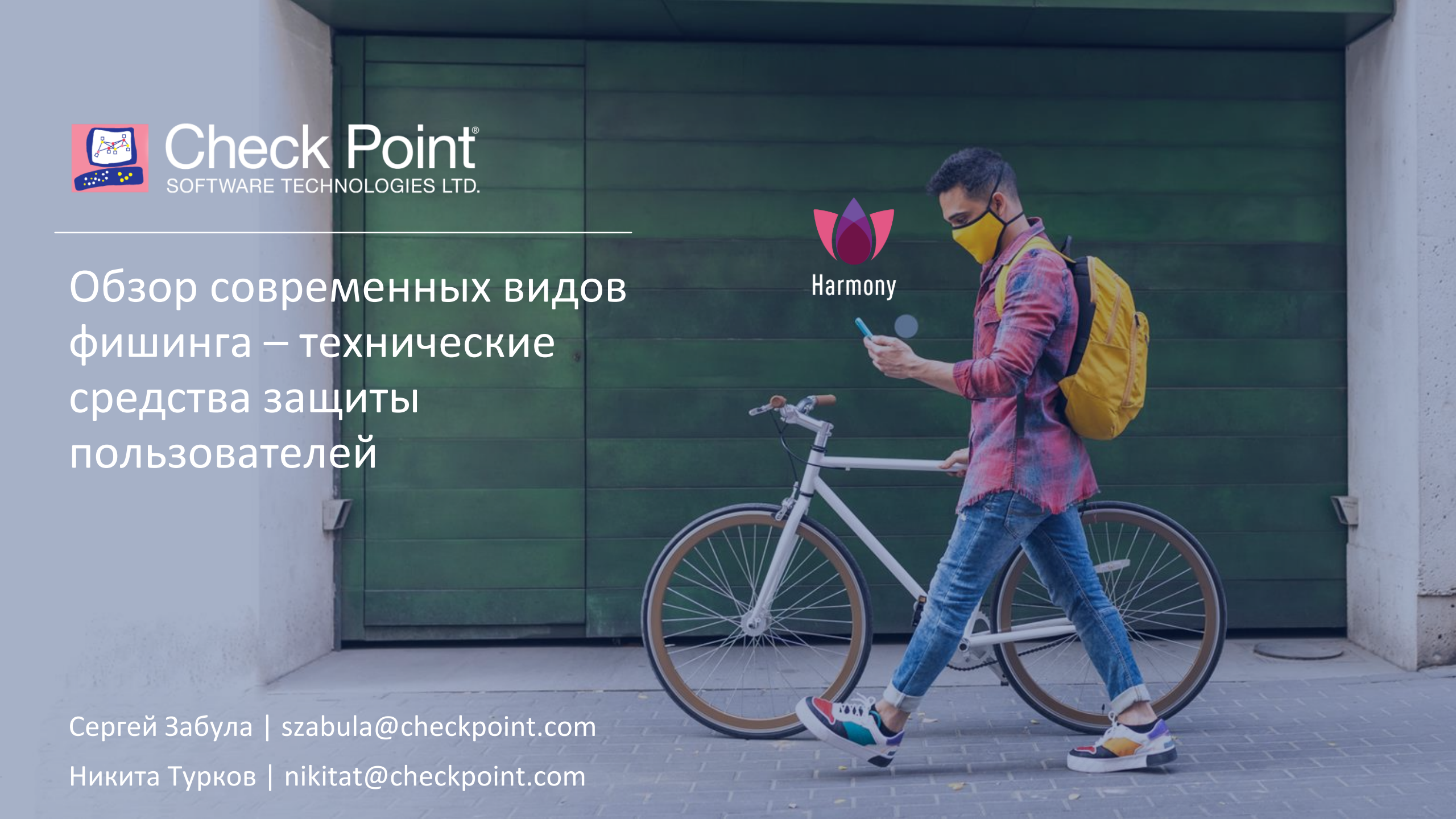
Check Point®
SOFTWARE TECHNOLOGIES LTD.

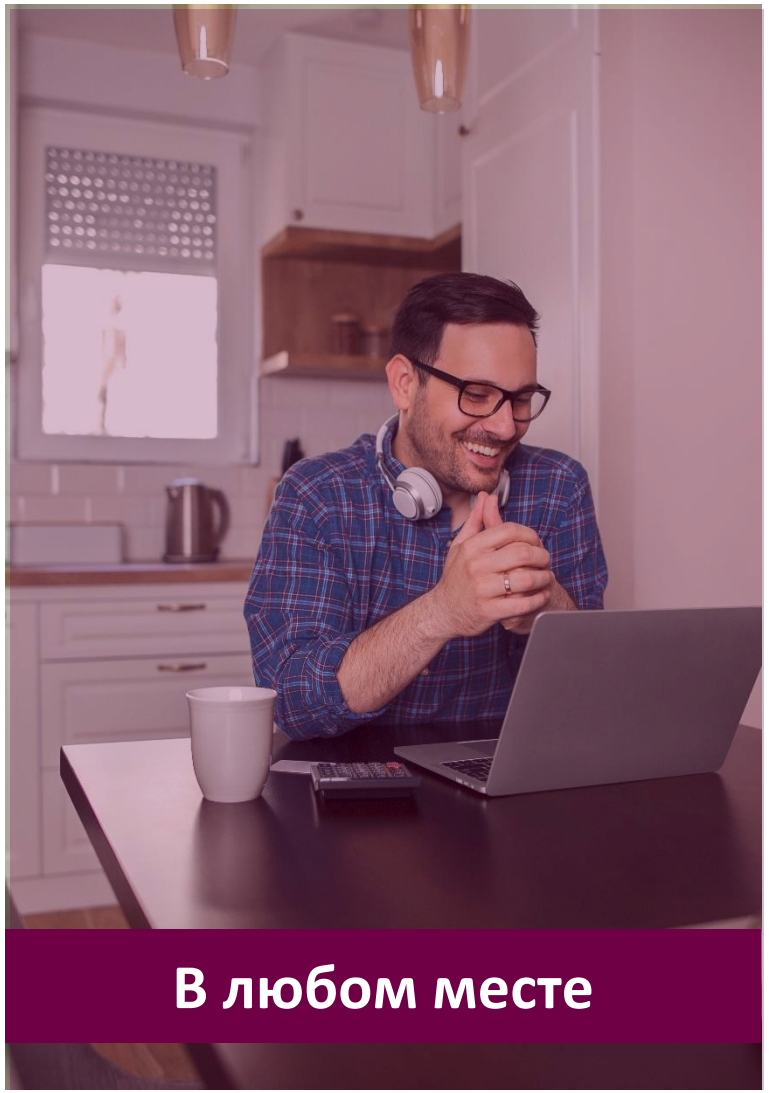
Обзор современных видов фишинга – технические средства защиты пользователей



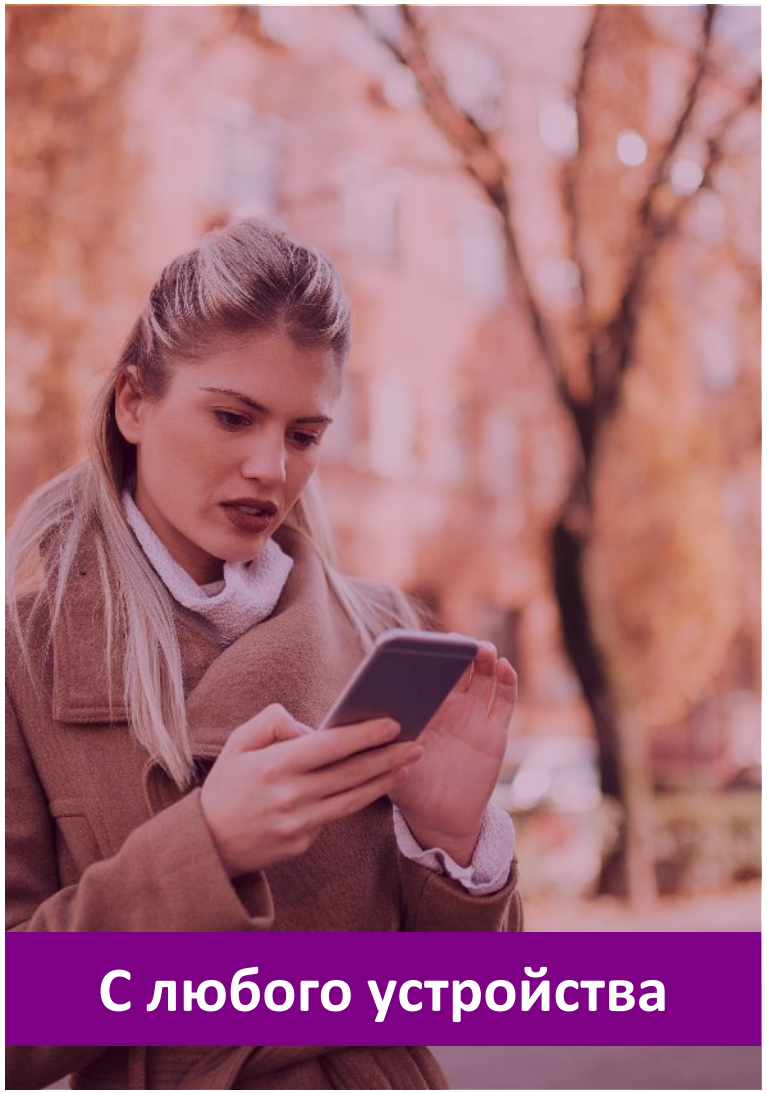
Сергей Забула | szabula@checkpoint.com

Никита Турков | nikitat@checkpoint.com

РАБОТАЕМ ОТКУДА УГОДНО И КАК УГОДНО



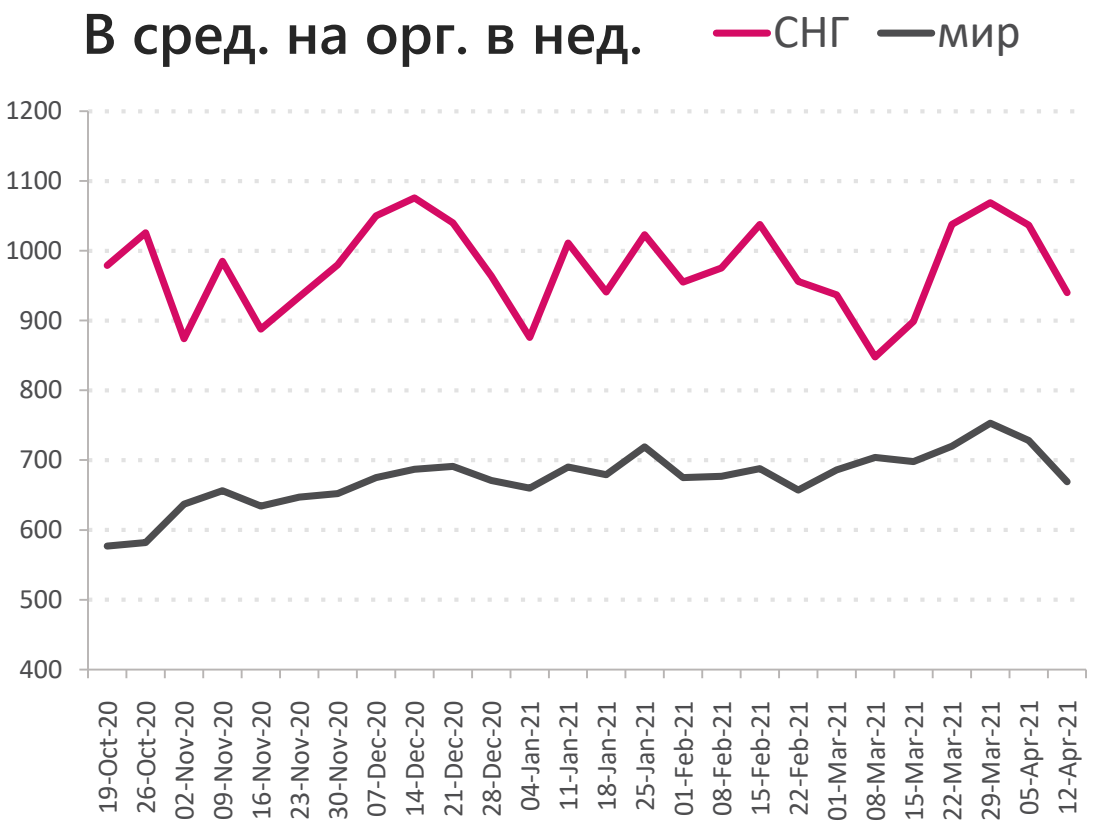
В любом месте



С любого устройства

Доступ к приложениям

КИБЕРАТАКИ НА ОРГАНИЗАЦИИ В РОССИИ И СНГ

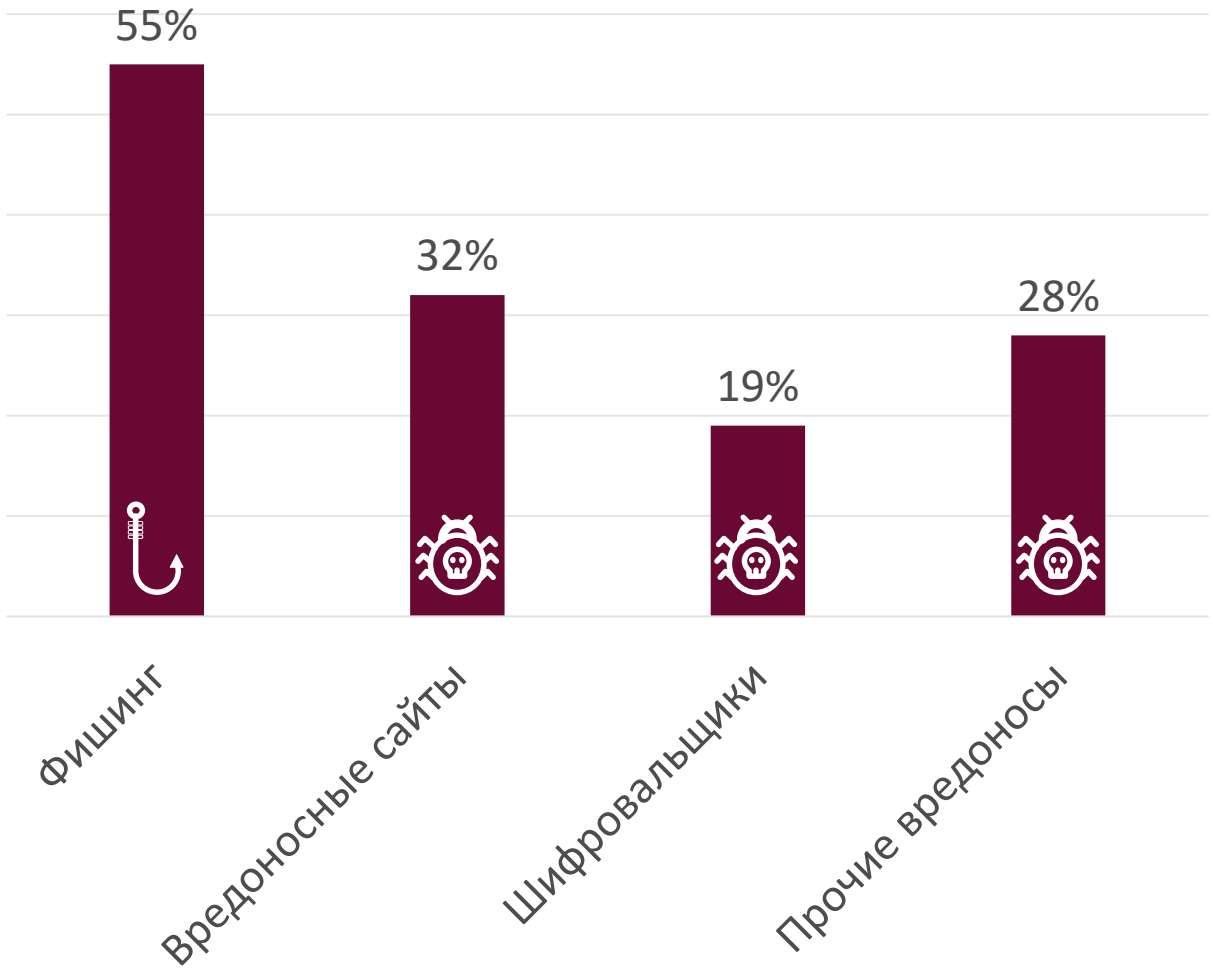


Топ вредоносов:

Fareit (9%), Trickbot (7%), XMRig (7%), Phorpiex (5%), Pykspa (4%)

https://research.checkpoint.com/2021/helping-you-immunize-your-organization-against-the-cyber-pandemic-check-point-researchs-2021-security-report/

УГРОЗЫ, КОТОРЫЕ ВИДЯТ СПЕЦИАЛИСТЫ ИТ И ИБ



71% из 411 опрошенных специалистов **столкнулись с увеличением количества кибер-атак** в связи эпидемией коронавируса и массовым переходом на удаленку

Источник: Check Point & Dimensional Research
Опрос среди организаций с 500+ сотрудников

https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/

$20 млрд.

ущерб от атак вымогательского ПО в мире в 2020

По сравнению с $11.5 млрд. в 2019

Более 50%

вымогателей угрожали опубликовать украденные данные, начиная с 3-го кв. 2020

$233 тыс.

средний размер выплаченного выкупа

На 30% выше, чем во 2-м кв. 2020

ЗЛОУМЫШЛЕННИКИ ПОЛЬЗУЮТСЯ СИТУАЦИЕЙ

ВСПЛЕСК АТАК ВЫМОГАТЕЛЕЙ И ФИШИНГА В МИРЕ

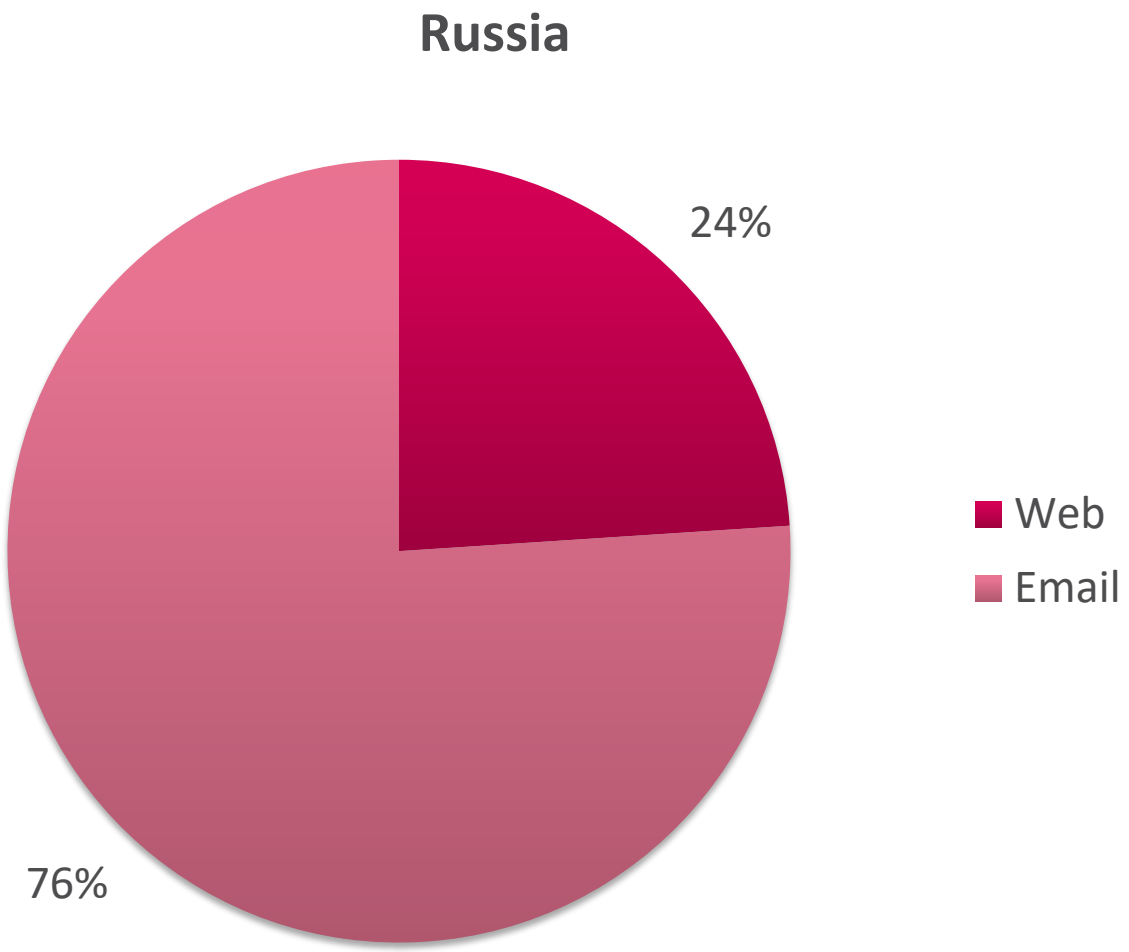
ЧТО ТАКОЕ ФИШИНГ?

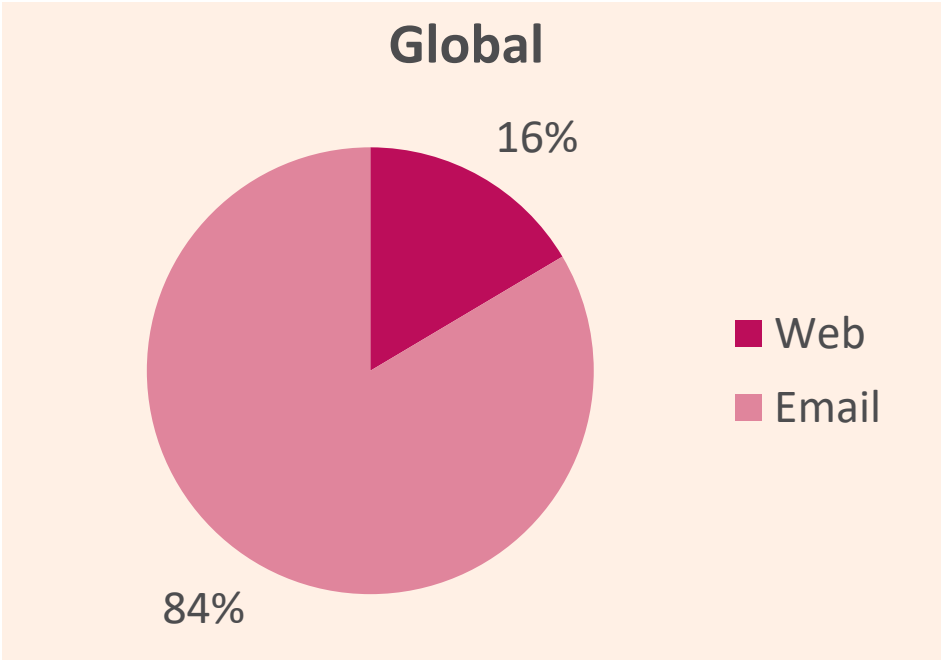
Фи́шинг (англ. phishing от fishing «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей.

Злоумышленник знает психологию и использует:

- **Эмоции**
- **Страх**
- **Желание помочь**
- **Рефлексы**

ВЕКТОРЫ АТАК В РФ ЗА ПОСЛЕДНИЕ 30 ДНЕЙ - ЭЛЕКТРОННАЯ ПОЧТА!





ВИДЫ ФИШИНГА

Фишинг

С его помощью кибермошенники пытаются выманить у человека конфиденциальные данные или вынудить его на какие-либо нежелательные действия. С этой целью злоумышленники используют мгновенные и почтовые сообщения и специально созданные поддельные веб-сайты.

Смишинг

от англ. SMiShing — от «SMS» и «фишинг» — вид фишинга с использованием SMS. Например, мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее получателя пройти на этот сайт.

Скам

Мошенничество, которое нацелено на быстрое получение денег обманным путём.

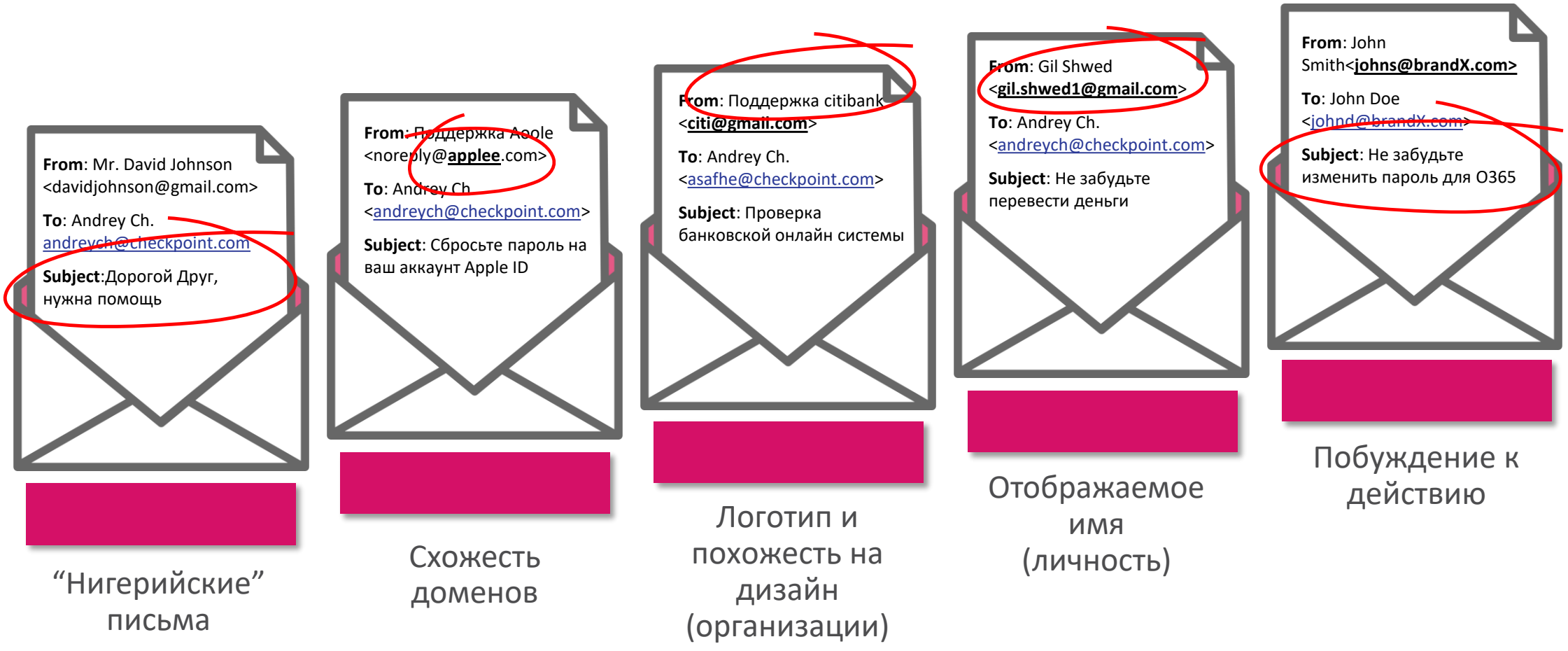
Вишинг

от англ. Vishing— «voice» и «фишинг». Мошенничество с помощью звонков. Мошенники, используя социальный инжиниринг, стараются получить от жертвы необходимые им данные.

Кража личности

Незаконное использование чужих персональных данных для получения выгоды.

ФИШИНГОВЫЕ АТАКИ ВСЕГДА ВКЛЮЧАЮТ В СЕБЯ КОМПРОМЕТАЦИЮ ЛИЧНОСТИ/ОРГАНИЗАЦИИ



ЛЕГКО «МИМИКРИРОВАТЬ» ПОД ИЗВЕСТНЫЙ БРЕНД

Ответить Ответить всем Переслать

Вт 06.12.2016 18:04

info@sberbank.ru

ОАО "Сбербанк России"

Кому [redacted]

Вы ответили: , 22 февраля 2017 г. 11:46.

СБЕРБАНК

Всегда рядом

Уважаемый [redacted]

Отдел по работе с клиентами Сберба
требованиями Федерального закона «О
полученных преступным путем и фина
Положения Банка России «Об идент
выгодоприобретателей в целях прот
полученных преступным путем, и фина
должны предоставить информацию сог
доступной в Личном Кабинете по ссылк

Форма «Информационные сведения Кли

В случае не предоставления информации
до предоставления информации.

С уважением,
Сбербанк России

Вт 06.12.2016 18:05

info@vtb24.ru

Уведомление о задолженности

Кому [redacted]

ВТБ24

Большое преимущество

Здравствуйте, Павел [redacted]!

Кредитный отдел ВТБ 24 (ПАО), Уведомляет Вас о том, что на Ваше имя 20.09.2015 был оформлен потребительский кредит через наш онлайн банкинг на сумму

680 000 рублей.

На данный момент задолженность не погашена. На 01.12.2016 Ваш долг составляет

663 773 рублей с учетом пени (0.7% в сутки).

В связи с этим на Ваше имя ВТБ 24 (ПАО) был составлен судебный иск.

Ознакомится с документами Вы можете по ссылке в личном кабинете

В случае Вашей неявки на заседание суда мы будем вынуждены поставить Вашего работодателя в известность о вышеуказанных фактах.

С уважением,
ВТБ 24 (ПАО)

ельство РФ
н России

жданскому делу №21365.
ыми, на вас должен быть
на судебное заседание по
приводу (ч.2 ст. 168 ГПК
электронный адрес был
лектронном виде услуг и
ски, вы можете оставить
Подробности в архиве

ктор Курицын В. А.

должности можно по ссылке

сть за 2015 год и ранее

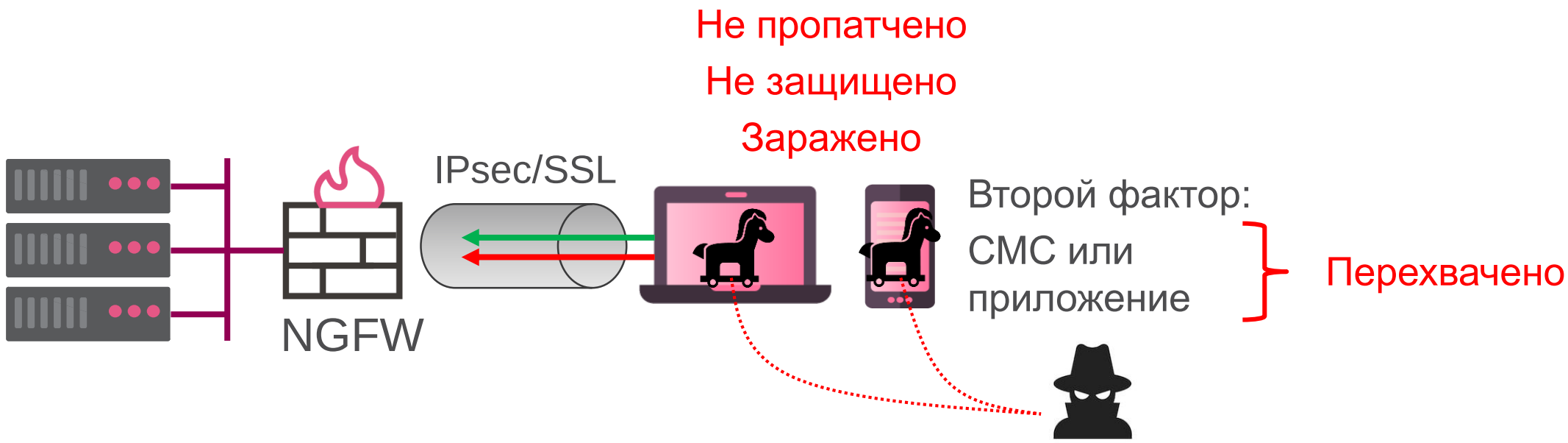
та сумм налога», неуплата
налога, либо к уголовной
лет. Пожалуйста погасите

АТАКИ МОГУТ БЫТЬ МАКСИМАЛЬНО ТАРГЕТИРОВАННЫМИ

Пример атаки Man-in-the-middle: Стартап и венчурный фонд

https://research.checkpoint.com/2019/incident-response-casefile-a-successful-bec-leveraging-lookalike-domains/

ДОСТАТОЧНО ЛИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ КАК СРЕДСТВА ЗАЩИТЫ?



This Android backdoor contains the following features:

Rampant Kitten

September 18, 2020

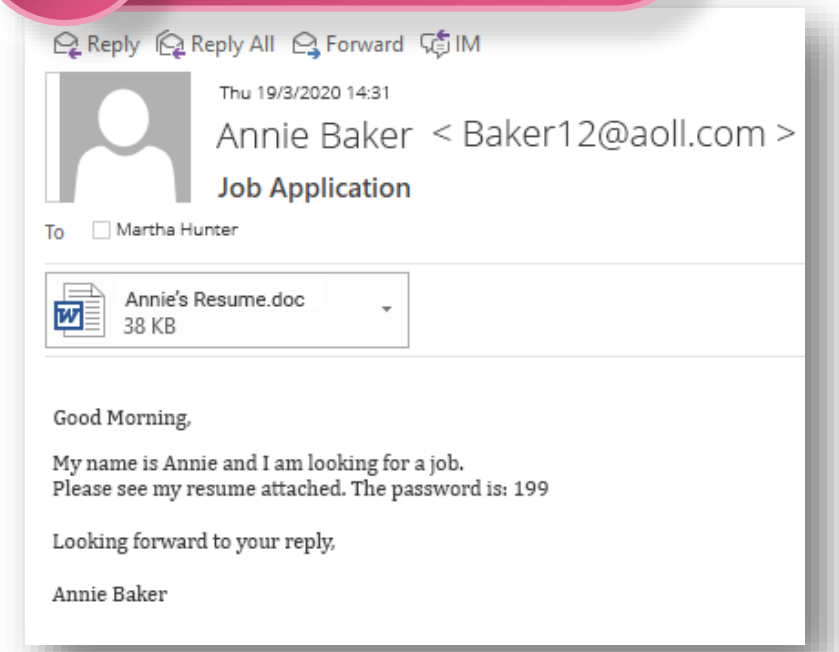
- Steal existing SMS messages
- Forward two-factor authentication SMS messages to a phone number provided by the attacker-controlled C&C server
- Retrieve personal information like contacts and accounts details
- Initiate a voice recording of the phone's surroundings
- Perform Google account phishing
- Retrieve device information such as installed applications and running processes

cp<r>
CHECK POINT RESEARCH

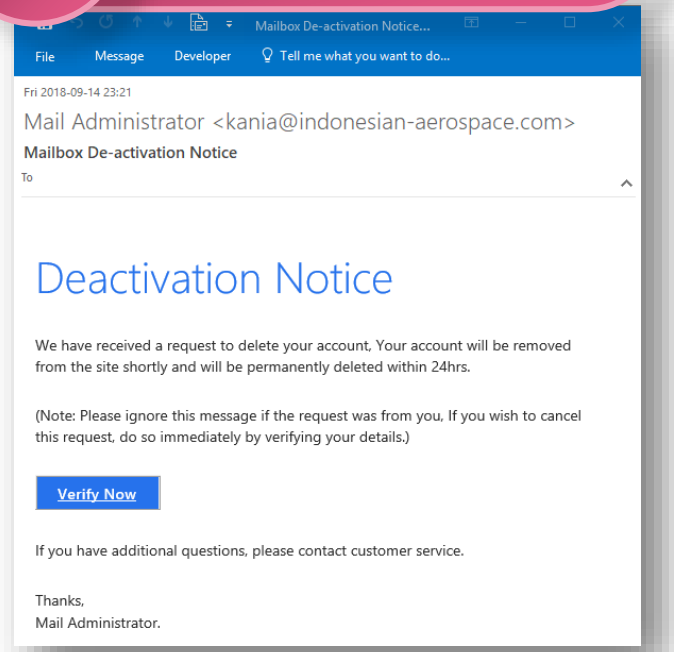
НЕСМОТРЯ НА ОБУЧЕНИЕ, ПОЛЬЗОВАТЕЛИ ПОПАДАЮТ НА УДОЧКУ ЗЛОУМЫШЛЕННИКОВ

Атаки слишком сложные, чтобы отличить подложный контент «на глаз»

Вредоносы
«Резюме»



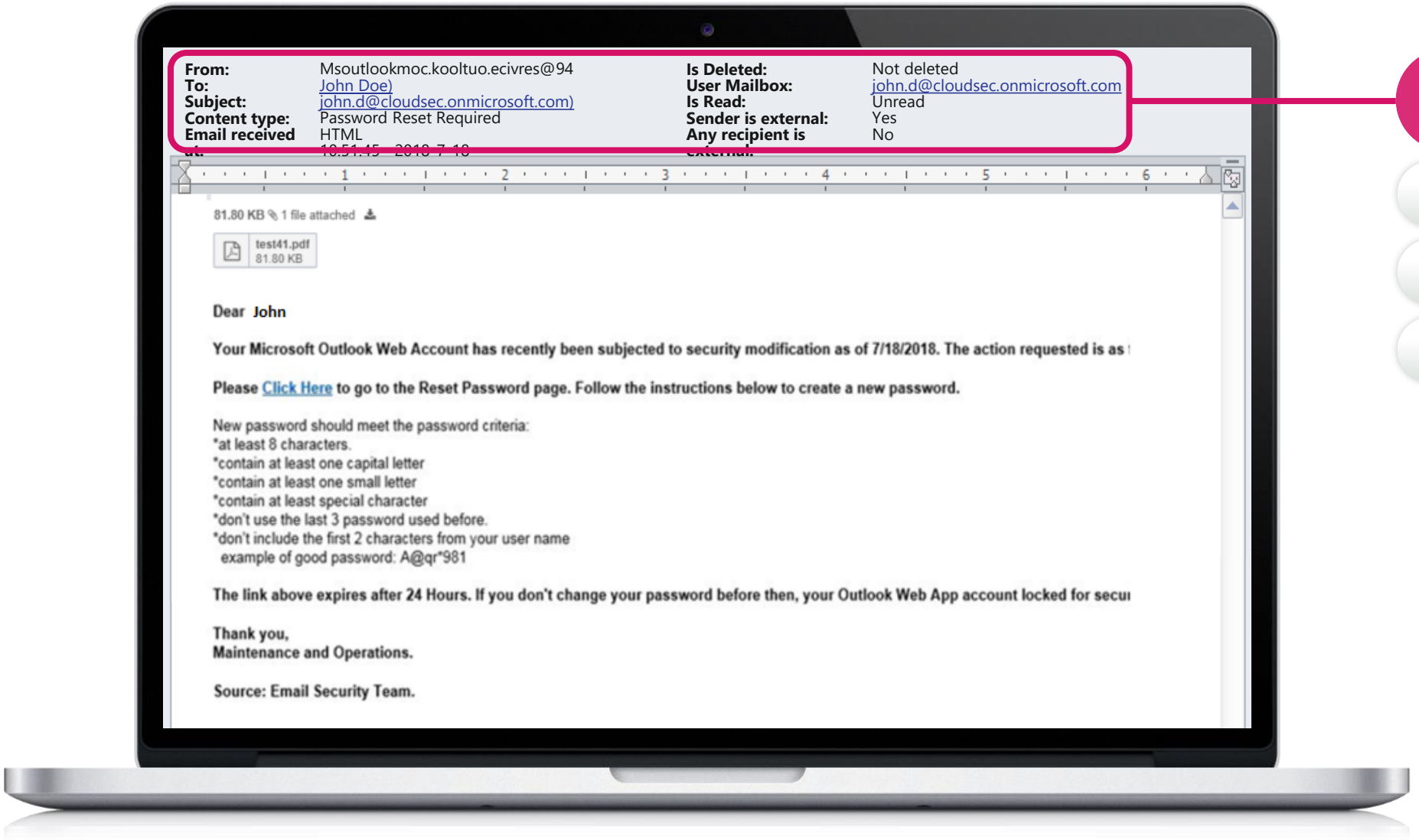
Фишинг
«Срочно!»



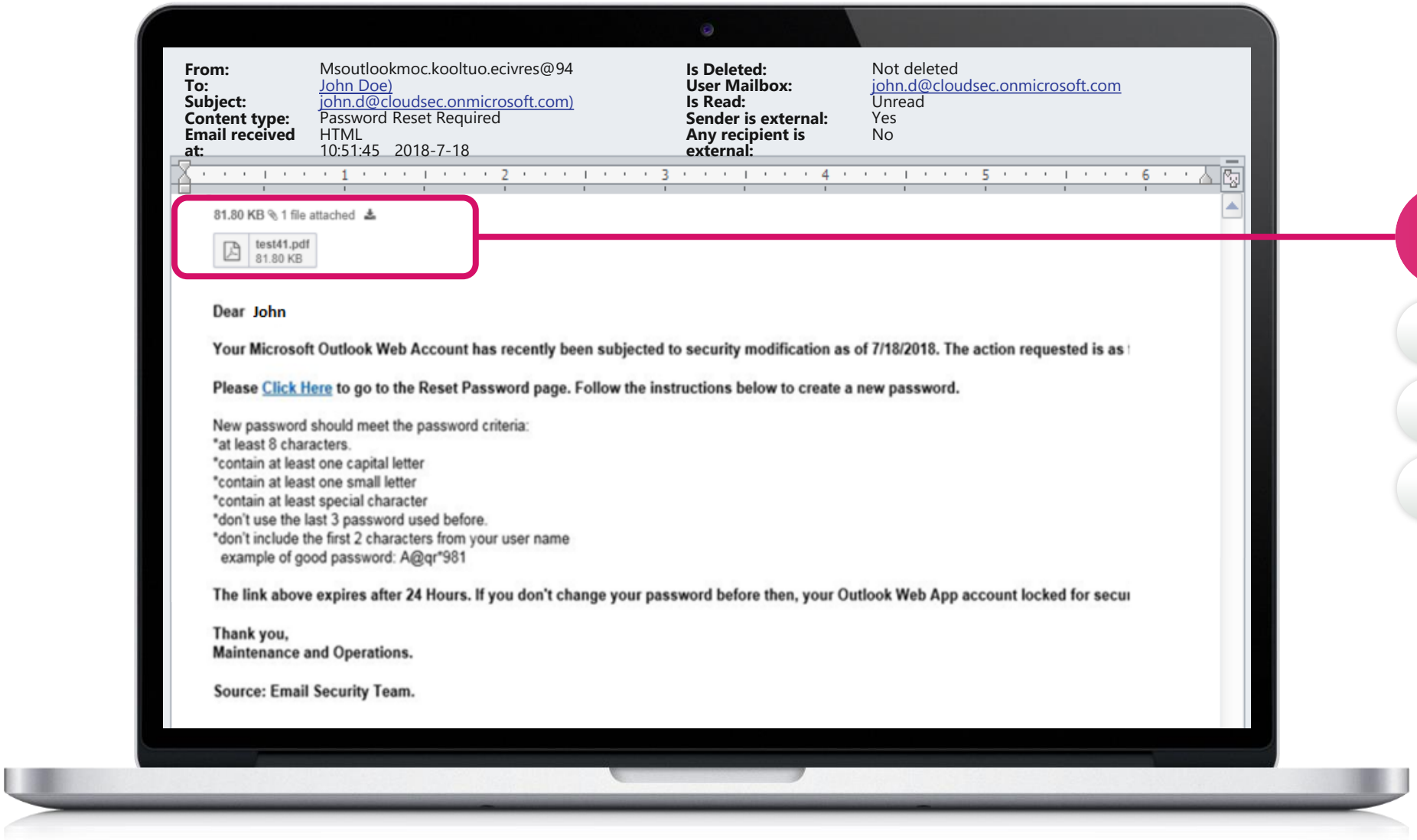
01

МЕТАДАННЫЕ
Проверить отправителя

- DNS
- База данных
- Имперсонализация



Своя ML-модель для каждого клиента: 300+ индикторов с разным весом

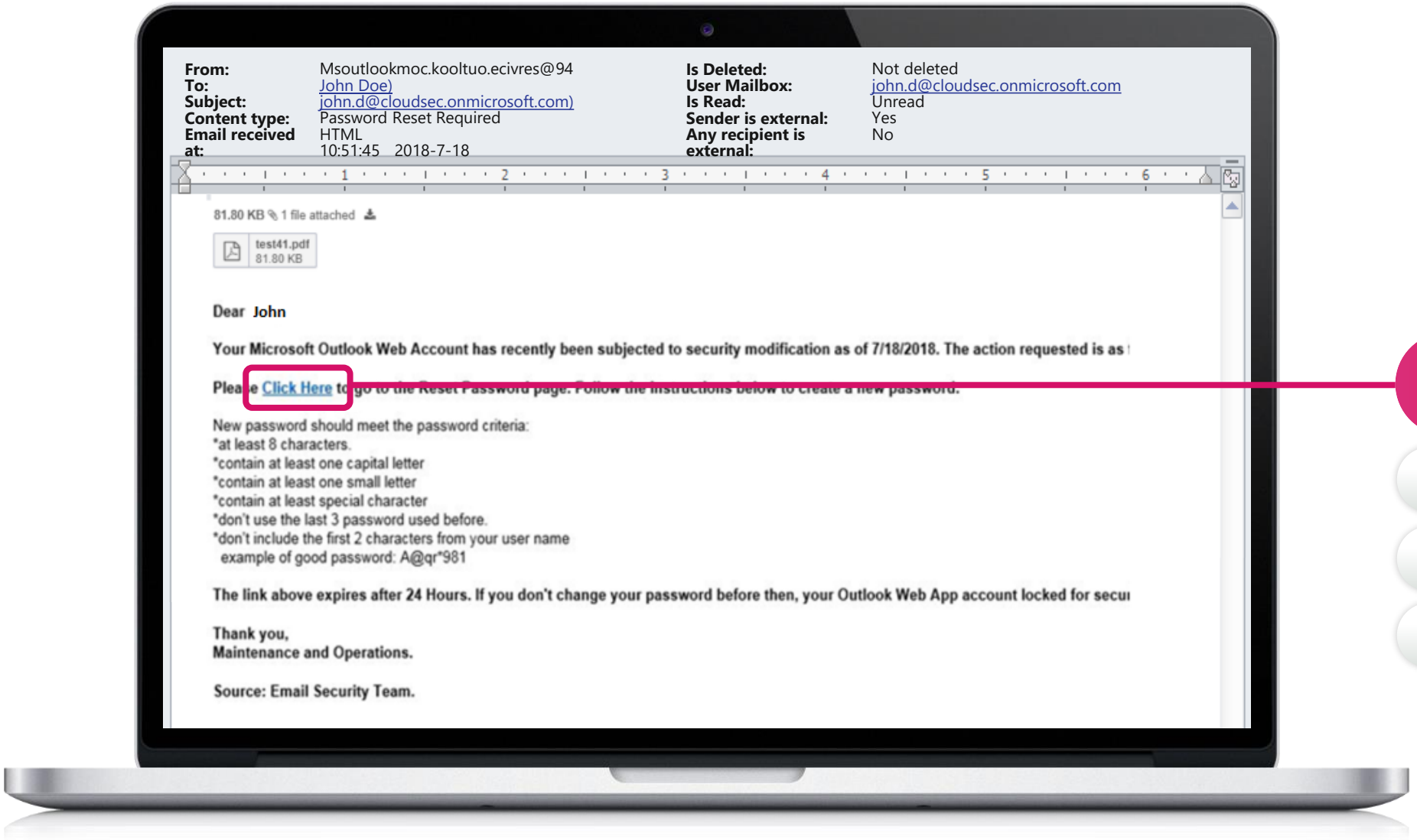


02

ВЛОЖЕНИЯ
Проверить файлы

- ANTI-VIRUS
- THREAT EMULATION
- THREAT EXTRACTION

Своя ML-модель для каждого клиента: 300+ индикторов с разным весом

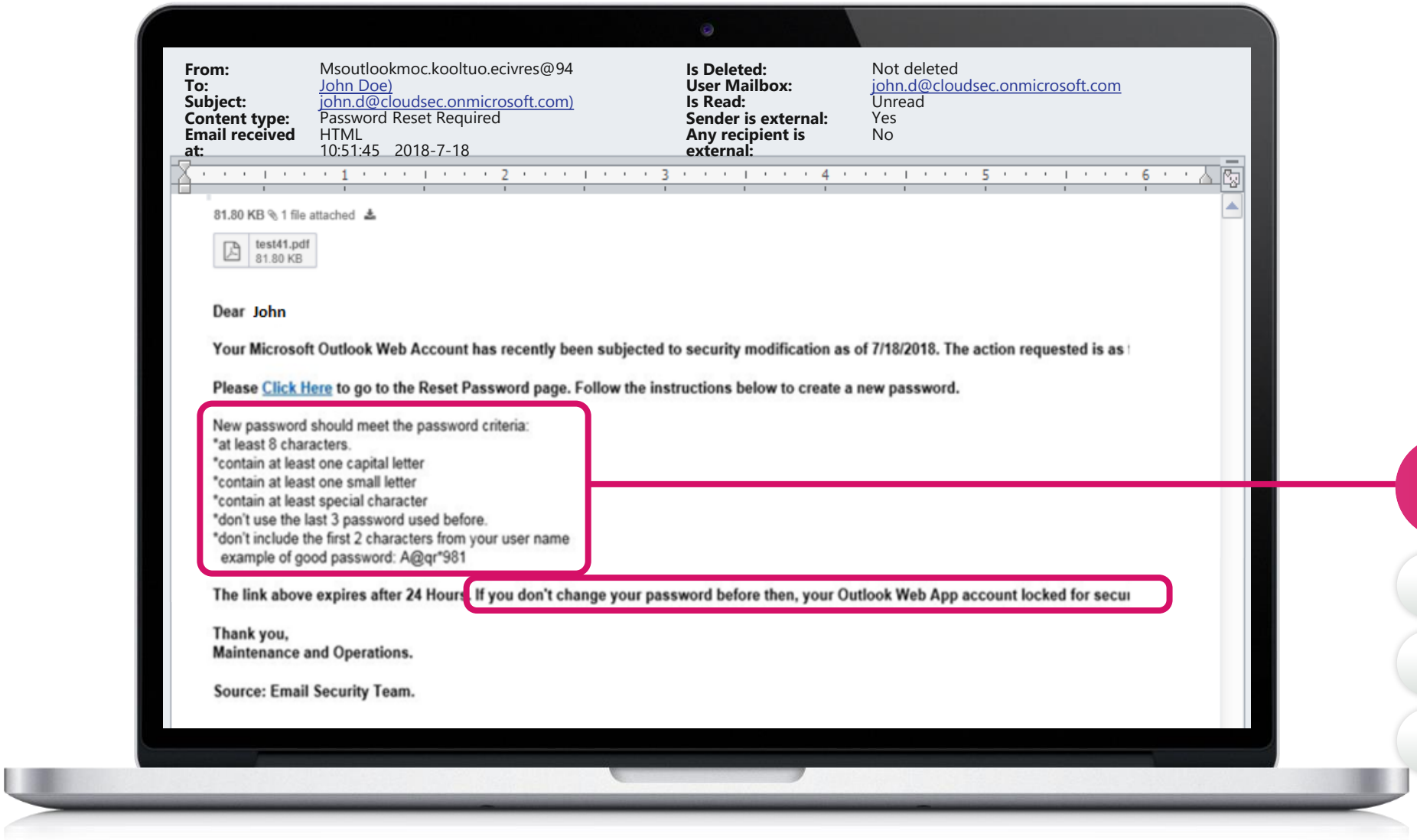


03

ССЫЛКИ

- Репутация и схожесть
- Сведения о домене
- Проверить в момент клика

Своя ML-модель для каждого клиента: 300+ индикторов с разным весом



04

ЯЗЫК

Проверить заголовок и тело

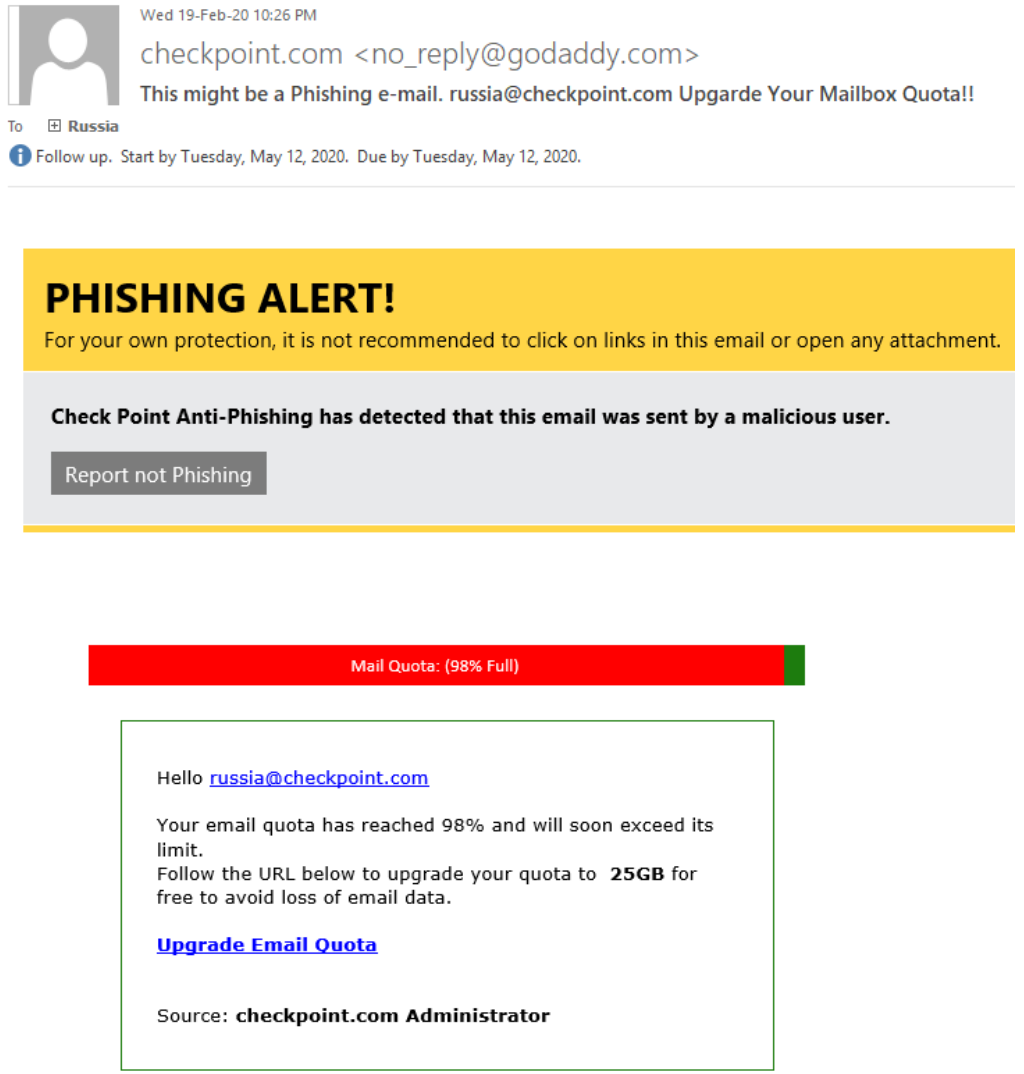
Сигнатуры фраз

Текст на картинках, QR-коды

Побуждение к действию

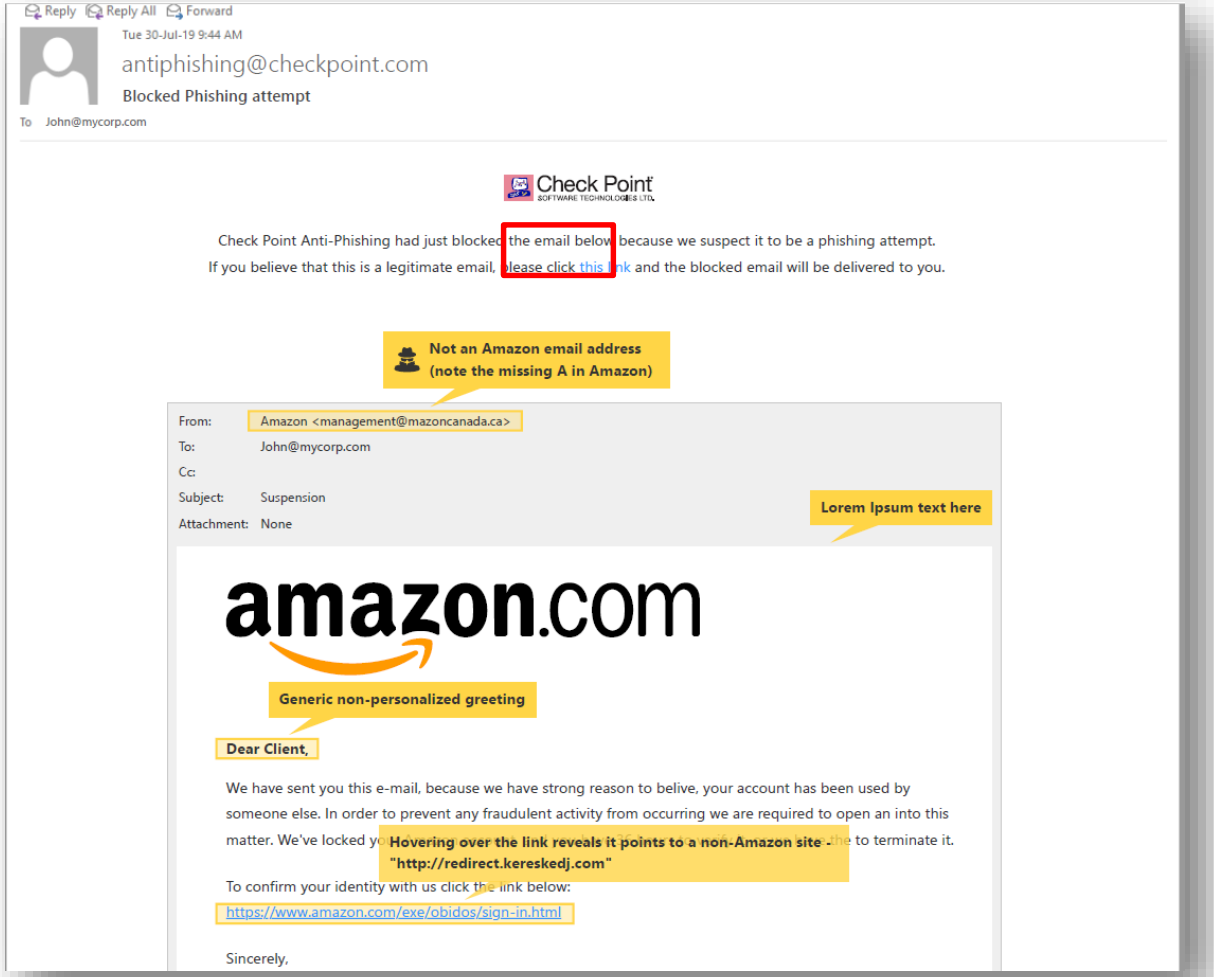
Своя ML-модель для каждого клиента: 300+ индикторов с разным весом

ПРИМЕР РАБОТЫ АНТИФИШИНГА НА ШЛЮЗЕ – ИНФОРМИРУЕМ ПОЛЬЗОВАТЕЛЯ

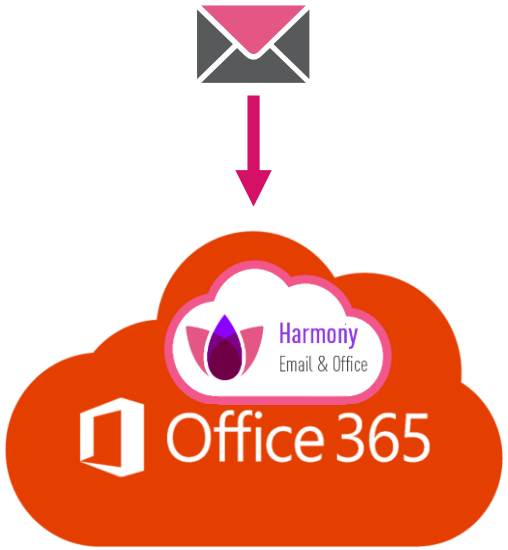


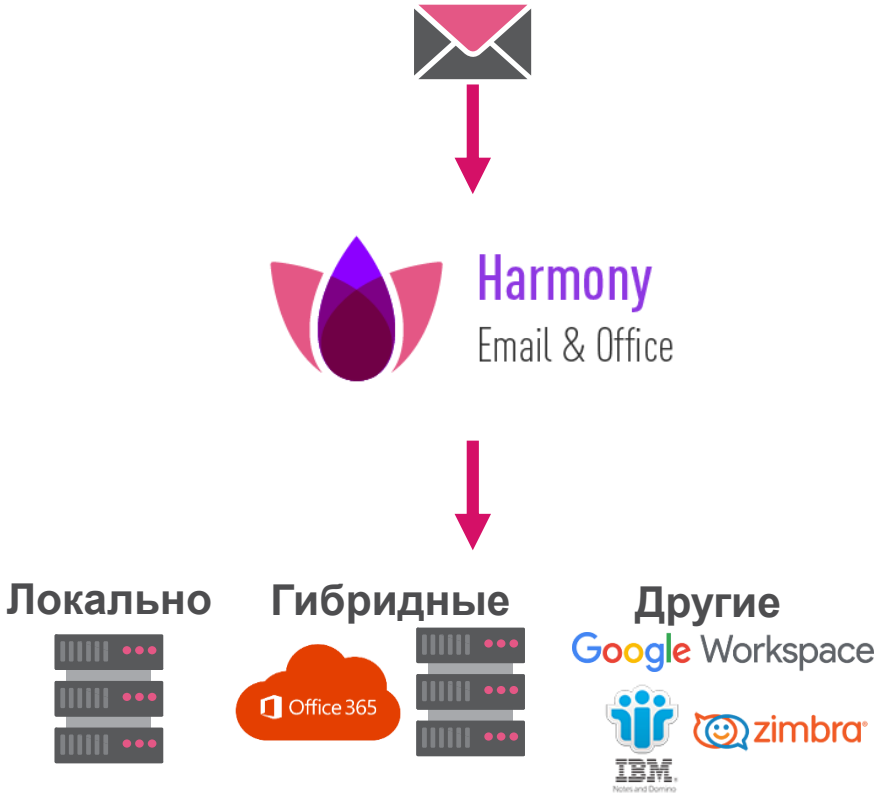
ДАЛЬНЕЙШЕЕ РАЗВИТИЕ АНТИФИШИНГА

Предотвращение угроз и обучение пользователей
Пользователи видят алерты, которые объясняют почему данное письмо было заблокировано
Возможна конфигурация, когда пользователи могут получить доступ к оригинальному письму и добавить отправителя и/или домен в доверенные



А что же для почты в облаке? Защита облачной/локальной эл. почты как сервис

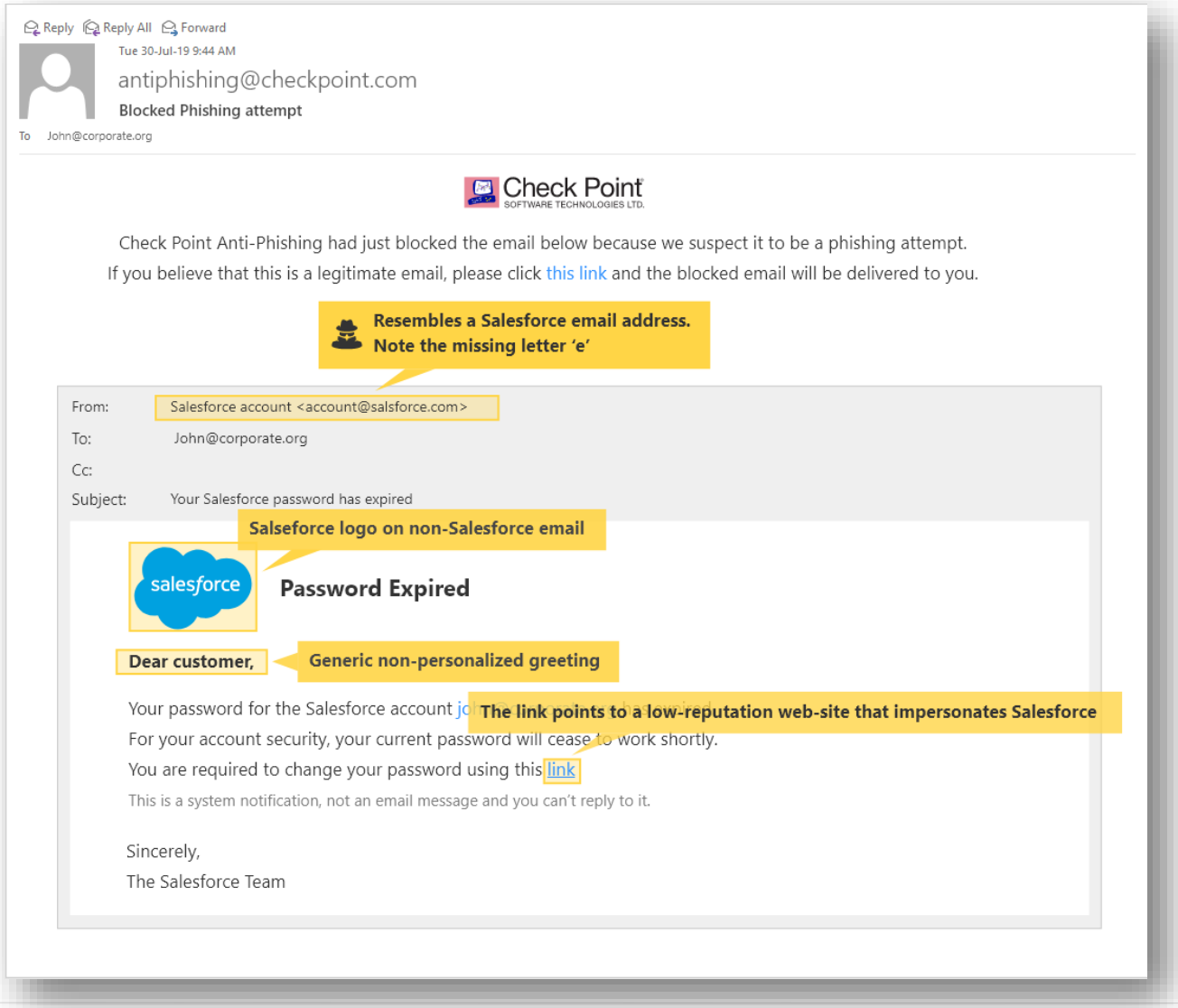




Harmony
Email & Office

Блокируем продвинутый фишинг нулевого дня

С помощью машинного обучения



300+
индикаторов
в модели
ML/AI

Обучаем пользователей,
на что обращать внимание

Проактивная очистка и быстрая доставка документов пользователям

Конвертация в безопасную копию и доставка **за 1 сек.**

Harmony Email & Office

Office 365 · SharePoint · OneDrive · G Suite

Threat Extraction (CDR)

Threat Emulation (песочница)

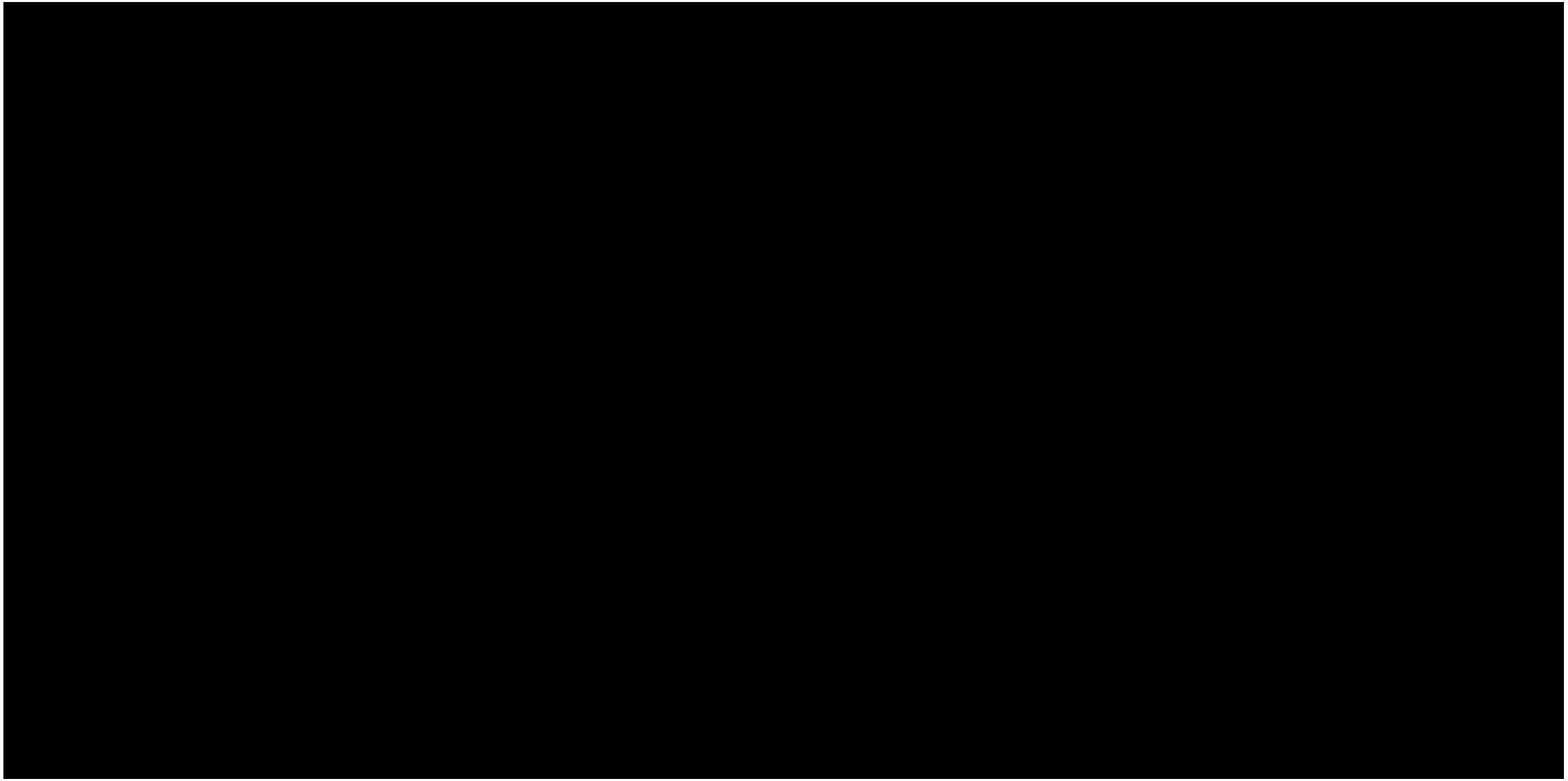
Sandbox

Оригинальный файл проверяется в песочнице

Доставка **проверенных безопасных оригиналов вложений по запросу пользователя.**
Запрашивается реже 1%

Harmony
Email & Office

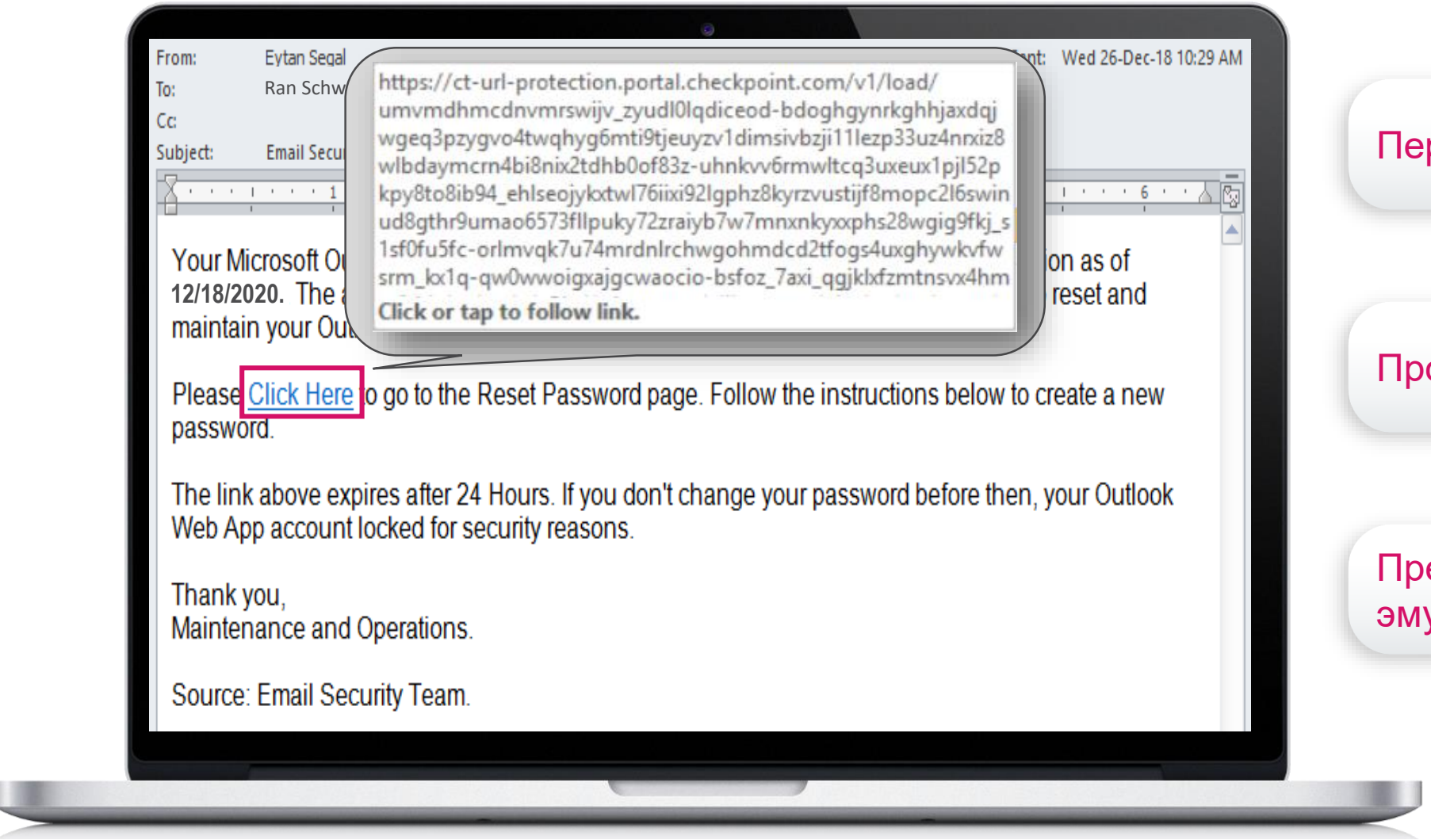
Инспекция вложений, защищенных паролем



Harmony
Email & Office

Click-Time URL Protection (CTUP)

Проверка ссылок в момент клика пользователя



- Переписываем ссылки
- Проверяем при каждом клике
- Предотвращаем вредоносы с эмуляцией в песочнице

Общие рекомендации (нулевое доверие!)

- **Будьте осторожны с подозрительными письмами, побуждающими Вас к немедленным действиям**.
- **Не переходите по ссылкам, не кликайте на подозрительные объекты.**
- **Будьте осторожны с вложениями**, открывайте только те, которые ждали. Во вложениях также будьте осторожны с ссылками.
- **Сверяйте адрес отправителя с доменом организации**.
- **Обращайте внимание на обращение и подпись к письму**.
- **Будьте осторожны** с подозрительными письмами от друзей и коллег.
- **Не звоните** по указанному в подозрительном письме или на сайте номеру телефона.
- **Не отвечайте** на подозрительные письма.

Check Point
SOFTWARE TECHNOLOGIES LTD.

Сергей Забула | szabula@checkpoint.com

Никита Турков | nikitat@checkpoint.com