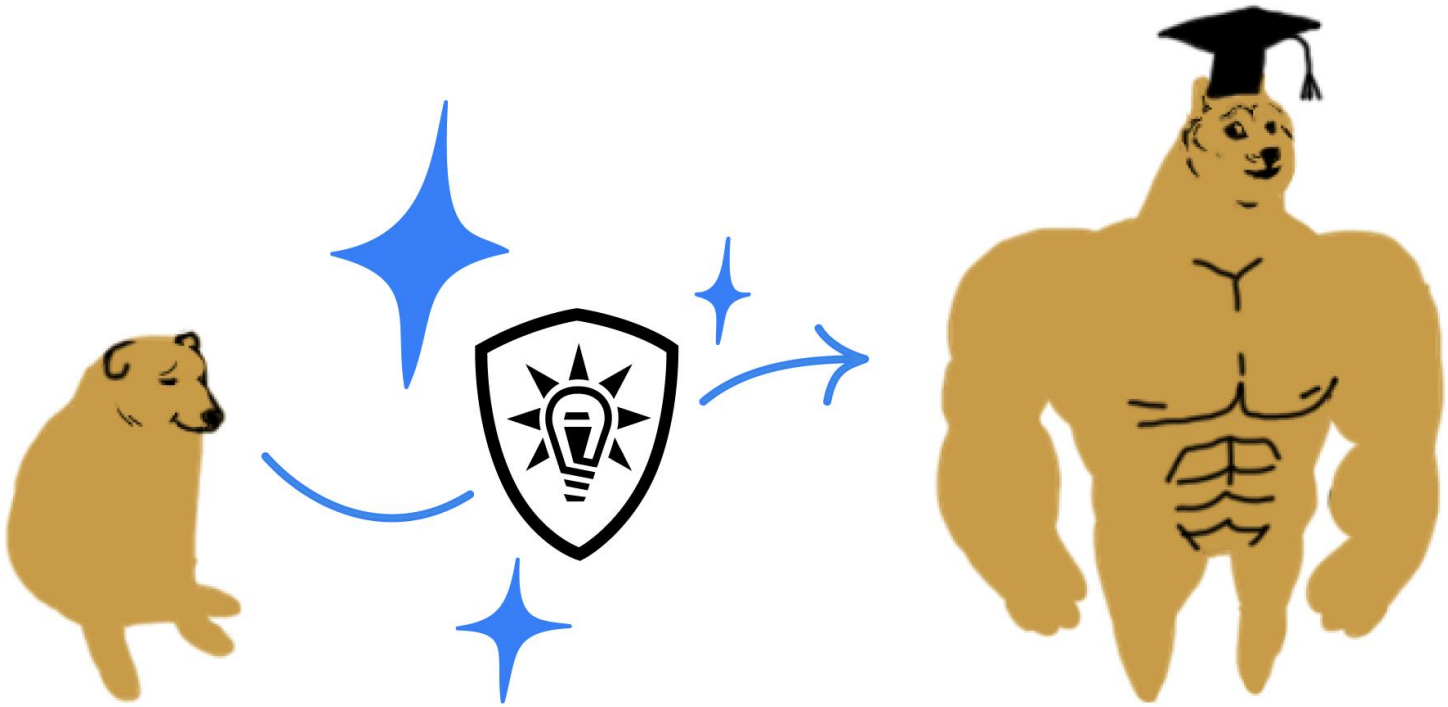
www.antiphish.ru



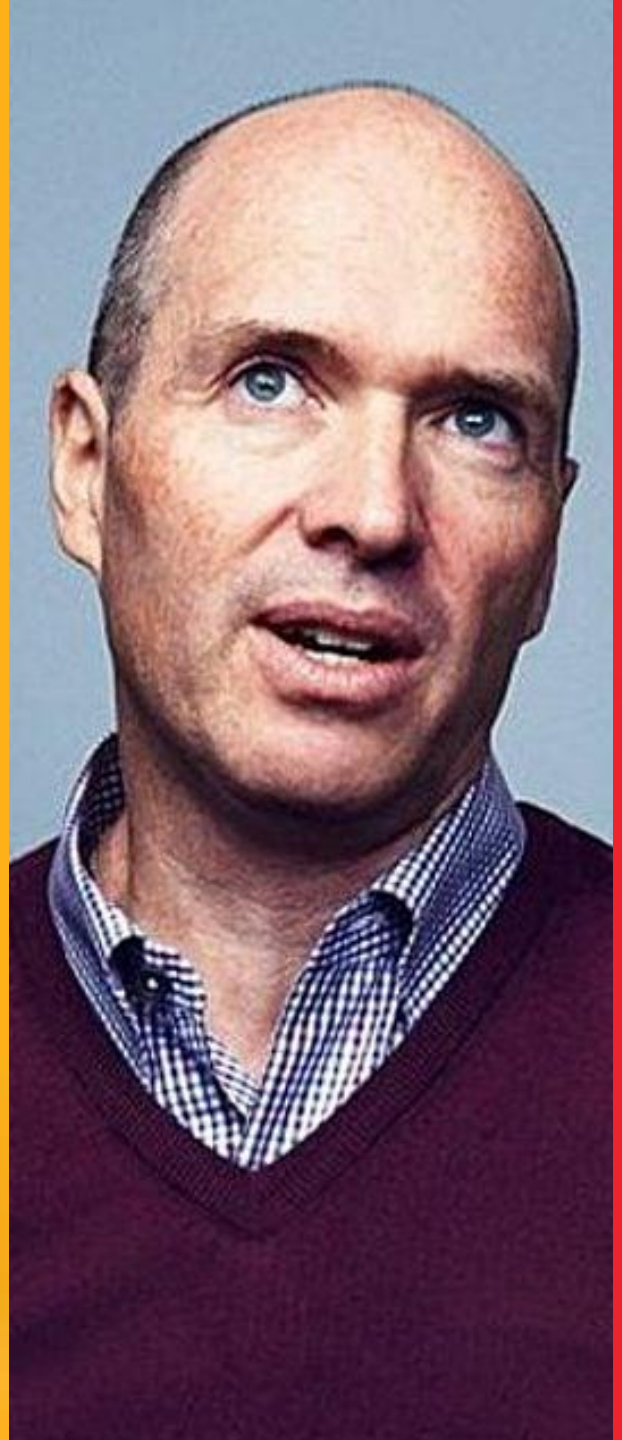
Культура безопасности

Ожидания и реальность. Как перейти от слов к делу

Бен Хоровиц

ЛЕГКО не БУДЕТ

Как построить бизнес, когда вопросов больше, чем ответов

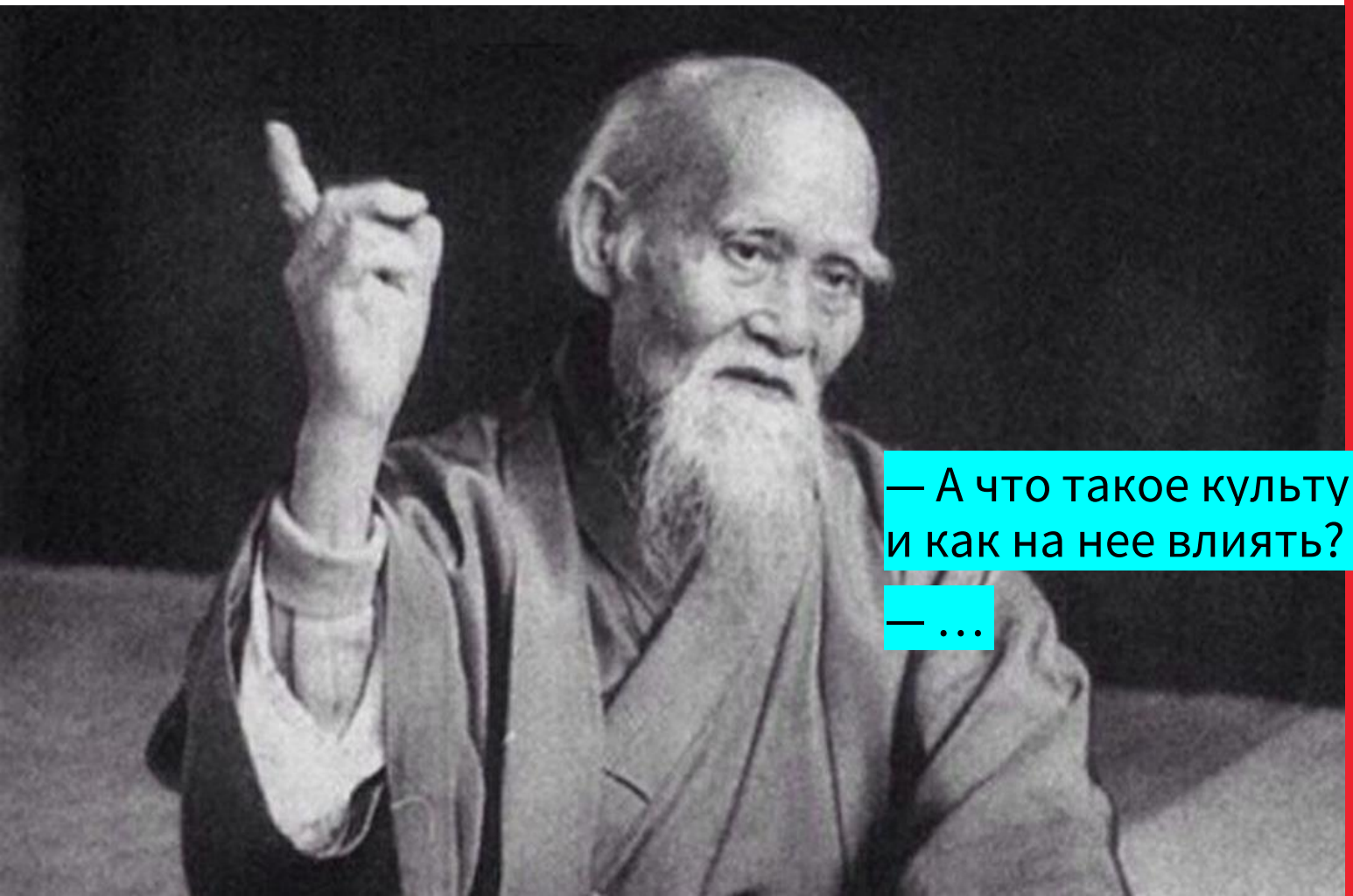


БЕН ХОРОВИЦ

МЫ — ТО, ЧТО МЫ ДЕЛАЕМ

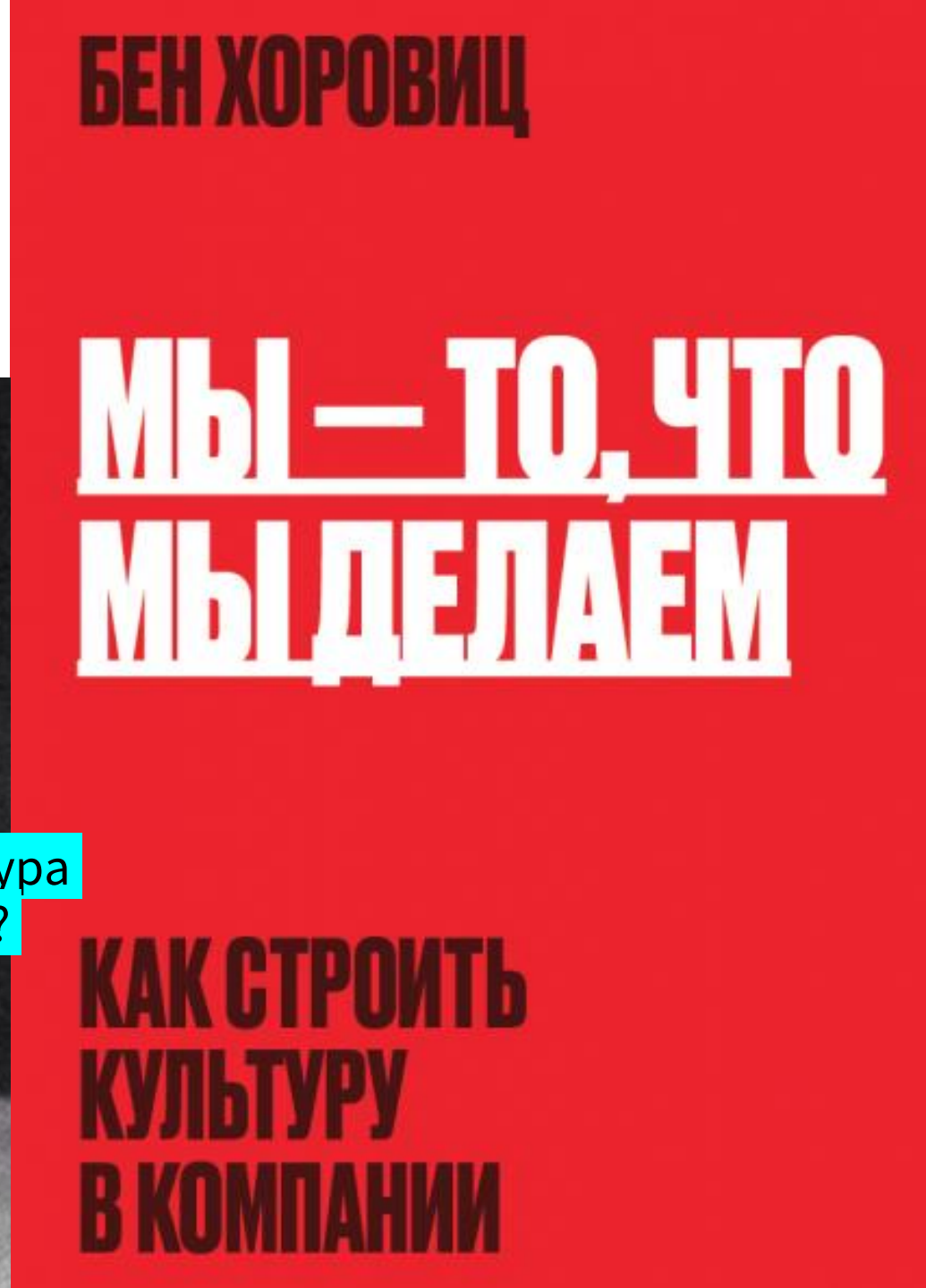
КАК СТРОИТЬ КУЛЬТУРУ В КОМПАНИИ

Удели особое внимание культуре компании. Она важнее всего!



— А что такое культура и как на нее влиять?

— …



Непростые вопросы

Наш продукт не соответствует требованиям, мы должны честно сказать об этом, или заявим соответствие и понадеемся, что клиент не обратит внимание?

Я должен прийти на эту встречу вовремя?

Можно ли уходить домой в пять вечера или нужно задержаться до восьми?

Я должен перезвонить клиенту сегодня же, или можно подождать до завтра?

Если я знаю, что в компании есть серьезные проблемы, стоит ли говорить об этом? И к кому обратиться?

Что важнее — победа или этика?

Ответы сотрудников на такие вопросы – и есть культура компании

Вопросы про безопасность — попроще

— Шеф звонит и требует выслать отчет через пять минут, но он у меня в офисе на рабочем столе. Скажу Любе пароль, чтобы она зашла в компьютер и переслала?

— Пишут «из поддержки» и просят запустить файл обновления, наверное надо сделать?

— Мне пришло счет_на_оплату.js ну я и открыл а что такое это же мне надо счета оплачивать у меня работа такая

Ответы сотрудников на такие вопросы – и есть культура безопасности компании

Вопросы про безопасность — посложнее

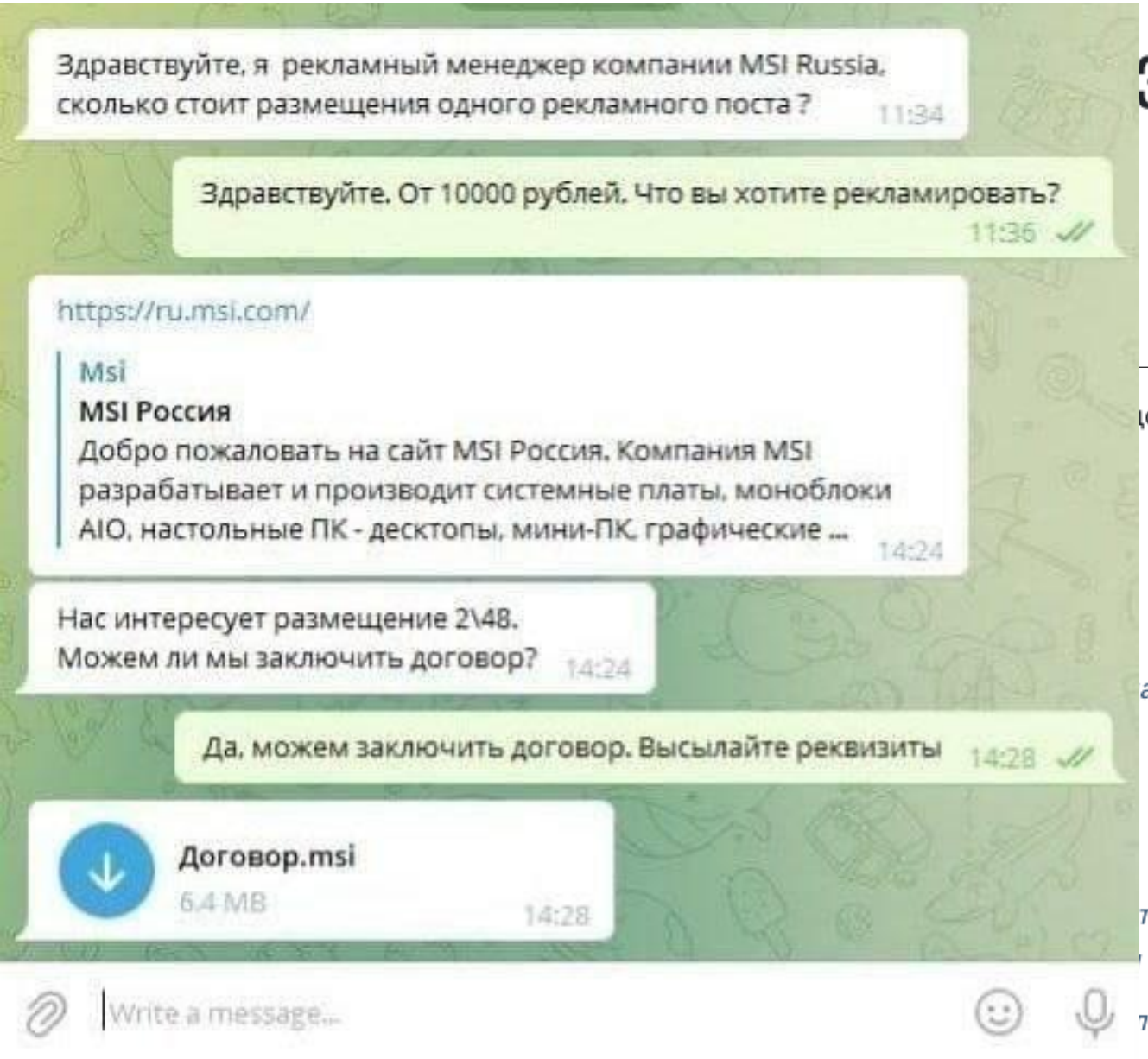
— Начальник требует доработать отчет, мне надо забирать ребенка из сада, а удаленку запретили. Я же могу отправить файлы себе на личную почту?

— Система требует сменить пароль, но придумывать новый лень, да и как запомнить непонятно, добавлю-ка новую цифру в конец, я уже три раза так делал11111

— Контрагент торопит с оплатой, я вижу, что реквизиты поменялись, но банк вроде тот же, обновлю в 1С и отправлю уже платежку

Ответы сотрудников на такие вопросы – и есть культура безопасности компании

Цена неправильных ответов



ЭТО СТАЛО ВОЗМОЖНЫМ СЕЙЧАС

https://mobile-review.com/all/articles/misc/u-nas-ukrali-youtube-kanal-kak-eto-stalo-vozmozhnym-i-chto-proishodit-sejchas/

обивается своего, более того, дальше общение идет очень мило.

аже если убрать scr.

ть вирус, мы честная компания, лидирующая в сегменте бюджетных гаджетов,
имею прямое отношение к компании Tecno
ли, возможно это какой то баг, я сейчас смотрю и у меня все хорошо.

Культура — это то, как люди принимают решения в ваше отсутствие и как ведут себя, когда никто не смотрит.

Культура — это ряд принципов для урегулирования повседневных проблем [безопасности].

Если не строить культуру компании скрупулезно и методично, то две ее трети будут случайным явлением, а оставшаяся треть — чудовищной ошибкой

Что знают коллеги, у которых получилось?

Безопасность— это бизнес-партнер.
Как HR-бизнес-партнер, только ИБ.
Задача ИБ — помогать, а не запрещать.

Бизнес говорит, чего он хочет — ИБ говорит, как это сделать с минимальными издержками и максимальной безопасностью.

Безопасность открыта для диалога.
Мы не просто спускаем требования,
а слушаем бизнес.

Правила прививаются только через принятие, ты не можешь повлиять на людей, если сам не открыт для влияния. Всегда понятно, к кому можно зайти или написать, если есть проблемы.

Безопасность — ответст[illegible]ость каждого.
Все должны понять, что [illegible]лать безопасно — это их работа.

Для этого ИБ плотно [illegible]ирует с руководите[illegible]не воспитае[illegible] непосред[illegible] помогае[illegible]

Идеальн[illegible]ко[illegible]ма[illegible]ИБ должен ум[illegible]б[illegible]ть [illegible]ть людей

Говорить на понятн[illegible]языке, находить баланс между системами и людьми, проявлять эмпатию к пользователям.

Коммуникация — ключевая компетенция безопасности

Безопасность— это бизнес-партнер.
Как HR-бизнес-партнер, только ИБ.
Задача ИБ — помогать, а не запрещать.

Бизнес говорит, чего он хочет — ИБ говорит, как это сделать с минимальными издержками и максимальной безопасностью.

Безопасность открыта для диалога.
Мы не просто спускаем требования,
а слушаем бизнес.

Правила прививаются только через принятие, ты не можешь повлиять на людей, если сам не открыт для влияния. Всегда понятно, к кому можно зайти или написать, если есть проблемы.

Безопасность — ответственность каждого.
Все должны понять, что делать безопасно — это их работа.

Для этого ИБ плотно контактирует с руководителями, потому что никто не воспитает культуру ИБ так, как непосредственный руководитель. ИБ помогает, но не делает за тебя.

Идеальный руководитель команды ИБ должен уметь объяснять и вовлекать людей

Говорить на понятном языке, находить баланс между системами и людьми, проявлять эмпатию к пользователям.

Хорошая коммуникация по безопасности:

1. Повышает осведомленность
2. Улучшает понимание
3. Развивает навыки
4. Поддерживает ре-трансляции

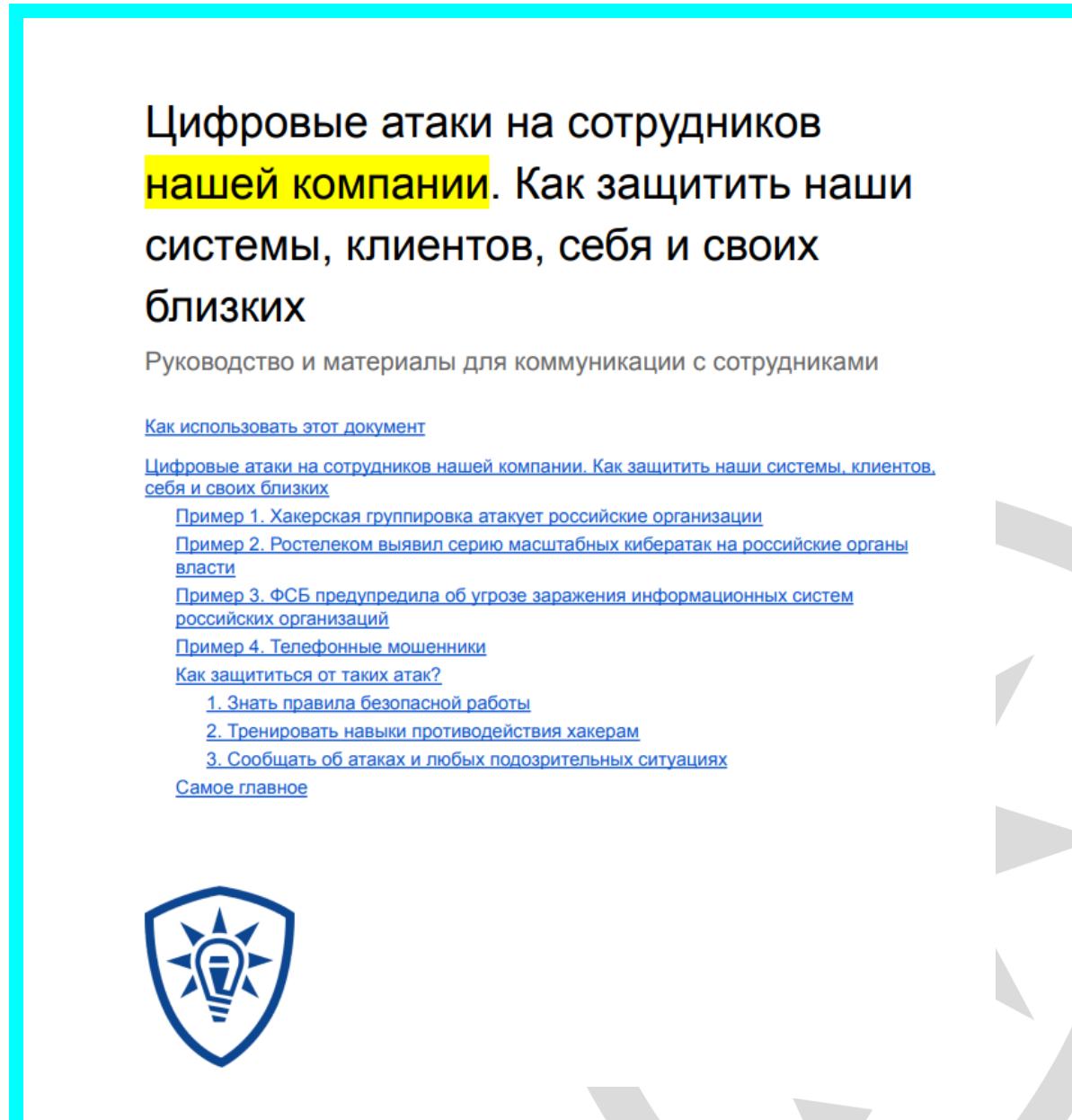
Квест: найдите автора мема в этом зале и получите ценный совет по коммуникации

Коммуникация. Повышаем осведомленность

1. У компании должно быть представление о состоянии дел в ИБ, которое достигается через аудиты и средства мониторинга. Люди должны быть в курсе, как дела. Если происходят инциденты, о них нужно рассказывать.
2. Коммуникация об опасностях: надо рассказывать про новые хаки и эксплойты.
3. Не только негатив: если была атака и мы с ней справились об этом надо тоже сказать. Достижения — важно, надо писать в интранет и может даже на Хабр.
4. Переходить от абстрактных запугиваний к конкретным наглядным мероприятиям: имитация атак, пен-тест, киберучения, полигон, вот Тесла, давайте ее сломаем.
5. Коммуникации МОЖЕТ быть слишком много. Нужно взвешивать интересность темы и занятость людей. Ты как мальчик, который кричит «волк», нельзя это делать слишком часто.

Коммуникация. Улучшаем понимание

1. Проблема дисциплины — это проблема непонимания. Нужно доносить ценность решений (зачем второй фактор аутентификации?) и отрабатывать возникающий негатив. Для этого надо быть открытым к негативу, иначе он копится, а ты не знаешь.
2. Не запрещать, а объяснять! Проводить игры, учения, объяснять через личные бытовые примеры.

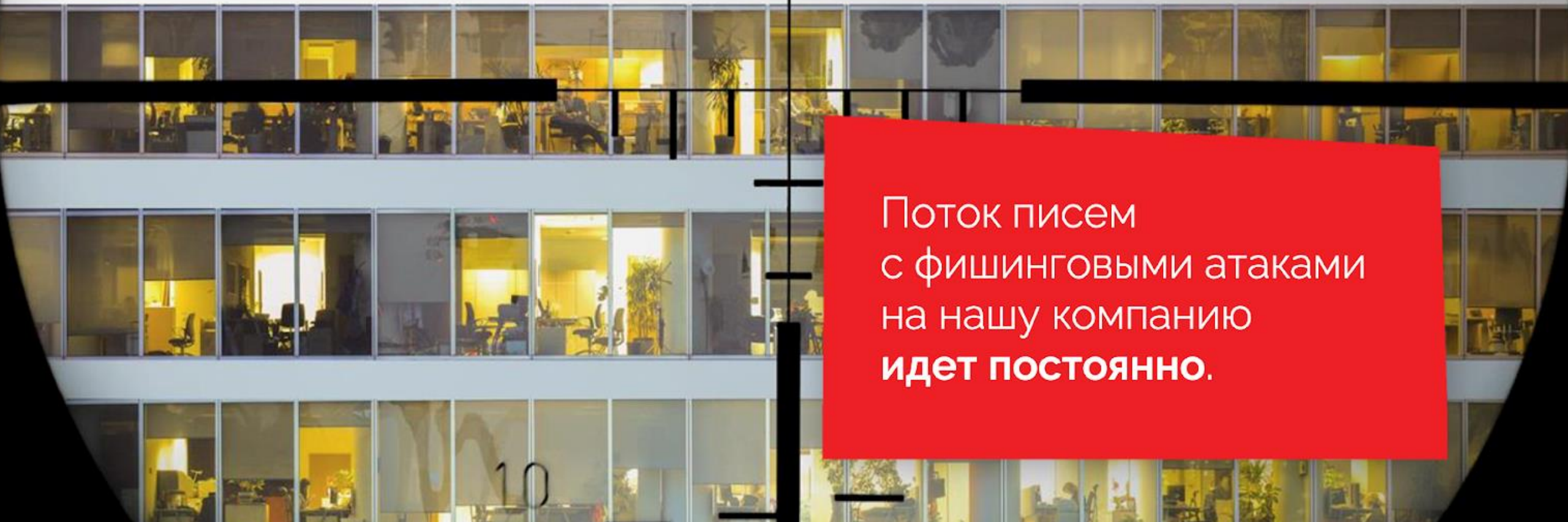


Цифровые атаки на сотрудников нашей компании. Как защитить наши системы, клиентов, себя и своих близких

Руководство и материалы для коммуникации с сотрудниками

Вы уже под прицелом

Рассылка фишинговых писем и заражение компьютеров обычно выполняются в **автоматическом режиме**, поэтому один хакер может одновременно атаковать **десятки тысяч потенциальных жертв.** Вероятность получить фишинговое письмо для каждого сотрудника очень большая.



Поток писем с фишинговыми атаками на нашу компанию **идет постоянно**.

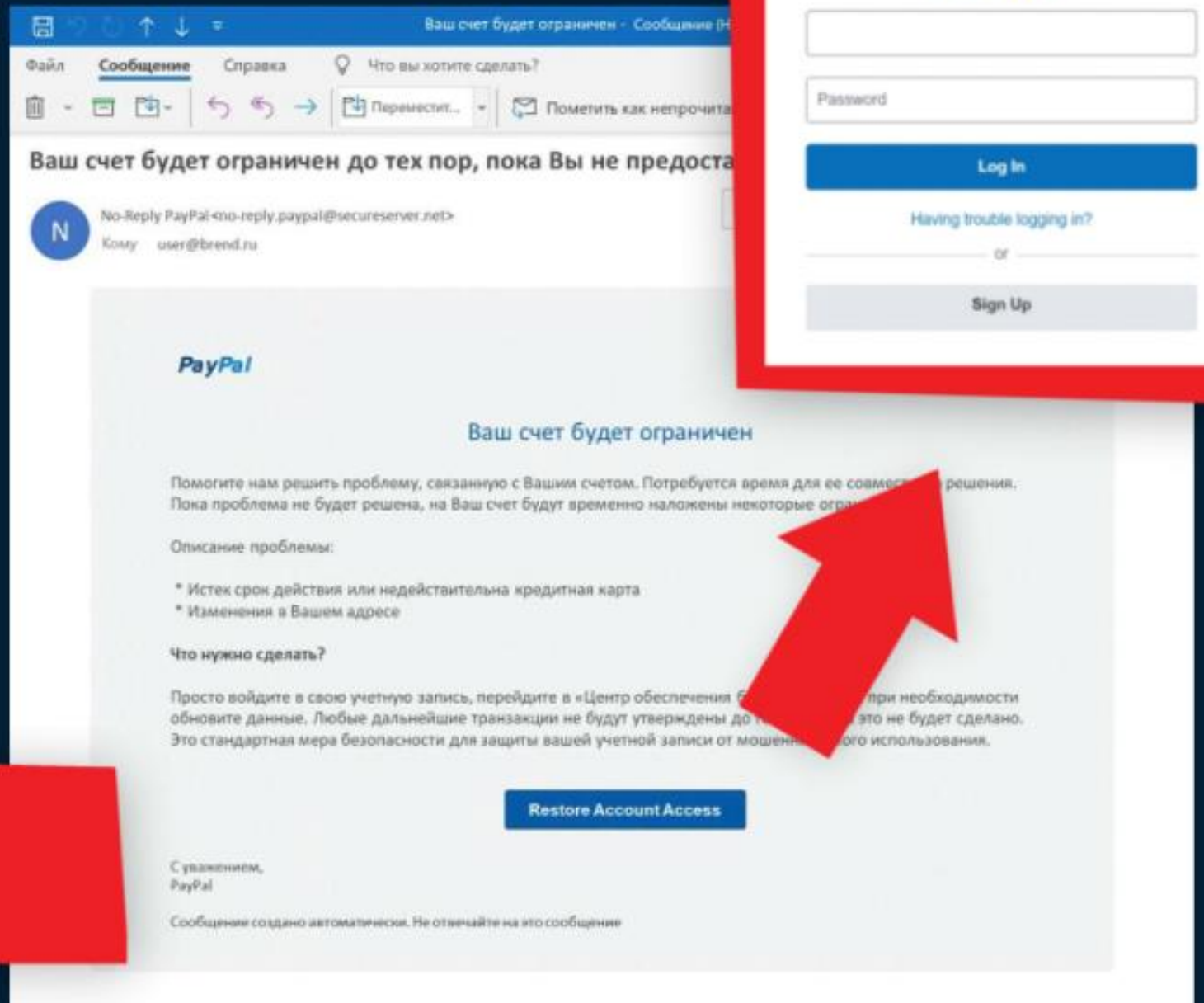
Разбор атаки от имени PayPal

Посмотрите внимательно на это письмо. Его отправил мошенник.

С виду оно ничем не отличается от обычного, но не все так просто. Посмотрите, как действовали мошенники в этом случае.

В письме говорится о проблемах с PayPal и предлагается нажать на кнопку, чтобы решить проблему. При нажатии на кнопку происходит переход на сайт, очень похожий на официальный сайт PayPal.

Такое письмо может прийти и вам! Давайте узнаем подробнее, как устроена эта атака



Коммуникация. Развиваем навыки

1. Прививать простые, даже «тупые» привычки: не знаешь — вот чатик, посоветуйся. Сомневаешься — не открывай. Не связывайся по каналу, который тебе навязывают (если тебе звонят, скажи что перезвонишь по официальному номеру)

Нет привычки
и простого алгоритма

2. Если есть понимание ценности, обучение проходит легко.
Но все равно нужно четко понимать аудиторию. Разрабам нужно одно, девопсам другое, простым сотрудникам — третье.

тового ящика

22:28
22:01
22:01
20:45
20:40
18:10
18:08
15:41
14:57

Счет на оплату

СА Соколова Анна Дмитриевна <sokolova.vis@oat-group.ru> <sokolova.vis-oat-group.ru@templates.antph.ru>
Кому orlenko@antiphish.ru

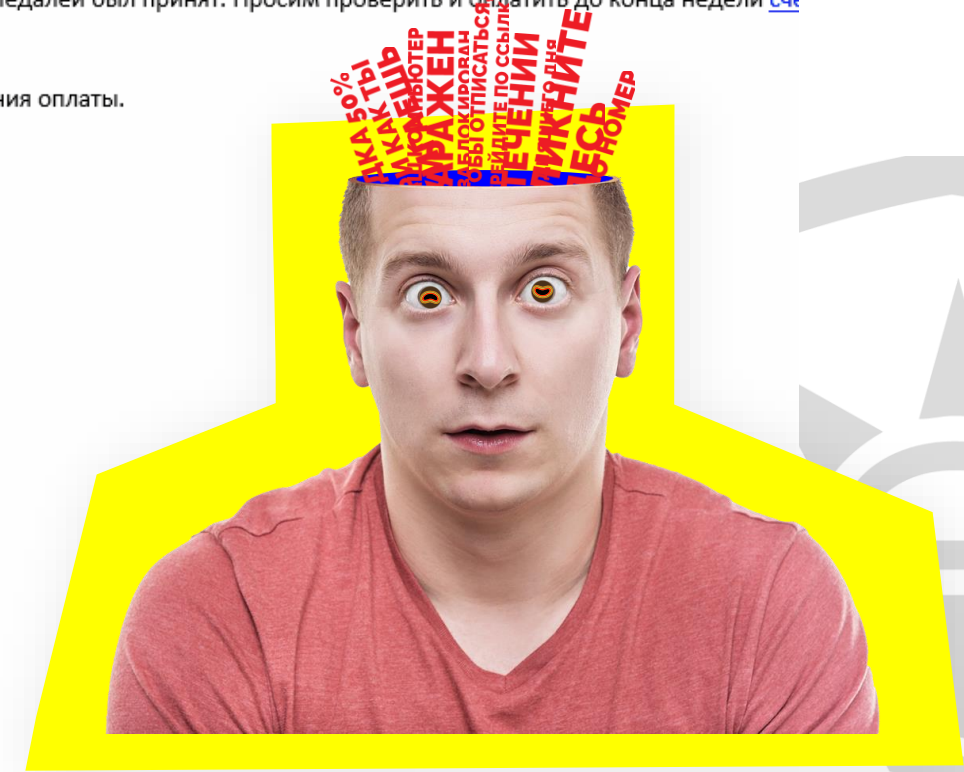
Ответить Ответить всем

Счет_8901_9 декабря 2019.docx
41 KB

Здравствуйте, Александр!

Ваш заказ на производство и поставку узлов и компонентов подвески, тормозной системы и блоков педалей был принят. Просим проверить и оплатить до конца недели сче
декабря 2019 года (во вложении).

Сообщите, когда планируете отправить платеж. Производство будет начато сразу после подтверждения оплаты.



С уважением,

Менеджер по продажам

Соколова Анна Дмитриевна

Тел.: +7 (8482) 69-15-21

vazinter.ru

АКЦИОНЕРНОЕ ОБЩЕСТВО
ВАЗИНТЕРСЕРВИС

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

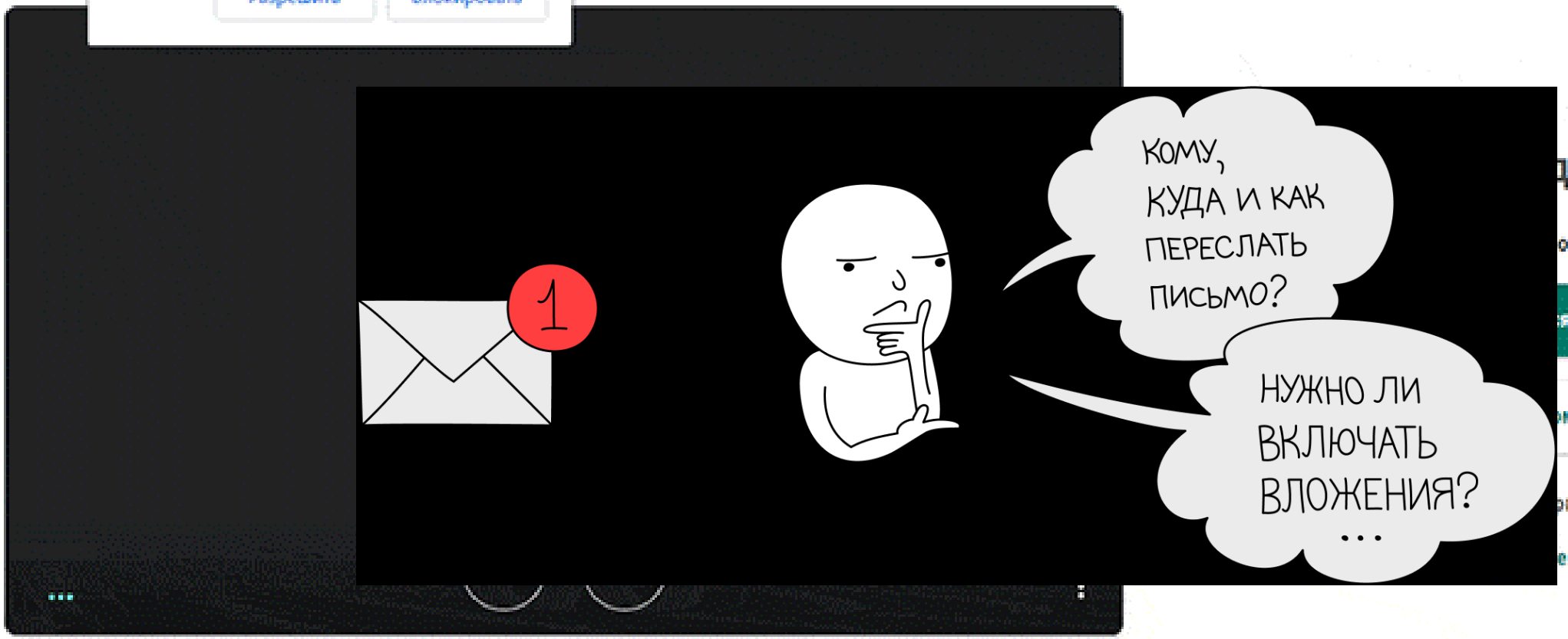
...ntph.ru запрашивает разрешение на:

Использование микрофона

Использование камеры

Разрешить | Блокировать

e.kravcova@antph.me
Алиса Кравцова



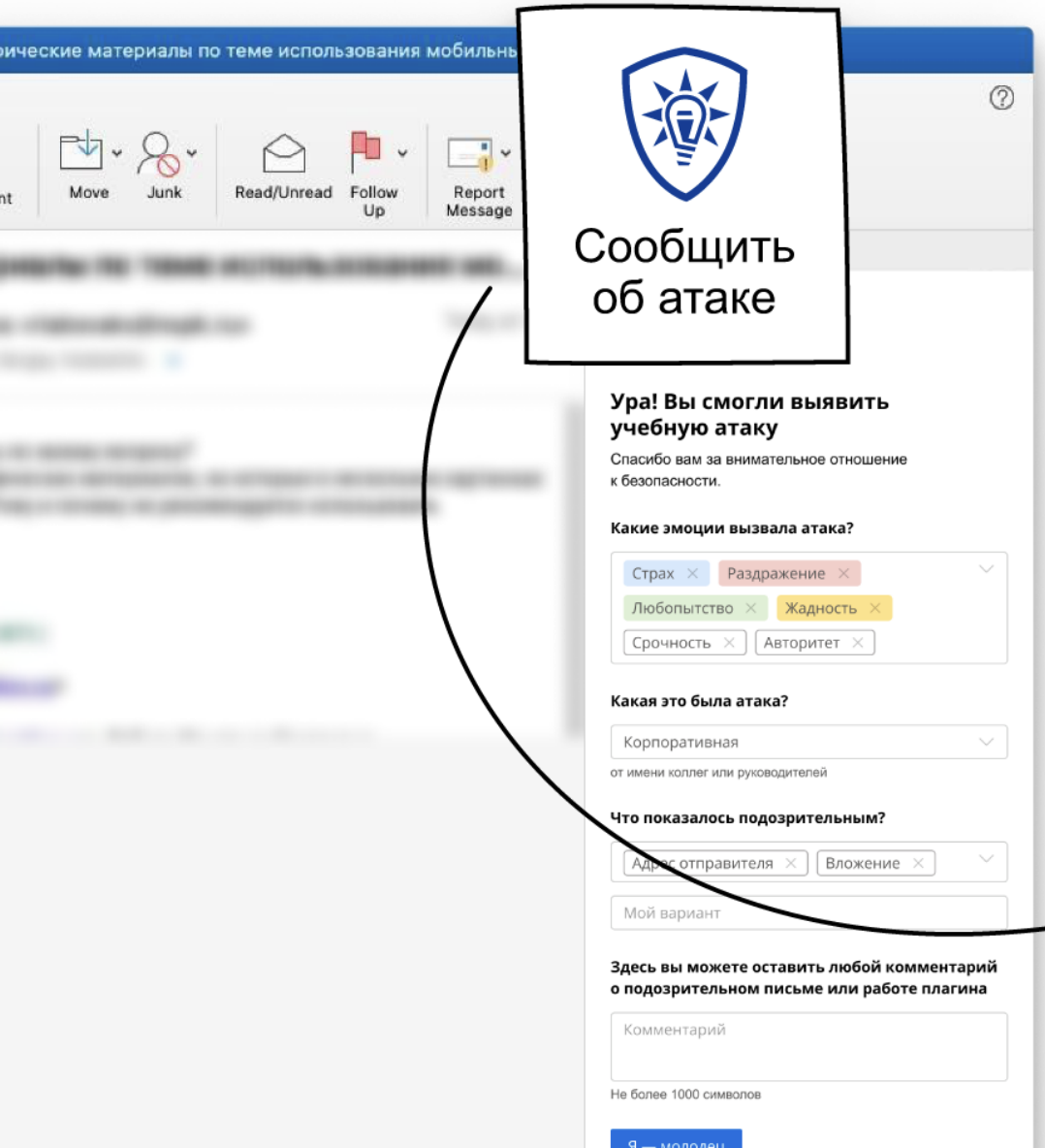
дение про...

овек

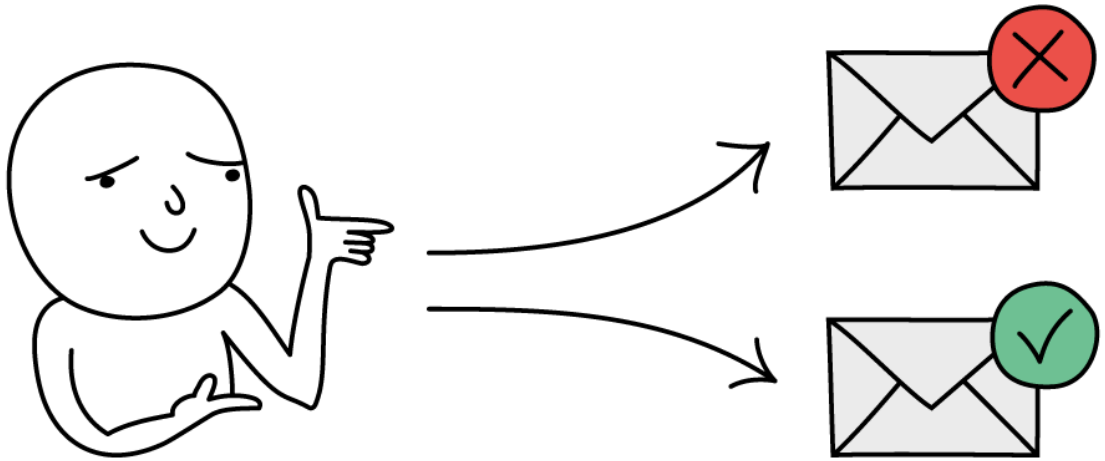
м экране

ежиме голосовой связи

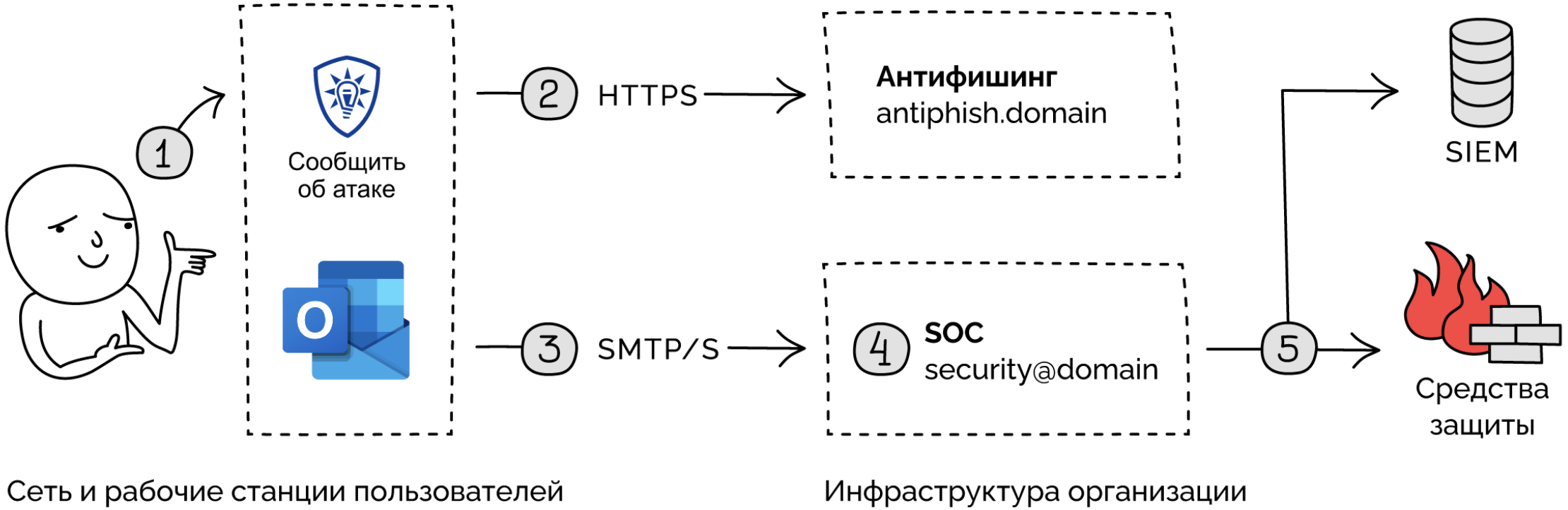
Очень простое действие через плагин Антифишинга



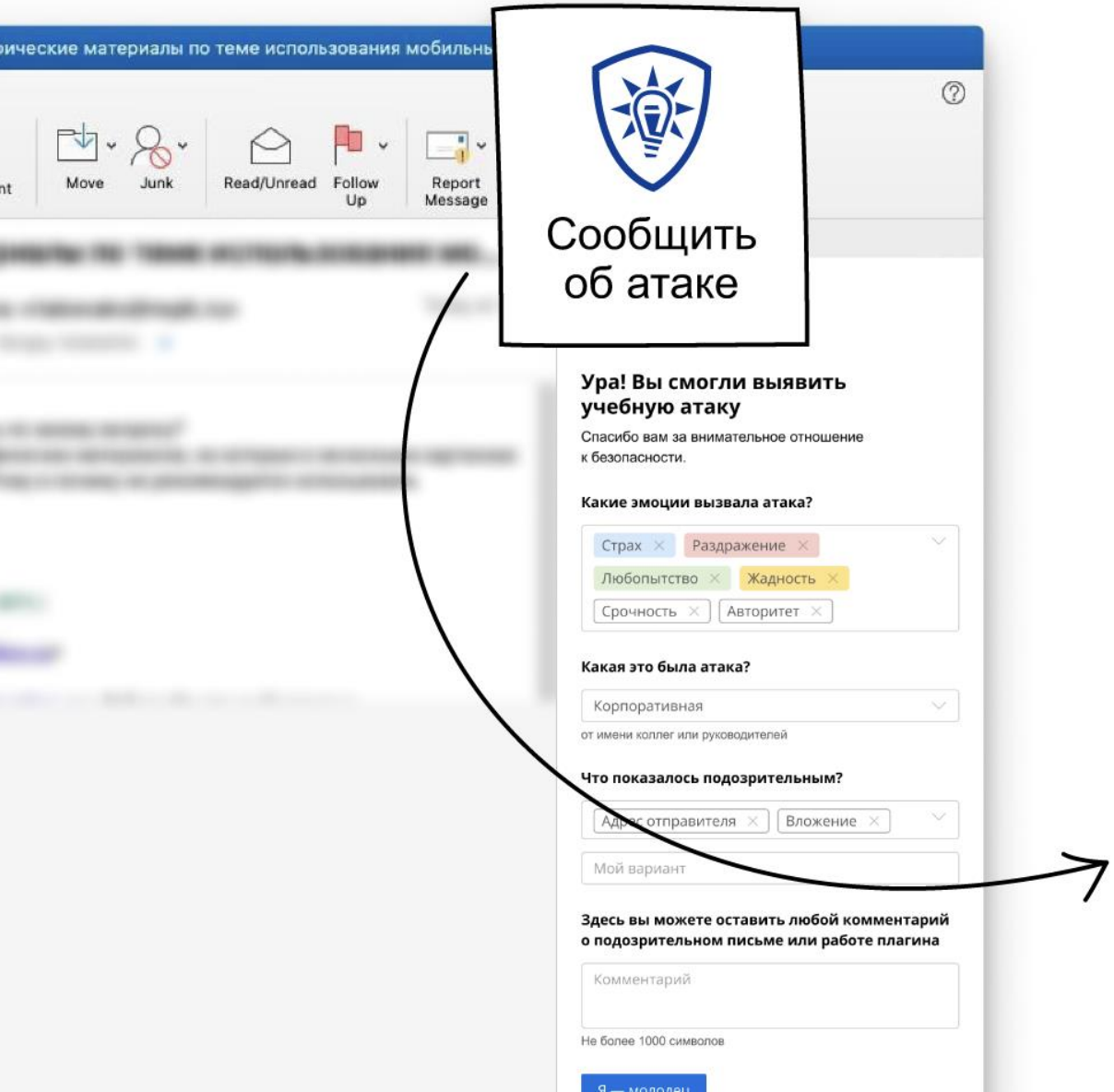
1. Устанавливается в почтовый клиент. Каждый сотрудник сможет сообщить о подозрительном письме или возможной атаке в один клик.
2. Сотрудник отправляет письмо по безопасному каналу кому нужно, с вложениями и важной для безопасности информацией.
3. Есть возможность фильтровать имитированные и реальные письма



Сотрудник реагирует на атаки и формирует социоинженерный TI-фид



Ваша лицензия на плагин Антифишинга



Начните получать обратную связь от сотрудников и формировать внутренний TI-фид уже сейчас

antiphish.ru/plugin-request

Коммуникация. Поддерживаем ре-трансляцию

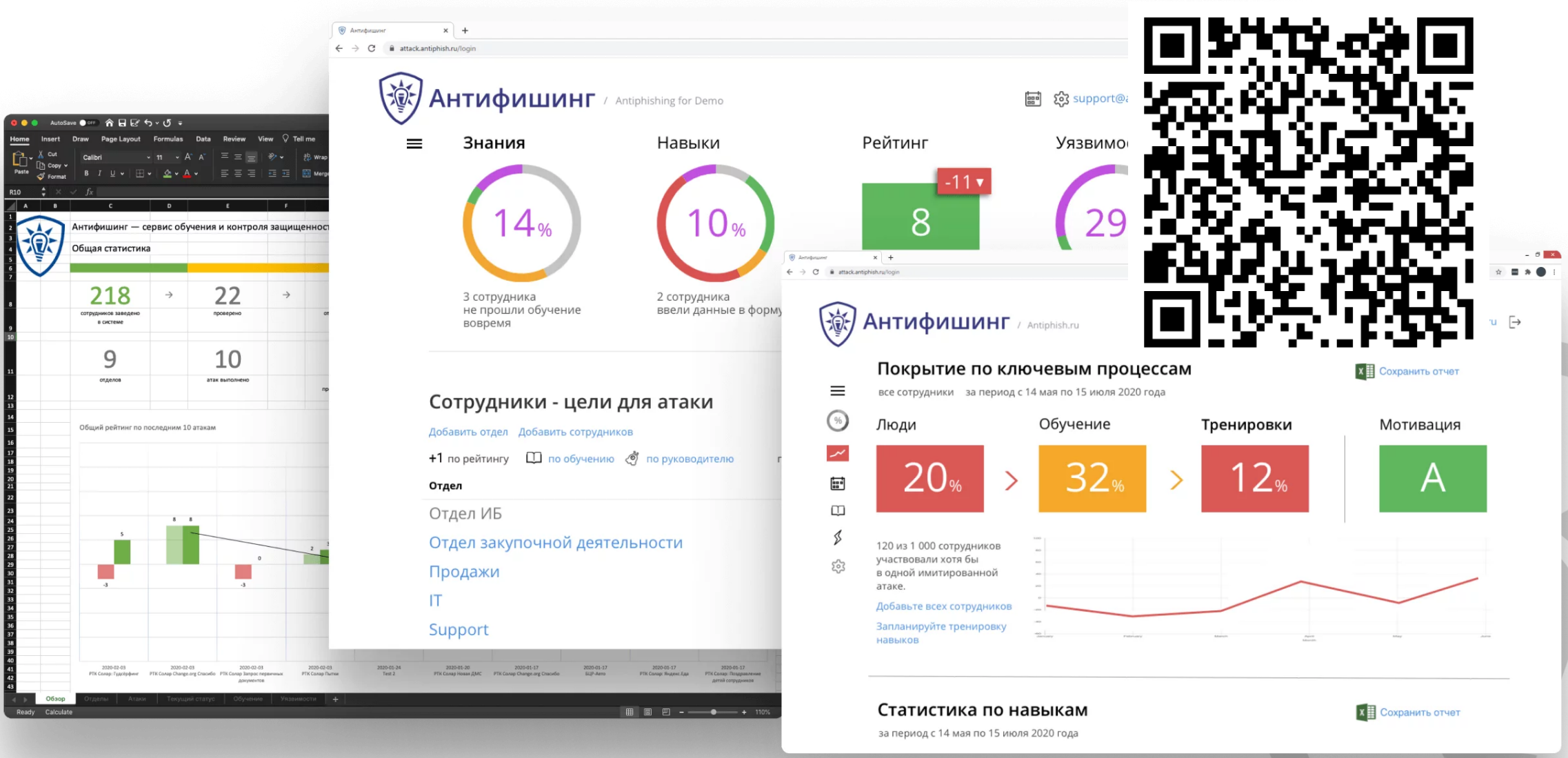
Люди учатся у коллег, если кто-то что-то хорошо сделал или наоборот налажал, надо помочь ему самому донести уроки для людей. Помочь написать статью, записать ролик. Искать добровольных помощников, поддерживать низовые активности, которые уже происходят.

— Мне пришло счет_на_оплату.js ну я и открыл а что такое это же мне надо счета оплачивать
у меня работа такая

— Ребята, тут контрагент прислал что-то странное, чекните плиз

Антифишинг для сотрудников

antiphish.ru/products



Сообщения сотрудников об атаках

Тренировка навыков может быть направлена не только на повышение индивидуальной устойчивости сотрудников к фишингу, но и на формирование таких привычек, полезных для обеспечения безопасности организации в целом, как сообщение об атаках. Это желаемое поведение с точки зрения специалистов по безопасности. Сообщения о подозрительных письмах от сотрудников помогают обогатить данными процессы реагирования на инциденты и помочь SOC-подразделениям и командам безопасности.

Мы сравнили количество сообщений об атаках от сотрудников после регулярно проведения имитированных атак средне уровня сложности. Если перед началом обучения и тренировки сообщений о подозрительных письмах не поступало, спустя в среднем 9 месяцев о фишингов письмах сообщали 66% сотрудников. Та образом, тренировки помогают мотивир сотрудников к действиям, повышающим защиту компании.

antiphish.ru/news/report2021

Вопросы про безопасность — продвинутый уровень

— Бизнес торопит с релизом, доступы у нас есть, может сделаем сейчас, а чейндж-тикет заведем завтра?

— Безопасники опять запускают свои сканы, а у нас от них иногда падает прод, может добавим ACL на пару часиков, чтобы ничего не упало?

— Апдейт кластера у клиента ведем уже третий час, вроде все сделали, но QA нашли багу. Разработчик говорит, что уже ее пофиксил, может по-быстрому зальем на прод и пойдем уже спать?

Вопросы про безопасность — продвинутый уровень

— Это точно не работает из-за межсетевого экрана, давайте сделаем досутуп any-any для проверки?

— Аутентифика
межсесрвисном
взаимодействи
очень медленно
нее?

асности
ail, но мы
не меняли,
)?

Shift Left Security: как подружить безопасность и продуктовые команды

Антифишинг

Место проведения: Зал 2 - 08.12.2022, 13:20 - 08.12.2022, 13:40 (UTC) (20 минут)

Волдохин Сергей

Директор в Антифишинг

Зал 2, 16.00

antiphish.ru/
plugin-request

antiphish.ru/antph-
motivation-letter-
request