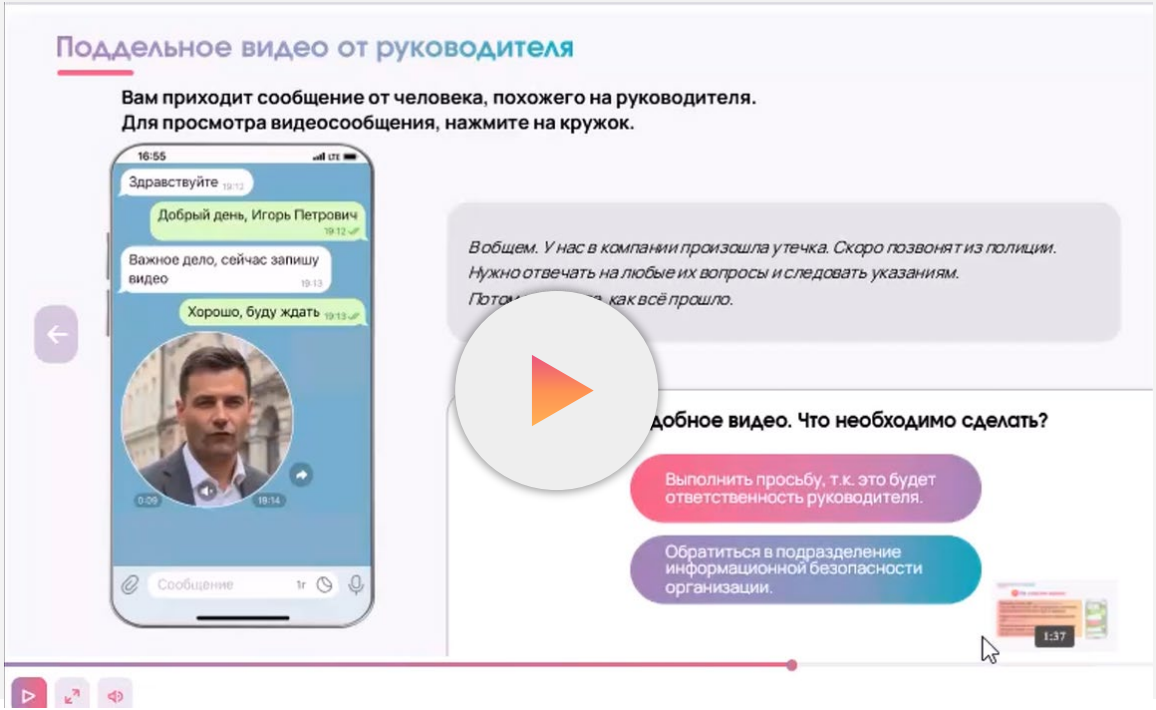
На подобных сайтах злоумышленники воруют пароли и заражают компьютеры вирусами.



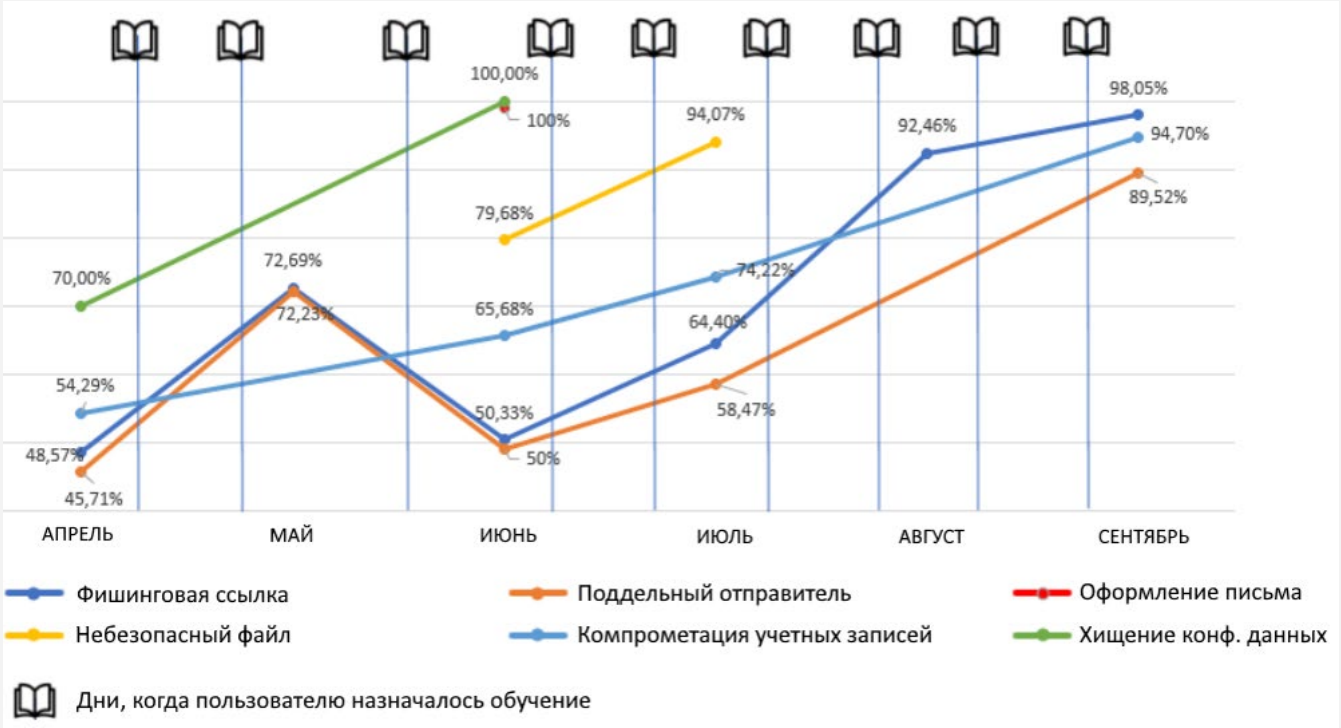
ТРЕНАЖЕР С E-MAIL АТАКАМИ



ТРЕНАЖЕР ПО ОТРАБОТКЕ АТАК В МЕССЕНДЖЕРАХ



РЕЗУЛЬТАТЫ УЖЕ ЧЕРЕЗ ПОЛГОДА



СПАСИБО ЗА ВНИМАНИЕ!

StopPhish

Бесплатные инструменты

- Плакаты
- Скринсейверы
- Бесплатные курсы
- Памятки
- ПО Free
- Плагины
- Генератор СИ
- Калькулятор