



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%

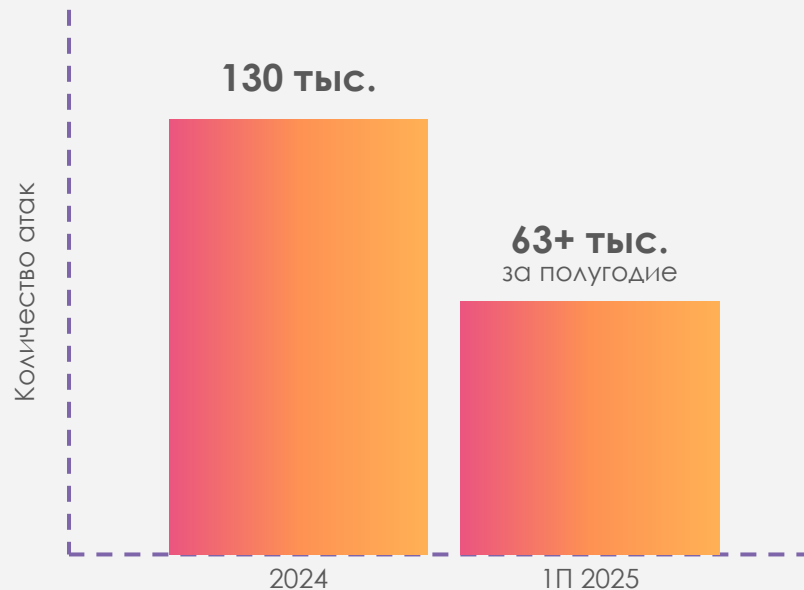
рост фишинговых атак в
РФ за 2024 год
(заблокировано >22 тыс.
фишинговых ресурсов).
ТАСС

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:



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,



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

Обучение

2

Практика в
безопасной
среде

3

Культура без
наказаний

4

Измеримость
результатов

ПОДХОДЫ, КОТОРЫЕ РАБОТАЮТ НА УДАЛЁНKE

- ▶ 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.

ОТ: Костина Ангелина < kostina@s0glasie.ru>

ТЕМА: Летний корпоратив

Коллеги, здравствуйте.

В ближайшее время мы хотим провести корпоратив.

Обычно мы проводим его в летний период. Чтобы мероприятие прошло успешно, просим пройти опрос:

 <http://internal.s0glasie.p0zis.ru/leto-2022/korporativ>

С уважением, Костина Ангелина

Зам. руководителя отдела HR-аналитики

ТРЕНАЖЕР С E-MAIL АТАКАМИ

Найдите 4 подозрительных признака в письме и кликните по НИМ МЫШКОЙ

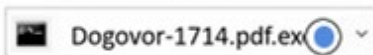
Доп. соглашение к договору



Андрей Б. <AndreyB@stophish.ru>

Кому Вам
Копия Геннадий Ф.

← Ответить ↶ Ответить всем → Переслать ...



Коллеги, добрый день.

У нас обновился трудовой договор. Посмотрите приложение к нему.

PDF-файл с договором во вложении.

Если файл не открывается, его можно скачать по ссылке

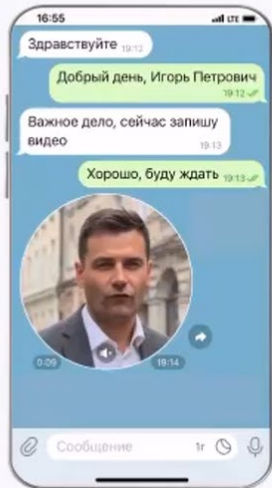
<https://stophish.ru.docsupport/dogovor-1714>

С уважением,
Андрей Баклажанов
StopPhish
+7 (499) 112-11-55

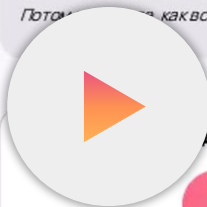
ТРЕНАЖЕР ПО ОТРАБОТКЕ АТАК В МЕССЕНДЖЕРАХ

Поддельное видео от руководителя

Вам приходит сообщение от человека, похожего на руководителя.
Для просмотра видеосообщения, нажмите на кружок.



Вобщем. У нас в компании произошла утечка. Скоро позвонят из полиции.
Нужно отвечать на любые их вопросы и следовать указаниям.
Потом всё как всё прошло.



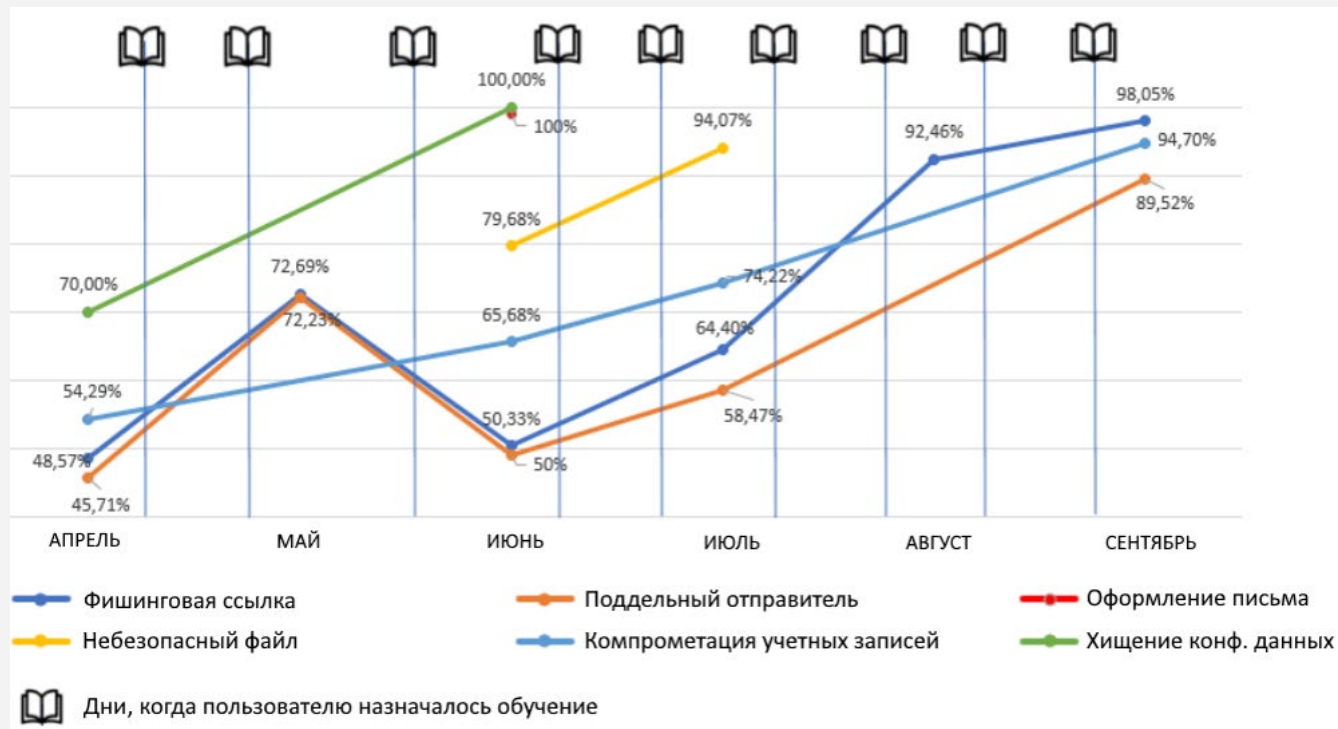
Поддельное видео. Что необходимо сделать?

Выполнить просьбу, т.к. это будет
ответственность руководителя.

Обратиться в подразделение
информационной безопасности
организации.



РЕЗУЛЬТАТЫ УЖЕ ЧЕРЕЗ ПОЛГОДА



СПАСИБО ЗА ВНИМАНИЕ!



Бесплатные инструменты

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

