Антифишинг
www.antiphish.ru

ДиалогНаука

Цифровые атаки на сотрудников. Кейсы. Статистика. Платформа Антифишинг как системное решение проблемы.

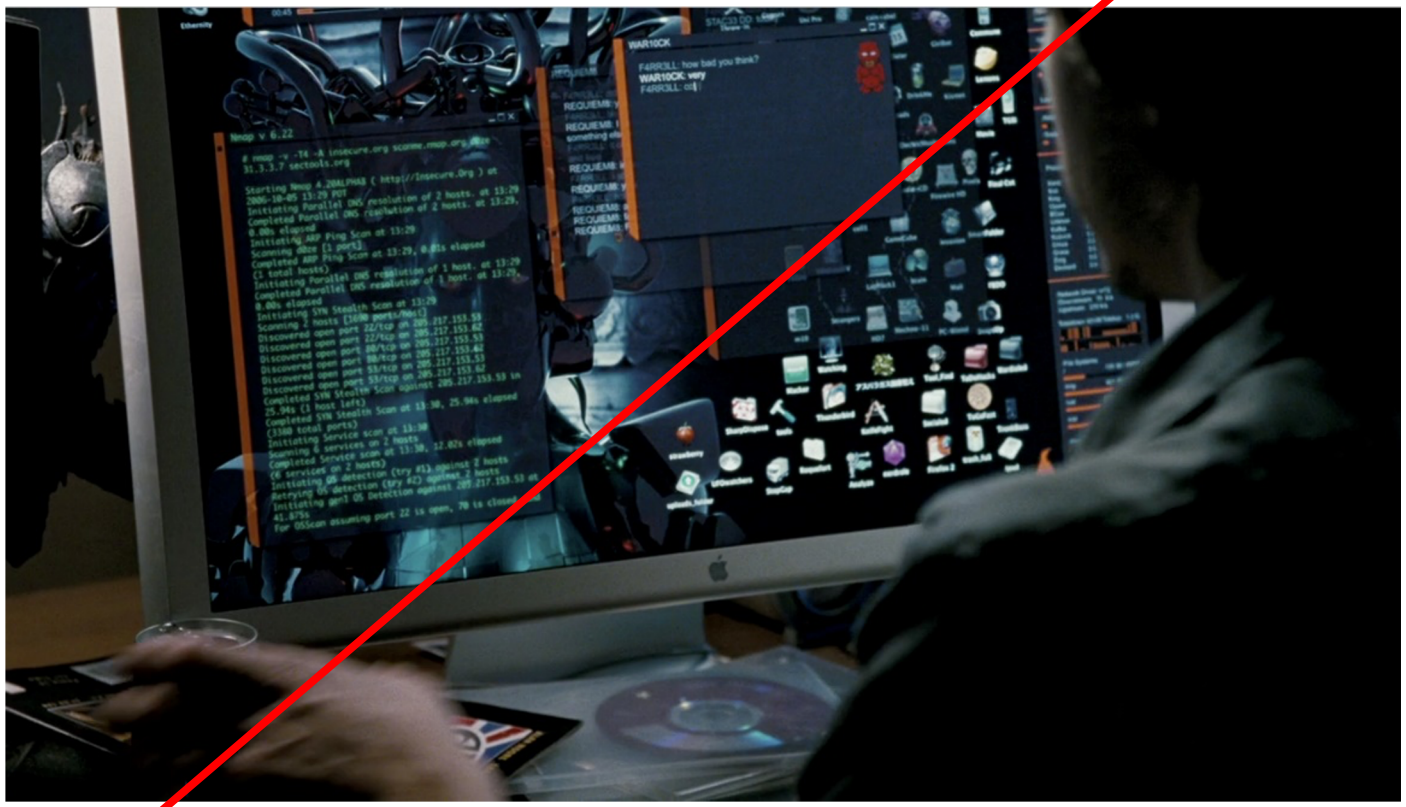
Вебинар. Начинаем через 5 минут

17 февраля 2021 года

Цифровые атаки на людей

Примеры и кейсы 2020 года

Как выглядит современная цифровая атака?



Перечень документов на проверку контрагента.doc


Подтвержденные инциденты
Эксплуатация: Нелегитимная аутентификация
10
10
Разведка: Сканирование
13
24
Закрепление: Использование хакерских утилит и утилит сбора...
17
28
Разведка: брутфорс
34
36
Доставка: Доставка ВПО через Email
22
92
0
20
40
60
80
100

Techniques

ID	Name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
.001	Spearphishing Attachment
.002	Spearphishing Link
.003	Spearphishing via Service
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
.001	Compromise Software Dependencies and Development Tools
.002	Compromise Software Supply Chain
.003	Compromise Hardware Supply Chain
T1199	Trusted Relationship
T1078	Valid Accounts

ATT&CK®

Techniques

ID	Name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
.001	Spearphishing Attachment
.002	Spearphishing Link
.003	Spearphishing via Service
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
.001	Compromise Software Dependencies and Development Tools
.002	Compromise Software Supply Chain
.003	Compromise Hardware Supply Chain
T1199	Trusted Relationship
T1078	Valid Accounts

Corona Antivirus – World's best P

antivirus-covid19.site

CORONA ANTIVIRUS

Corona Antivirus — World's best protection

Download our AI Corona Antivirus for the best possible protection against the Corona COVID-

Download Corona Anti-Virus

update.exe

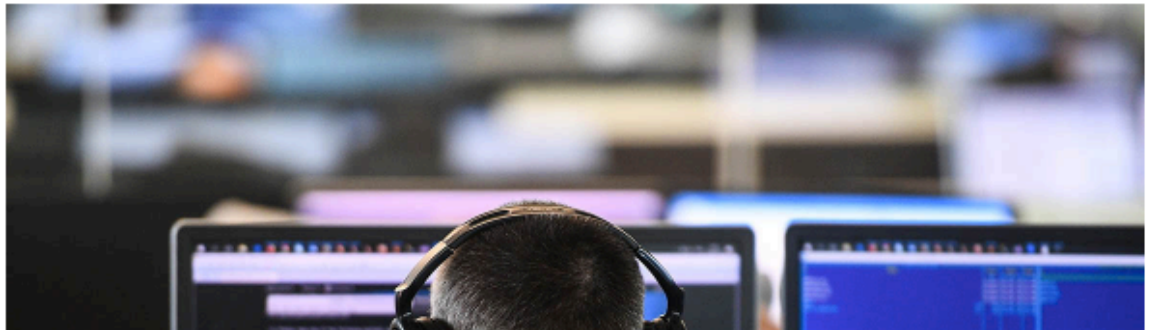
В 2020 году большинству организаций и их сотрудников пришлось перейти на новый для себя формат работы — онлайн, удаленно, вне офиса. И пока службы безопасности были заняты подготовкой защищенных каналов связи и другой инфраструктуры, мошенники атаковали людей, а основным вектором атак стала социальная инженерия.

+91,7% число киберпреступлений в первом полугодии 2020 года

Технологии и медиа, 14 авг, 12:35 | 11 002 | Поделиться

Новая хакерская группировка атаковала банки под видом журналистов Вместо вопросов для интервью финансисты получали вредоносное ПО

Хакеры из группировки TinyScouts отправляют письма в банки с предупреждением о второй волне COVID-19. Сотрудникам финучреждений также предлагается дать интервью — злоумышленники маскируются под журналистов, в том числе из РБК



На первом этапе атаки киберпреступники рассылают сотрудникам организаций фишинговые письма, в которых предупреждают о начале второй волны пандемии коронавируса. Для получения дополнительной информации адресату предлагают пройти по внешней ссылке.

Встречаются также варианты фишинговых писем, имеющих четкий таргетинг: сообщение напрямую относится к деятельности организации и выглядит «вполне убедительно»

Финансы Таня Боброва 25 дек 2020

«Мы облажались и подвели клиентов»: глава «Фридом Финанса» извинился за утечку данных пользователей

Одному из сотрудников пришло фишинговое письмо, а пароли не были скомпрометированы.

+2 61 8207 просмотров

Глава брокера «Фридом Финанс» Тимур Турлов признал утечку данных клиентов. По его словам, среди них почти нет клиентов, которые открывали счета на американском рынке, и нет международных клиентов.

Турлов пояснил, что неизвестные атаковали сегмент внутренней сети и похитили часть данных с локальных машин нескольких сотрудников в России. Машины относятся к сотрудникам российского брокера, оказывающего доступ на российский фондовый рынок, а почти весь пакет данных датирован 2018 годом.

Статистика безопасного поведения

На базе 100 тысяч атак, на выборке 20 тысяч человек

АНТИФИШИНГ

ГОДОВОЙ ОТЧЕТ О ЗАЩИЩЕННОСТИ СОТРУДНИКОВ

2020

Структура отчета и источники данных

1. В первом разделе отчета мы оценили защищенность сотрудников: по отраслям, отделам, должностям, дням недели и времени, в которые выполнялись атаки, а также по территориальному расположению.

2. Во втором разделе мы оценили технические факторы, которые влияют на успех реальных цифровых атак против сотрудников: действия при работе со стационарных и мобильных устройств, наличие уязвимостей в клиентском ПО, зависимость действий сотрудников от типа вложений.

3. В третьем разделе мы оценили психологические факторы, которые наиболее сильно влияют на небезопасное поведение: психологические векторы атак, персонификацию, психологические усилители, а также источники атак.

4. В четвертом разделе мы сравнили эффективность различных мер для решения проблемы защищенности сотрдуников: обучение, тренировка навыков через имитированные атаки, мгновенная обратная связь при совершении небезопасных действий, особенности процессов при высокой текучести кадров.

Отчет составлен на основе обезличенных данных от наших клиентов

>100 000
имитированных фишинговых атак за 2020 год

~20 000
сотрудников

48
компаний

Также мы использовали данные по поведению нескольких сотен пользователей, не являющихся сотрудниками указанных компаний, но согласившихся принять участие в практическом исследовании Антифишинга.

Основные выводы

37% сотрудников компаний открывают фишинговые письма

79% из них затем совершают небезопасные действия

11% из них имеют уязвимости в приложениях

Наиболее опасные психологические факторы

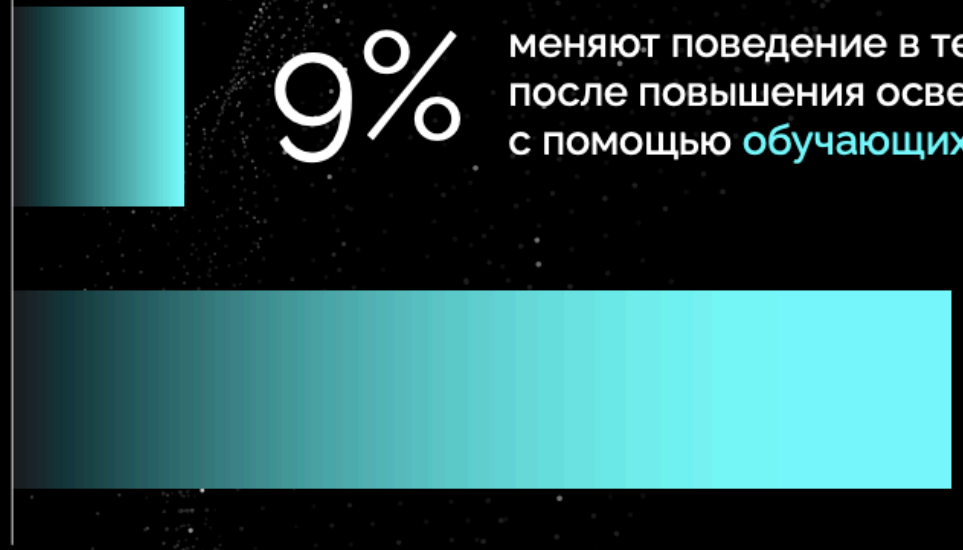
- Корпоративная атрибуция — письма от имени коллег или руководителей
- Персонификация — обращение к жертве по имени
- Авторитетность источника атаки

Наиболее уязвимы к фишингу

- Сотрудники из отделов дизайна, технической поддержки и информационных технологий
- Сотрудники компаний из сферы услуг и производства
- Сотрудники компаний из дальних регионов

Наибольшее количество небезопасных действий совершается с PDF-файлами

Основные выводы

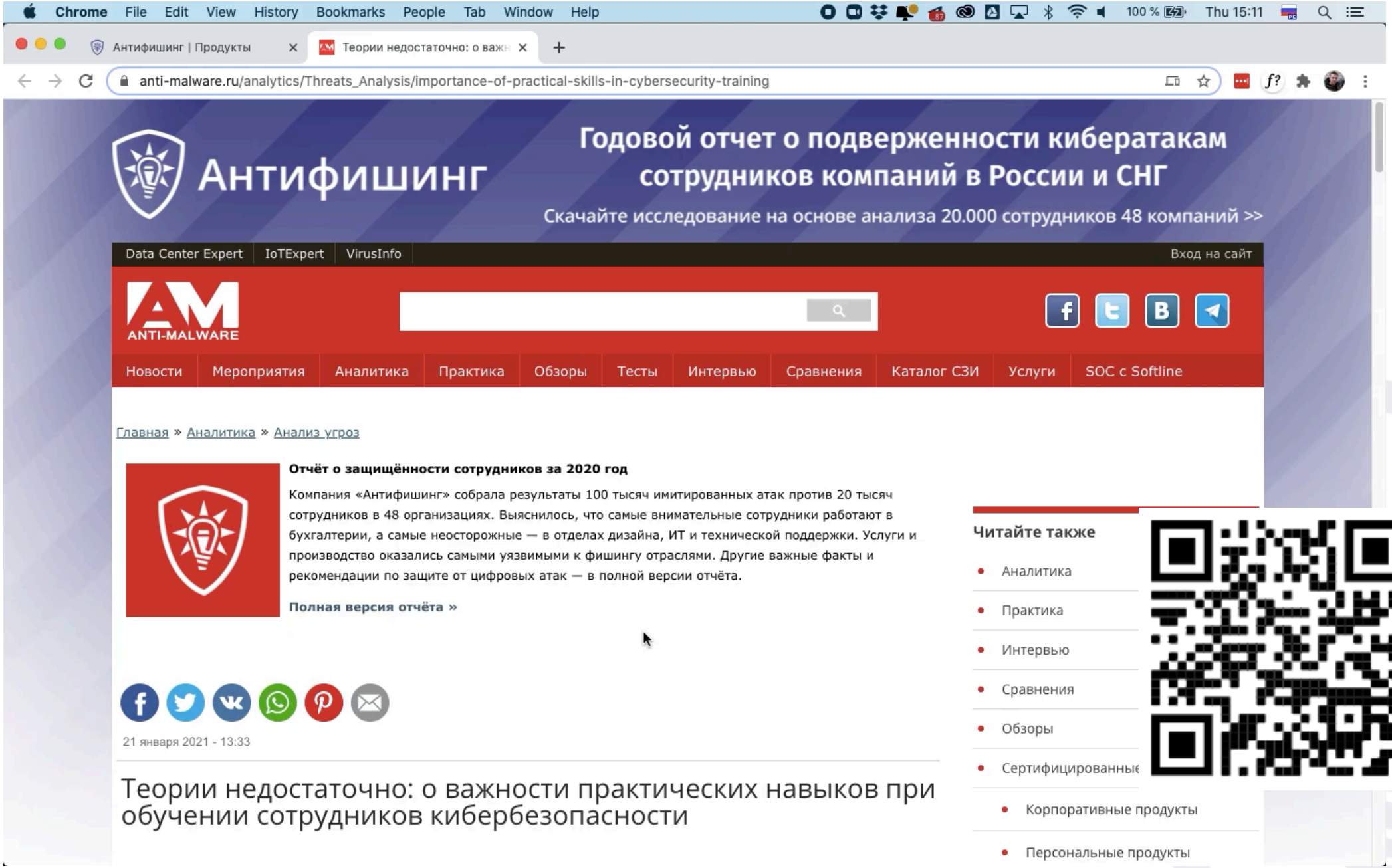


9% меняют поведение в течение года, после повышения осведомленности с помощью обучающих курсов

49% меняют поведение в течение года, после тренировки навыков через имитированные атаки

×2 эффективность навыков

при использование мгновенной обратной связи при небезопасных действиях


Chrome File Edit View History Bookmarks People Tab Window Help
Thu 15:11
Антифишинг | Продукты
Теории недостаточно: о важн
anti-malware.ru/analytics/Threats_Analysis/importance-of-practical-skills-in-cybersecurity-training
Антифишинг
Годовой отчет о подверженности кибератакам сотрудников компаний в России и СНГ
Скачайте исследование на основе анализа 20.000 сотрудников 48 компаний >>
Data Center Expert
IoTExpert
VirusInfo
Вход на сайт
ANTI-MALWARE
Новости
Мероприятия
Аналитика
Практика
Обзоры
Тесты
Интервью
Сравнения
Каталог СЗИ
Услуги
SOC с Softline
Главная » Аналитика » Анализ угроз
Отчёт о защищённости сотрудников за 2020 год
Компания «Антифишинг» собрала результаты 100 тысяч имитированных атак против 20 тысяч сотрудников в 48 организациях. Выяснилось, что самые внимательные сотрудники работают в бухгалтерии, а самые неосторожные — в отделах дизайна, ИТ и технической поддержки. Услуги и производство оказались самыми уязвимыми к фишингу отраслями. Другие важные факты и рекомендации по защите от цифровых атак — в полной версии отчёта.
Полная версия отчёта »
21 января 2021 - 13:33
Теории недостаточно: о важности практических навыков при обучении сотрудников кибербезопасности
Читайте также
Аналитика
Практика
Интервью
Сравнения
Обзоры
Сертифицированные
Корпоративные продукты
Персональные продукты

Антифишинг как решение

Защита компаний и организаций в новых условиях

blog.antiphish.ru

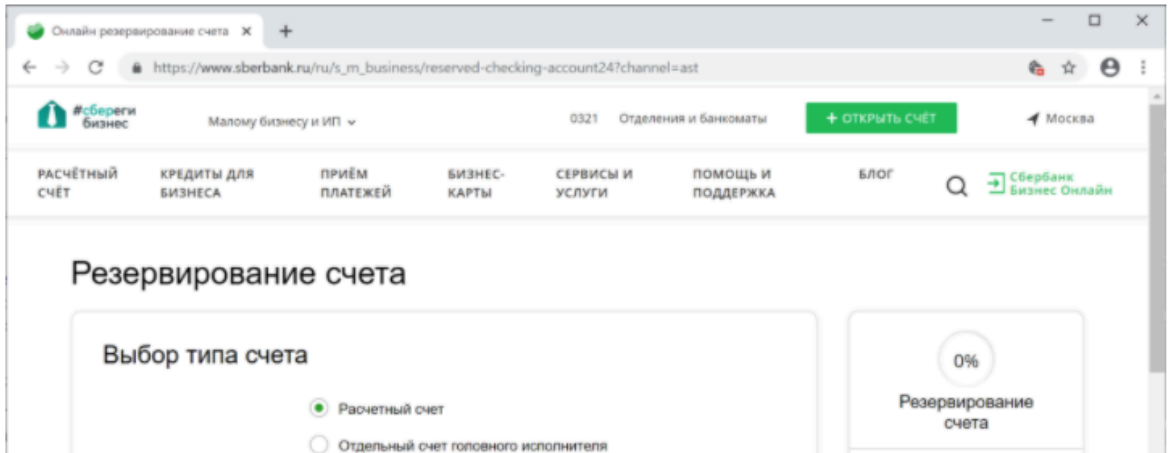
16 июля, 23:16

Антифишинг-дайджест № 179 с 10 по 16 июля 2020 года

Представляем новости об актуальных технологиях фишинга и других атаках на человека с 10 по 16 июля 2020 года

Мошенники

Мошенники используют сервис Сбербанка по дистанционному резервированию расчётных счетов, чтобы отправлять потенциальным жертвам в нужный момент СМС-сообщения с официального номера банка 900 для подтверждения подлинности звонка.



Андрей Жаркевич
редактор

Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

antiphish.ru/classification

Outline

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sbernbank.ru», «www.gmall.com»

Любопытство

«Смотри, как ты отжигаешь на видео»

Жадность

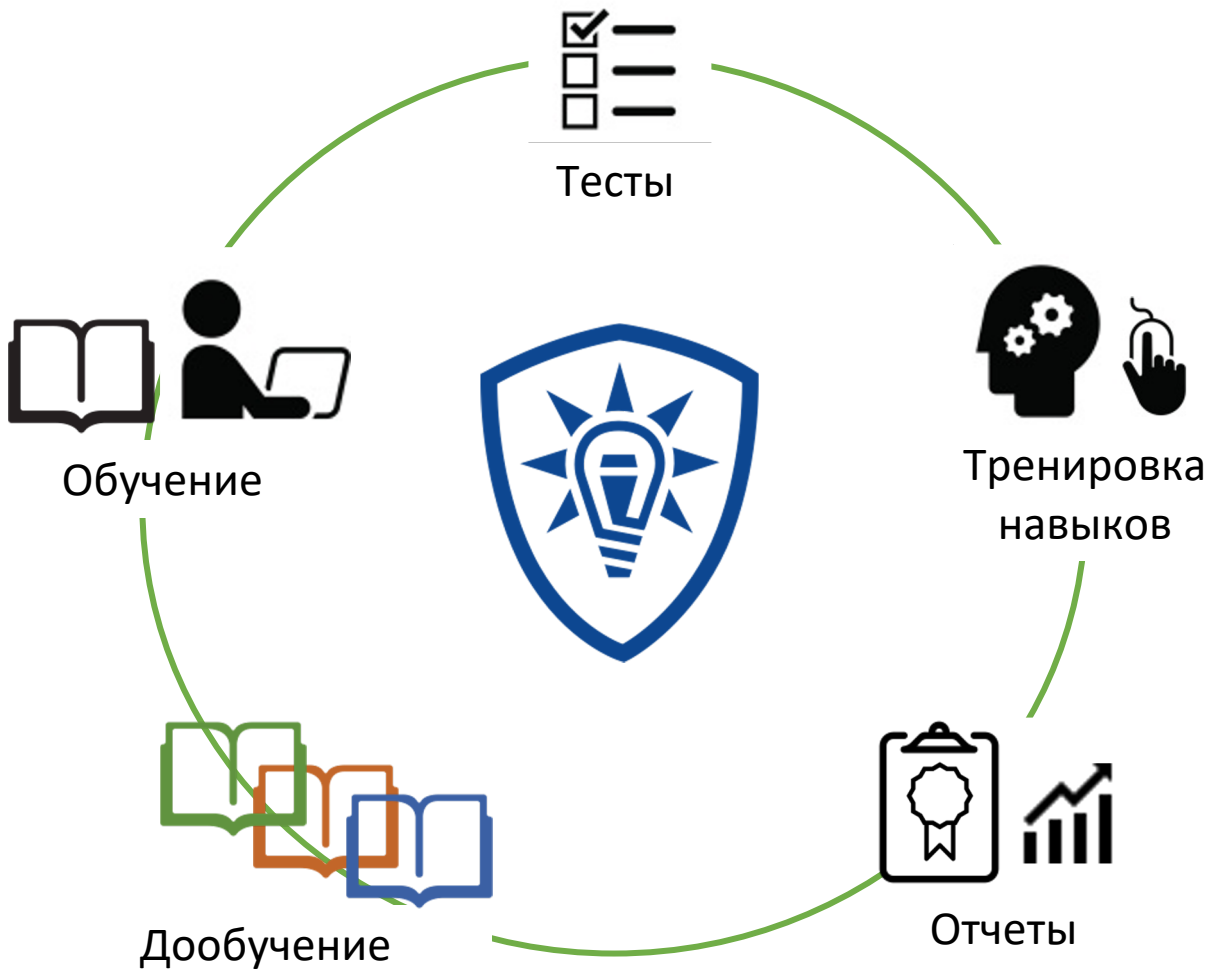
«Скидка 50% при оплате прямо сейчас»

Желание помочь

«Кажется, ваш коллега потерял свои вещи. Дайте мне его номер»


ДОБРО ПОЖАЛОВАТЬ НА КОРПОРАТИВНЫЙ ТРЕНИНГ ПО БЕЗОПАСНОСТИ.
DILBERT.COM @SCOTTADAMSSAYS
НИЧЕГО НЕ ТРОГАЙТЕ, НИКУДА НЕ ХОДИТЕ И НИ С КЕМ НЕ РАЗГОВАРИВАЙТЕ. НИКОГДА!
СПАСИБО, ЧТО ПРИШЛИ.
6-18-20 2020 Scott Adams, Inc./Dist. by Andrews McMeel
И ЭТО ВСЁ?
НЕ МОЯ ВИНА, ЧТО Я УМЕЮ КРАТКО ИЗЛАГАТЬ.

Антифишинг для сотрудников



Платформа для непрерывного обучения и тренировки навыков по безопасности

(Знания + Навыки) x Измерение

Антифишинг для сотрудников

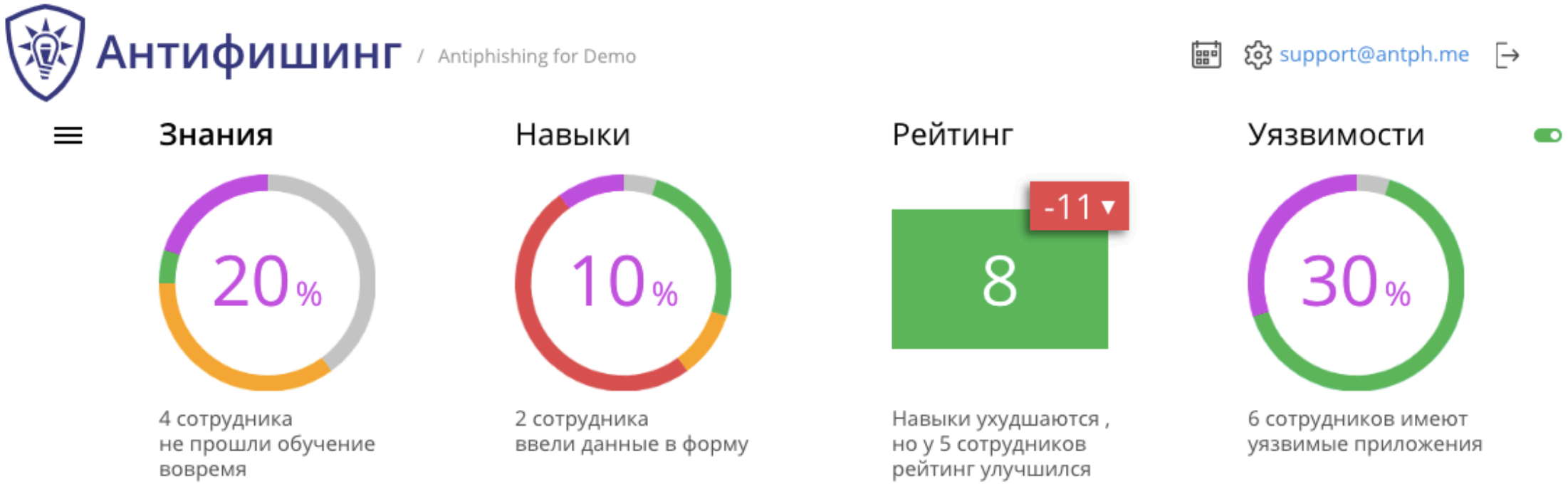
Платформа, которая содержит онлайн-курсы и тесты для обучения, а также шаблоны целевых атак для тренировки и формирования навыков безопасной работы.

Помогает защитить бизнес от цифровых атак на людей.

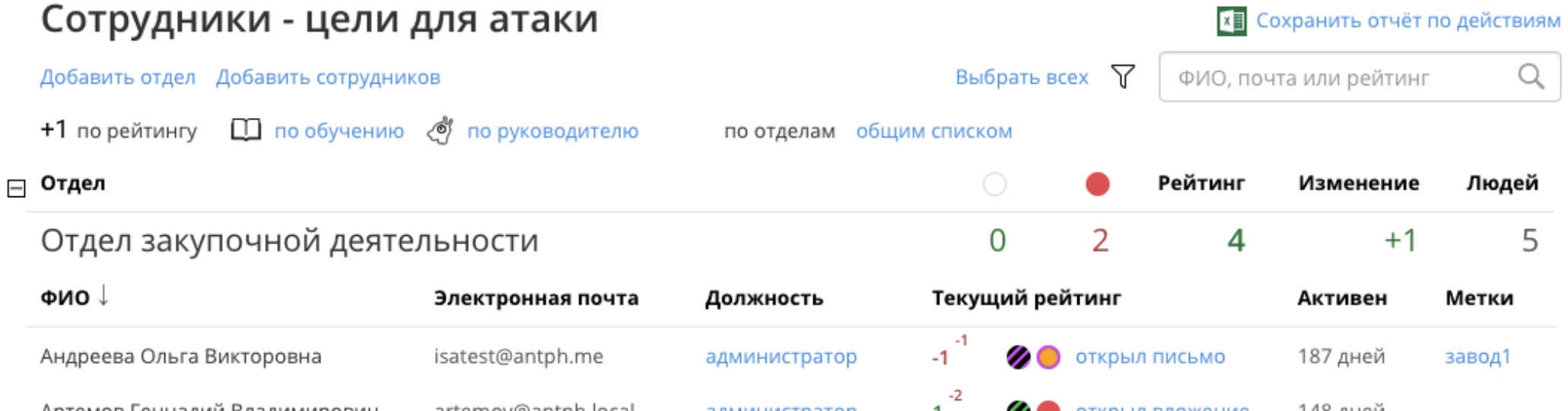
Непрерывно обучать и тренировать удаленных сотрудников.

Выполнять требования регуляторов:

ГОСТ Р 57580.1-2017, 552-П, PCI DSS,
152-ФЗ (ПДн), 187-ФЗ (КИИ) / ФСТЭК 239 XVII ИПО,



SaaS, On-premise



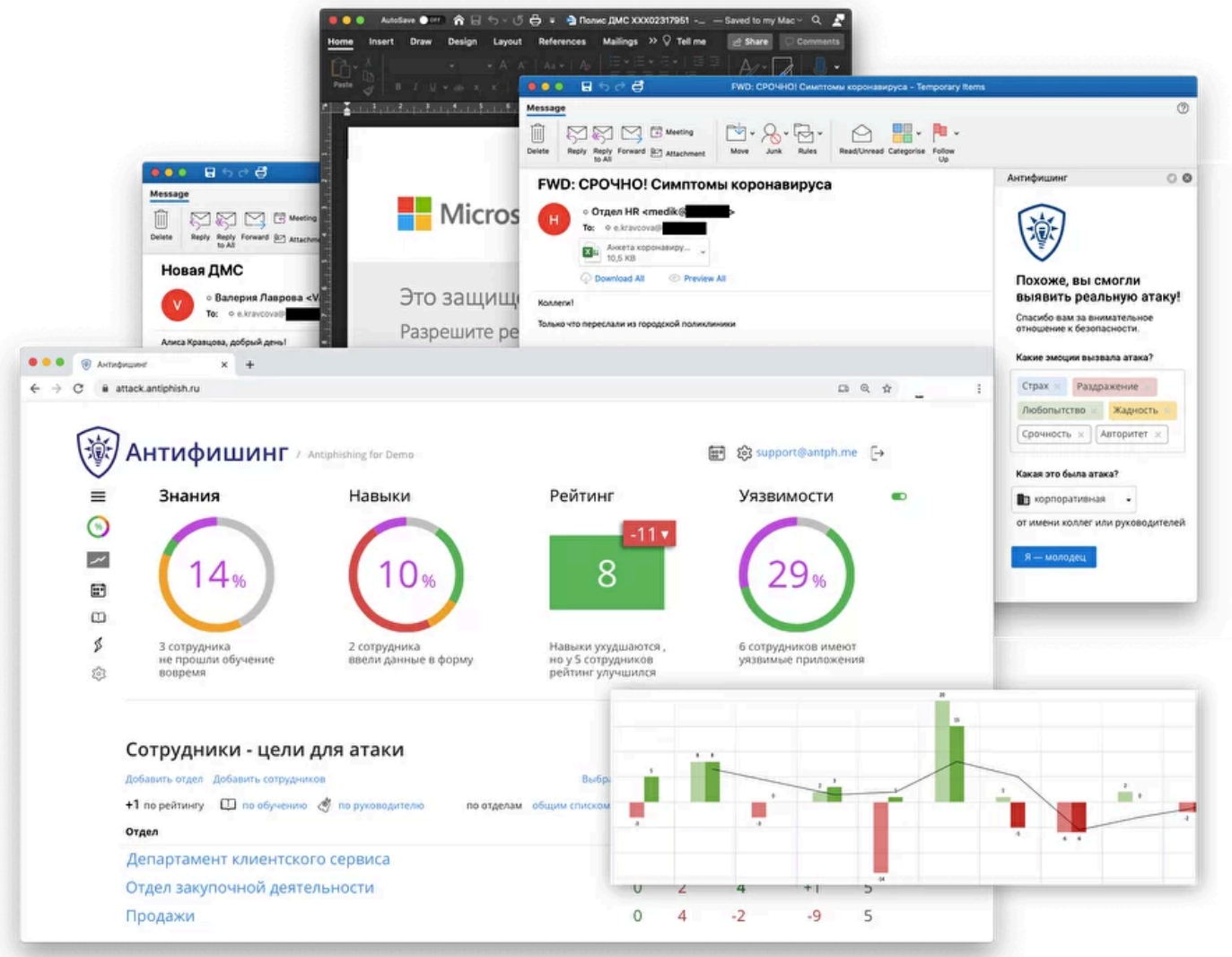
Научим сотрудников защищать свою компанию от цифровых атак

Антифишинг — платформа для формирования навыков противодействия всем видам цифровых атак на людей: через электронную почту, сайты, соцсети, мессенджеры и т.д.

Проверить своих сотрудников

Бесплатно проведём три учебные атаки и покажем слабые места в безопасности компании

Платформа входит в реестр Минкомсвязи



Дополнительные метрики по каждому сотруднику

1. Уровень знаний

Не обучался

Прошел обучение

На обучении

Не прошел обучение вовремя

2. Уровень навыков

Выдержал атаку -5^{-2}

Сообщил об атаке

Открыл письмо 2^{-1}

Перешел по ссылке или открыл файл

Ввел данные в форму

перешел по ссылке

открыл письмо

-213 ▼

1014

3. Опасные уязвимости ПО

.NET 3.0 версий 3.0.30729 и ниже

Shockwave Flash версий 23.0 r0 и ниже

meet.templates.antph.ru/page?token=b4ab775ba60b366f2adc47518d542ec12db5c09e0ac438b51c2159c26bf67c5b

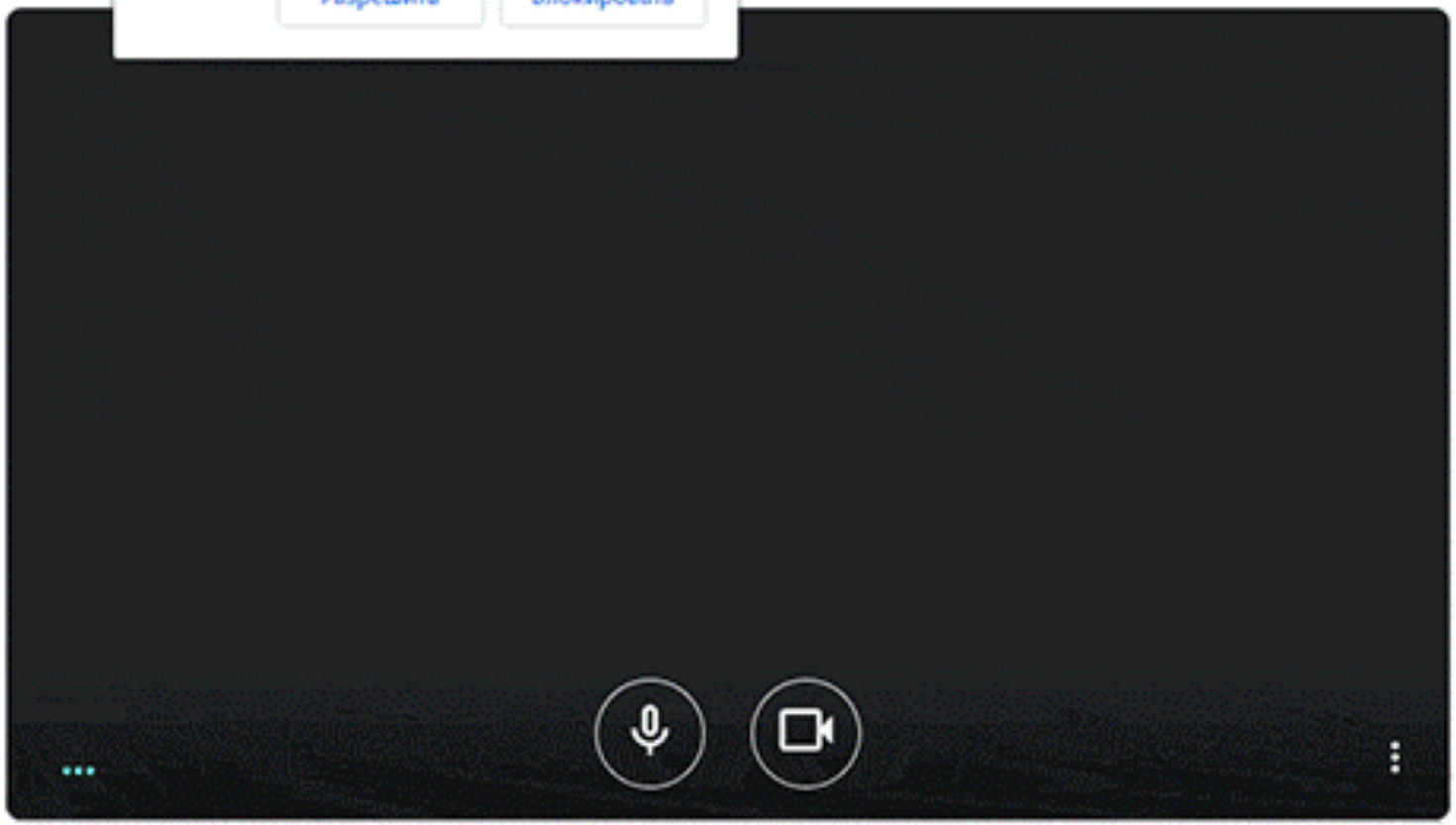
Mee

...ntph.ru запрашивает разрешение на:

Использование микрофона

Использование камеры

Разрешить Блокировать



e.kravcova@antph.me
Алиса Кравцова

16.09.2020 Об

Подключено 2 человек

Присоединиться

Показать на главном экране

Другие параметры

Присоединиться по телефону в режиме голосовой связи

Риски безопасности

Сохранить

Уязвимые приложения | Уязвимые сотрудники

Кол-во	Приложение и версия	Рейтинг	Комментарий
1	Macintosh Mac OS X версий 10_9_3 и ниже		Приложения содержат критические уязвимости и могут использоваться злоумышленниками для проведения ат на пользователей, получения удаленного контроля над системой и проникновения в сеть компании. Рекомендуется обновить приложения
1	Microsoft Outlook версий 16.0.13110 и ниже		
10	Chrome версий 84.0.4147.125 и ниже		
1	Safari версий 7.0.3 и ниже		Приложения содержат незначительные уязвимости. Использование может привести к нестабильной работе будущим рискам безопасности. Рекомендуется обновить приложения
1	Apple Mail версий 13.0 и ниже		

Обзор Антифишинга, платформы обучения и тренировки навыков по кибербезопасности

Павел Лего
Обозреватель Anti-Malware.ru

Проголосовало: 24

Обзоры | Сертификация | Корпорации | Антифишинг | Антифишинг | ...

«Антифишинг» — система, которая содержит электронные курсы и тесты, а также сценарии и шаблоны имитированных атак для непрерывного обучения, повышения осведомлённости, тренировки навыков сотрудников. Мы рассмотрим версию продукта 2.4.2, которая доступна клиентам с августа 2020 года.

www.amtestlab.ru
CERTIFIED
AM
TEST LAB
REG # 00311 10/2020

Сертификат AM Test Lab

Номер сертификата: 311

Дата выдачи: 14.10.2020

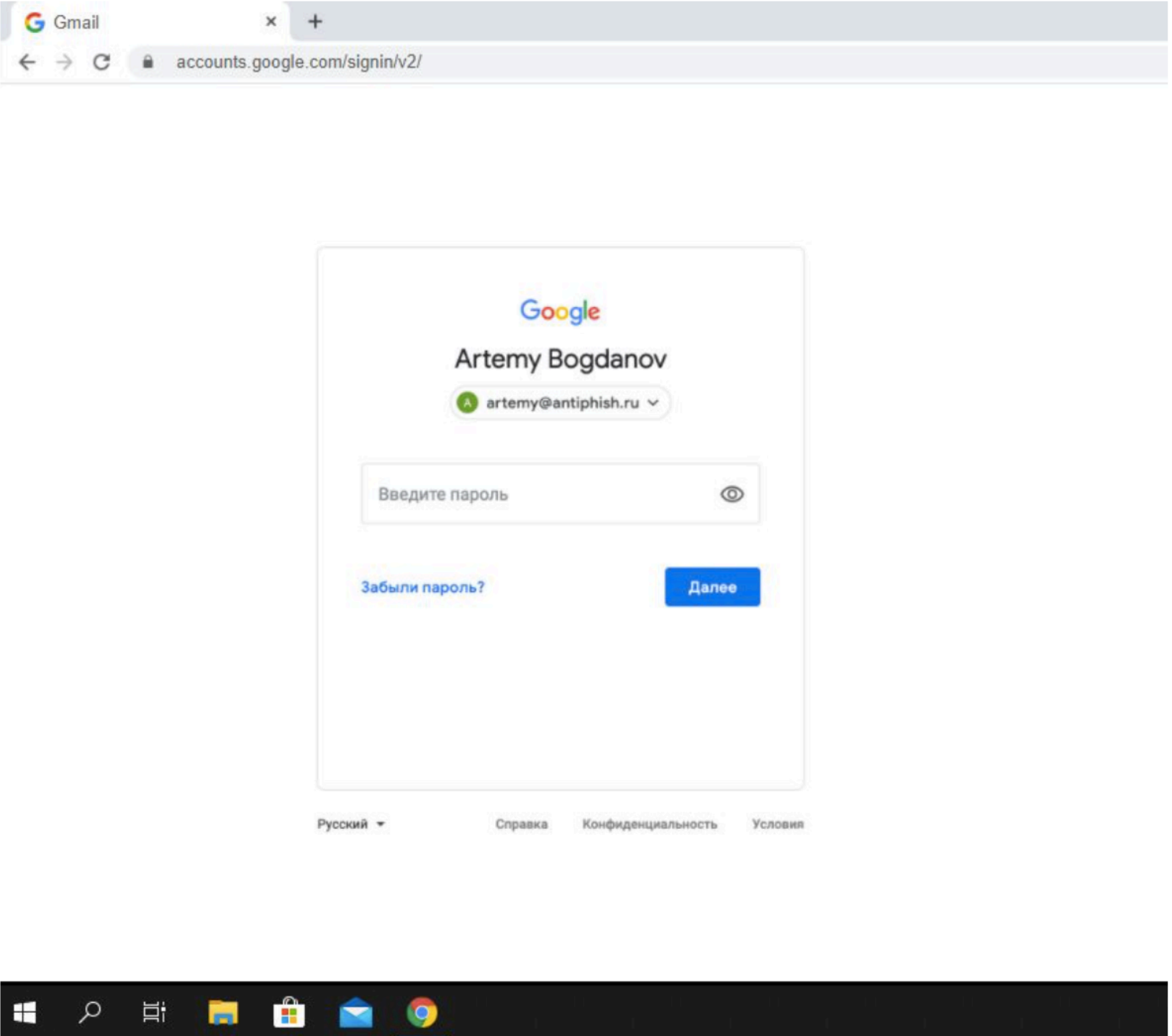
Срок действия: 14.10.2025

Реестр сертифицированных продуктов »

https://www.anti-malware.ru/reviews/antiphish

Новый релиз

Версия 2.4.3 уже доступна для пилота


Gmail
accounts.google.com/signin/v2/
Google
Artemy Bogdanov
artemy@antiphish.ru
Введите пароль
Забыли пароль?
Далее
Русский
Справка
Конфиденциальность
Условия

Люди 20%

Обучение 32%

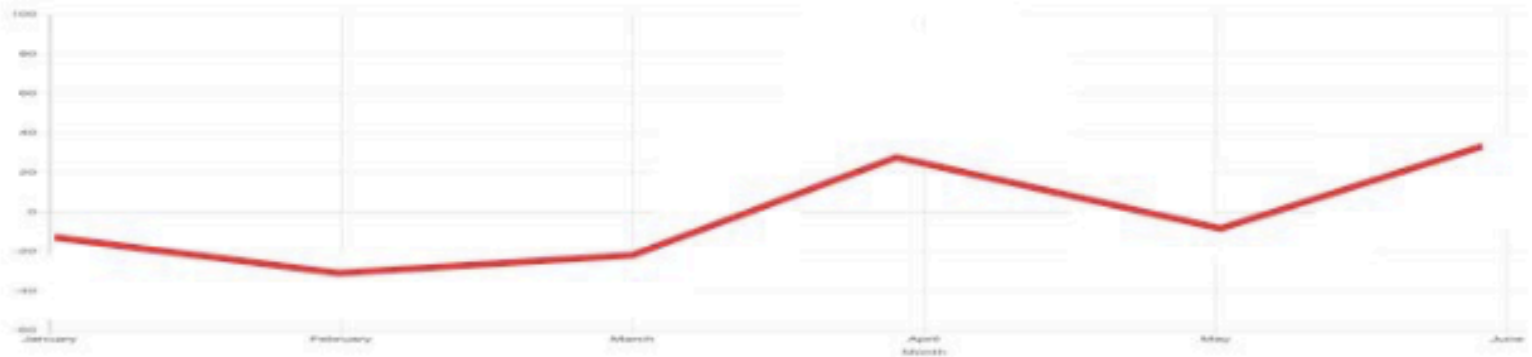
Тренировки 12%

Мотивация A

Только 250 из 1 000 сотрудников добавлены в систему.

Добавьте всех сотрудников

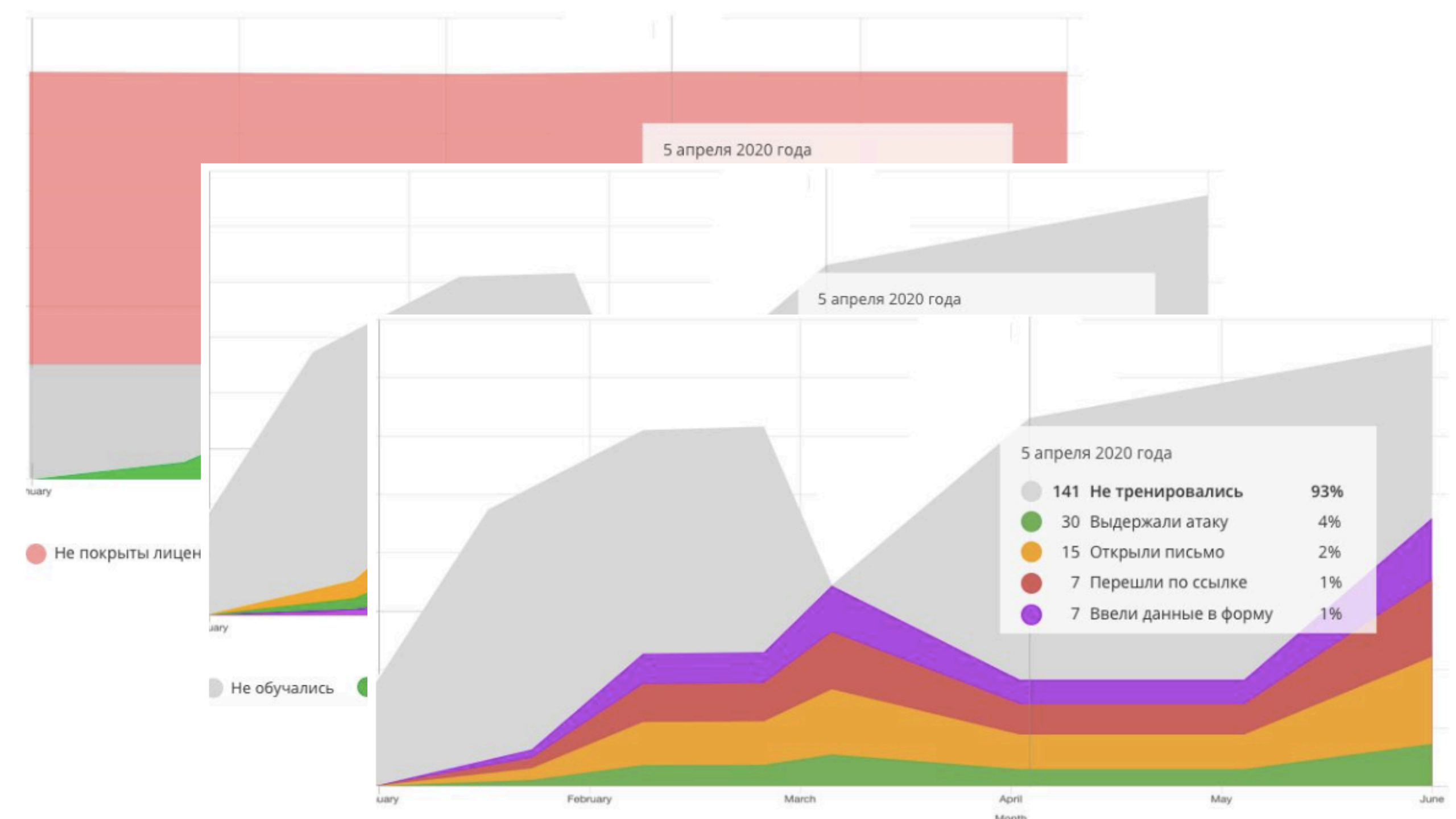
Запланируйте расширение лицензии

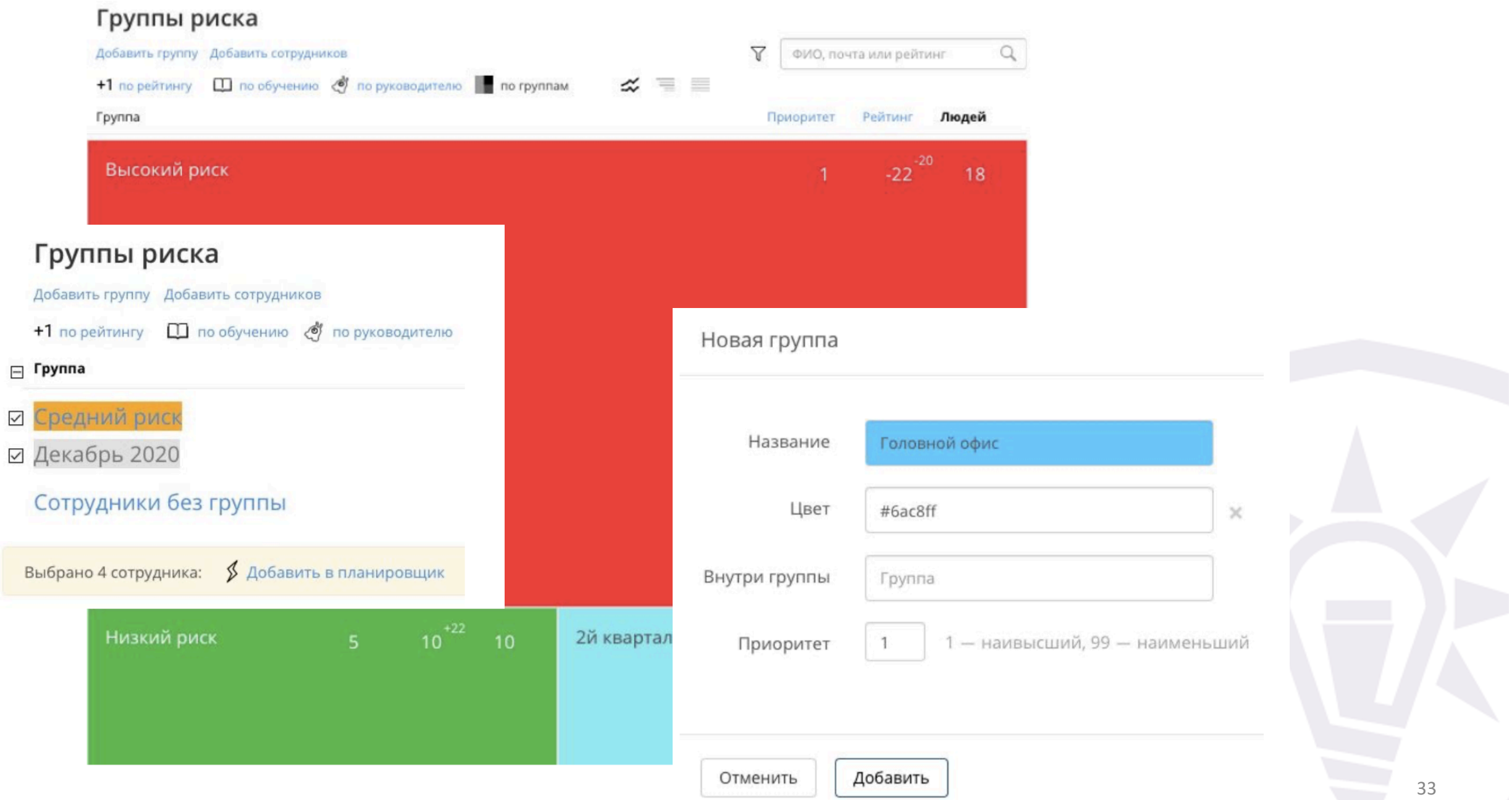


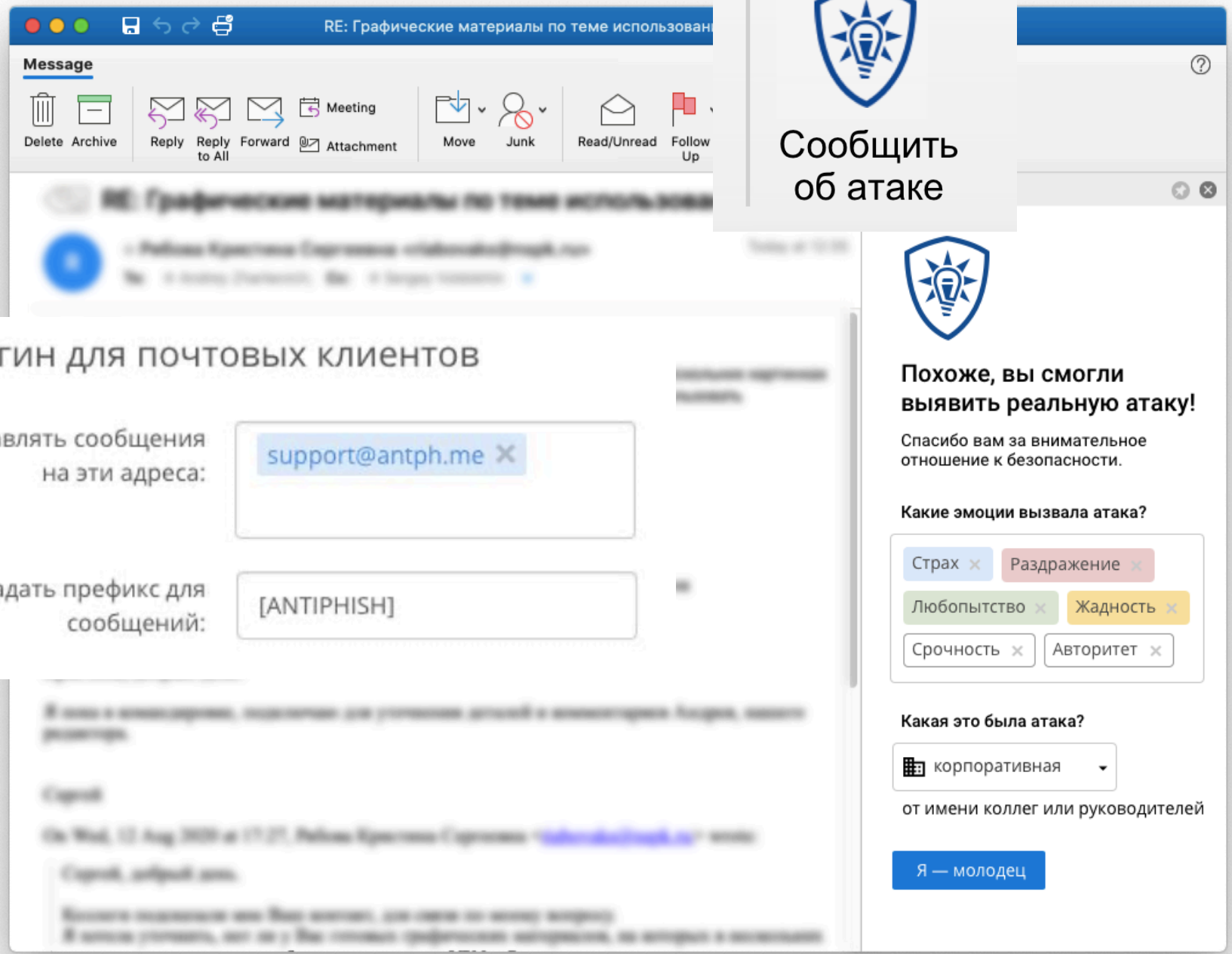
Уровень мотивации — средний

действует с 12 мая 2020 года

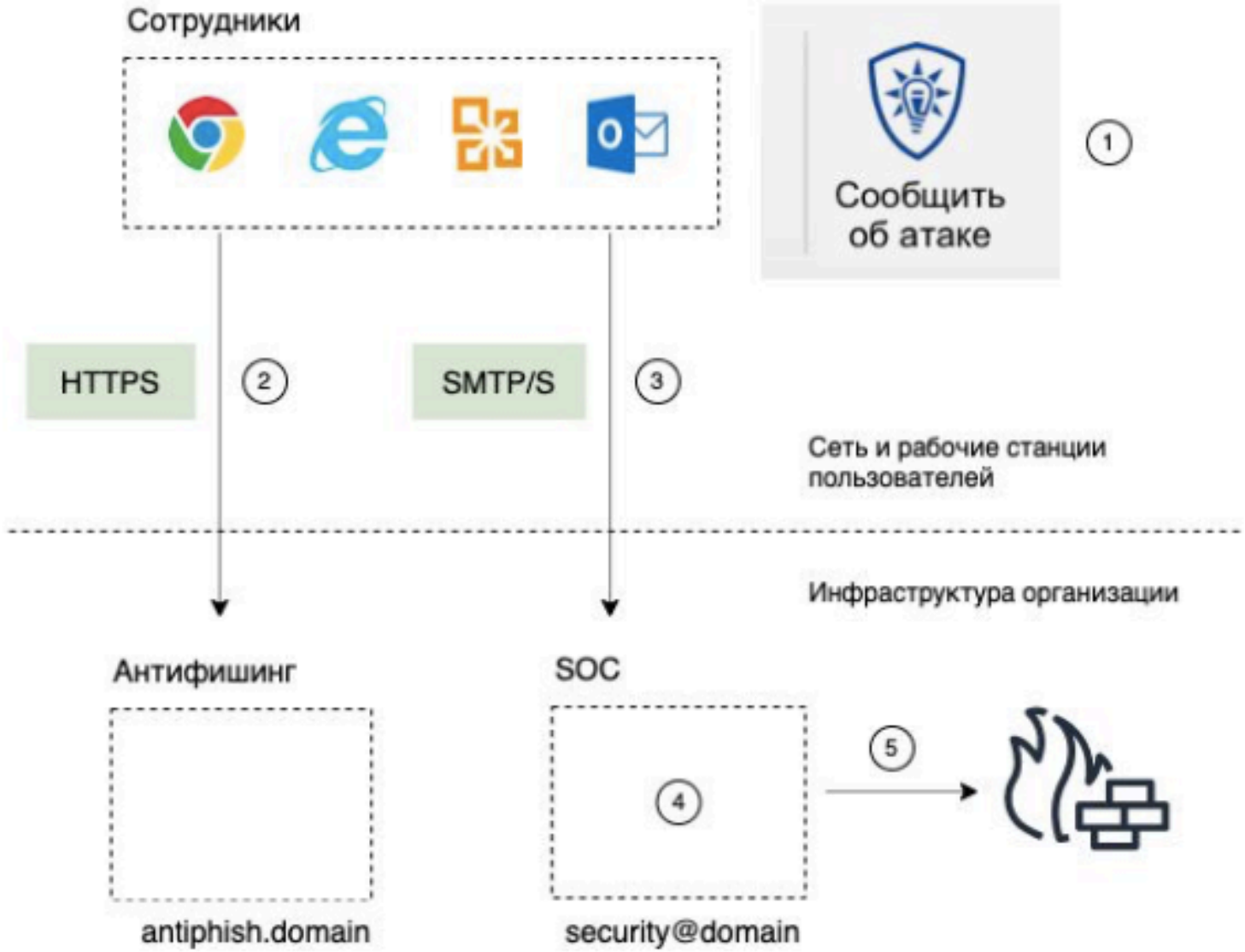
A	B	C	D
Отличный	Хороший	Средний	Низкий


5 апреля 2020 года
Не покрыты лицен
5 апреля 2020 года
Не обучались
5 апреля 2020 года
141 Не тренировались 93%
30 Выдержали атаку 4%
15 Открыли письмо 2%
7 Перешли по ссылке 1%
7 Ввели данные в форму 1%
February
March
April
May
June


Группы риска
Добавить группу
Добавить сотрудников
ФИО, почта или рейтинг
+1 по рейтингу
по обучению
по руководителю
по группам
Группа
Приоритет
Рейтинг
Людей
Высокий риск
1
-22
-20
18
Группы риска
Добавить группу
Добавить сотрудников
+1 по рейтингу
по обучению
по руководителю
Группа
Средний риск
Декабрь 2020
Сотрудники без группы
Выбрано 4 сотрудника:
Добавить в планировщик
Низкий риск
5
10
+22
10
2й квартал
Новая группа
Название
Головной офис
Цвет
#6ac8ff
Внутри группы
Группа
Приоритет
1
1 — наивысший, 99 — наименьший
Отменить
Добавить


RE: Графические материалы по теме использовани
Message
Delete
Archive
Reply
Reply to All
Forward
Meeting
Attachment
Move
Junk
Read/Unread
Follow Up
Плагин для почтовых клиентов
Отправлять сообщения на эти адреса:
support@antph.me
Задать префикс для сообщений:
[ANTIPHISH]
Похоже, вы смогли выявить реальную атаку!
Спасибо вам за внимательное отношение к безопасности.
Какие эмоции вызвала атака?
Страх
Раздражение
Любопытство
Жадность
Срочность
Авторитет
Какая это была атака?
корпоративная
от имени коллег или руководителей
Я — молодец

Сообщить об атаке


Сотрудники
Сообщить об атаке
1
HTTPS
2
SMTP/S
3
Сеть и рабочие станции пользователей
Инфраструктура организации
Антифишинг
SOC
4
5
antiphish.domain
security@domain

Антифишинг — устав пилота

Файл Правка Вид Вставка Формат Инструменты Дополнения Справка Последнее изменение: Evgenii Malov 6 августа 2020 г.

100% Название Arial 26

Антифишинг — устав пилота

План, сценарии и критерии успеха пилотного внедрения

© ООО «Антифишинг», 2020

Грамотные сотрудники –
ваша лучшая защита.

Обучайте и тренируйте своих людей.

ДиалогНаука

ask@antiphish.ru
www.antiphish.ru

marketing@dialognauka.ru
www.dialognauka.ru