



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Обзор современных видов фишинга – технические средства защиты пользователей



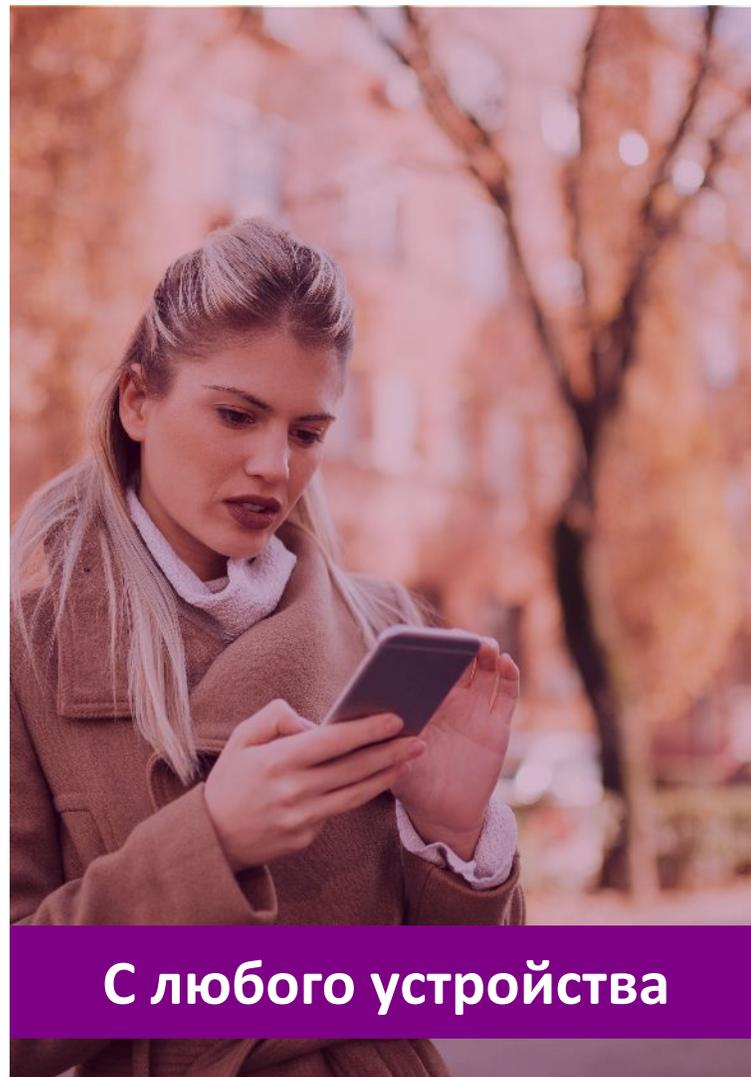
Harmony



Сергей Забула | szabula@checkpoint.com

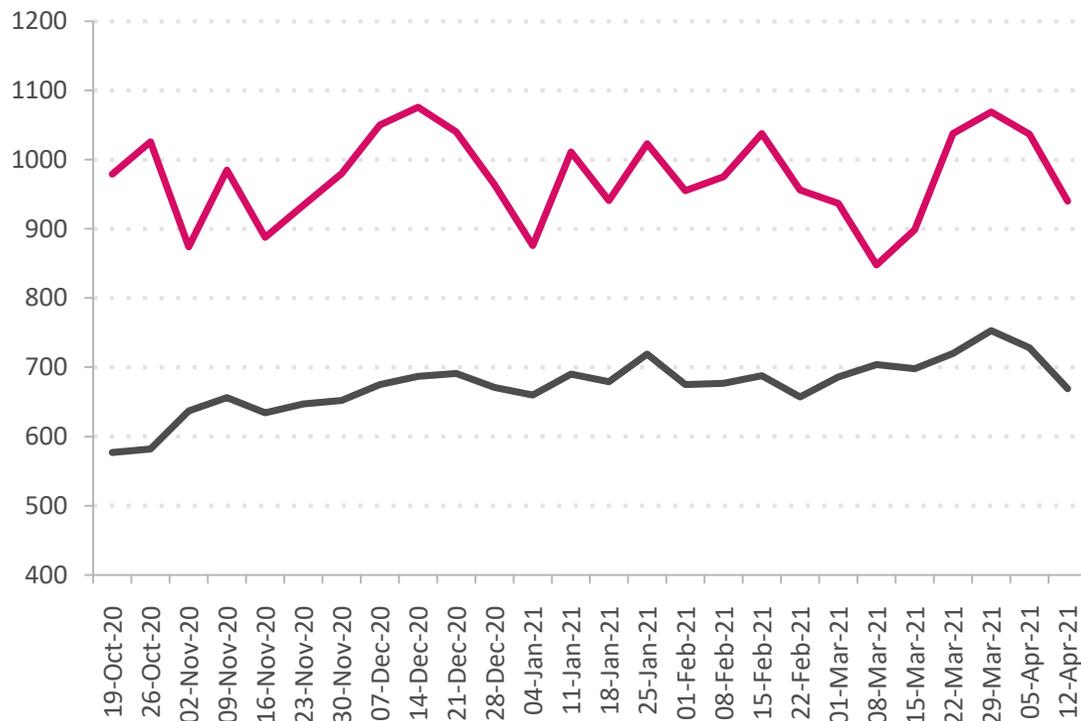
Никита Турков | nikitat@checkpoint.com

РАБОТАЕМ ОТКУДА УГОДНО И КАК УГОДНО

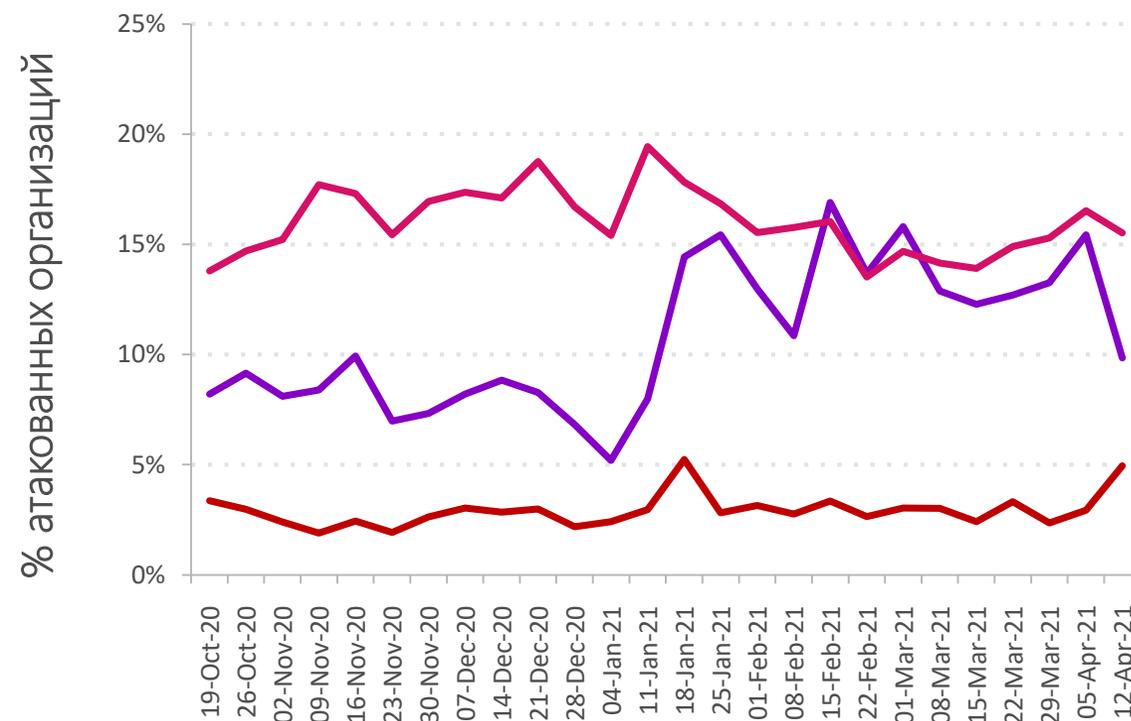


КИБЕРАТАКИ НА ОРГАНИЗАЦИИ В РОССИИ И СНГ

В сред. на орг. в нед. — СНГ — мир



— Банкеры — Ботнеты — Вымогатели

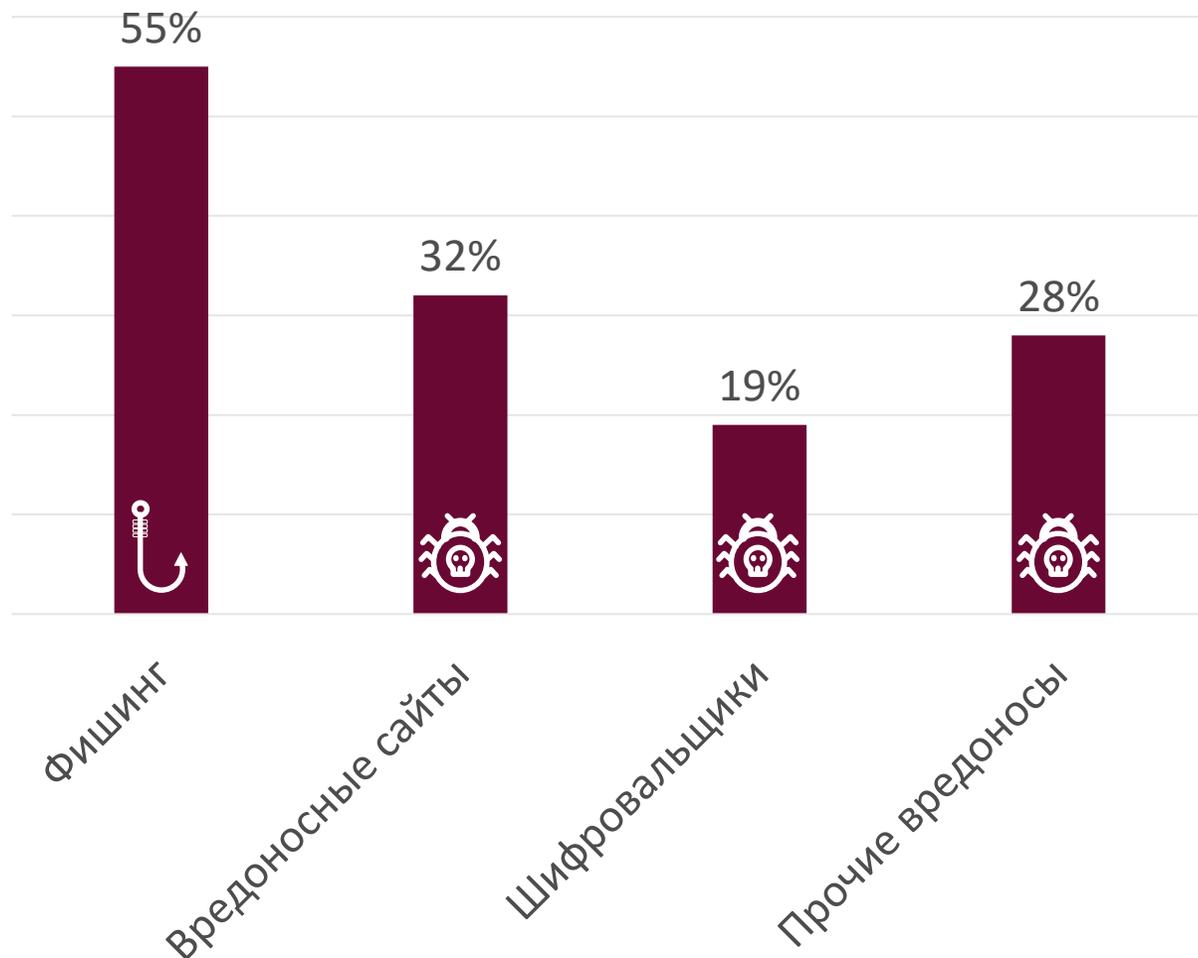


Топ вредоносков:

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



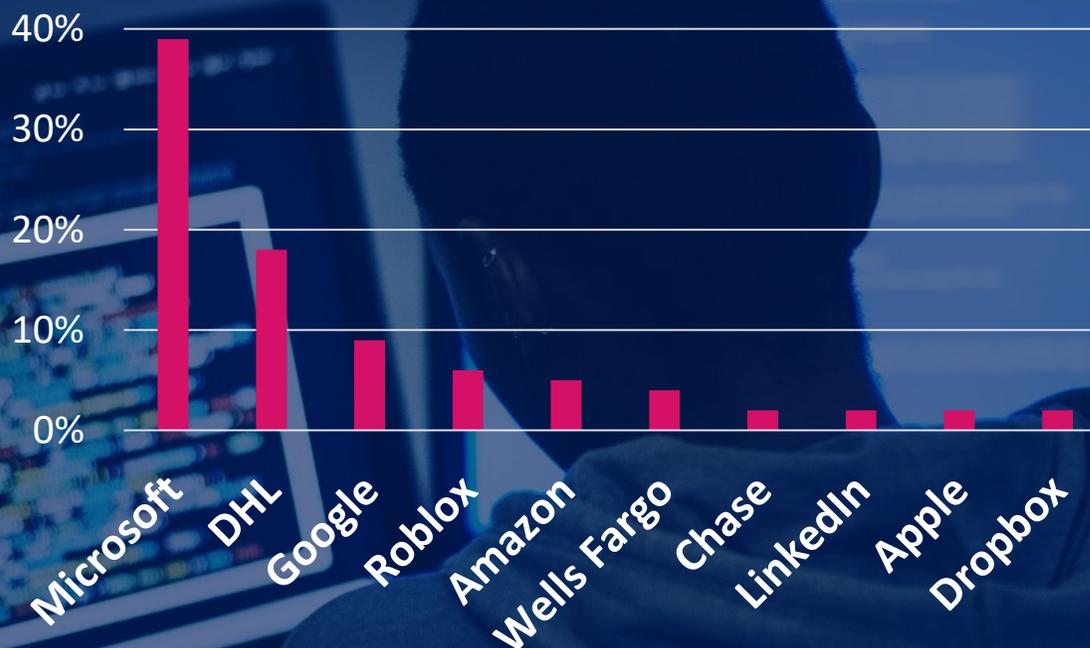
71% из 411 опрошенных специалистов **столкнулись с увеличением количества кибер-атак** в связи эпидемией коронавируса и массовым переходом на удаленку

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/>



Фишинг в 1 кв. 2021



ЗЛОУМЫШЛЕННИКИ ПОЛЬЗУЮТСЯ СИТУАЦИЕЙ
**ВСПЛЕСК АТАК ВЫМОГАТЕЛЕЙ И
ФИШИНГА В МИРЕ**

\$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

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.

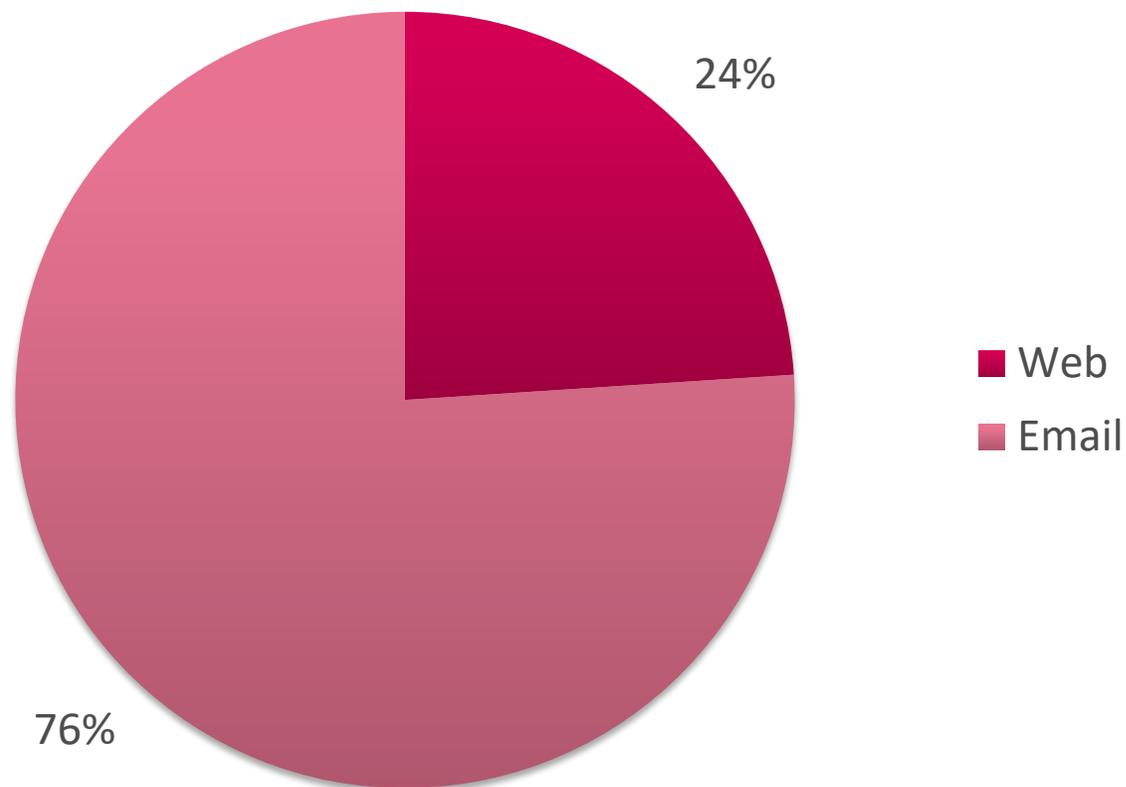
Злоумышленник знает психологию и использует:

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

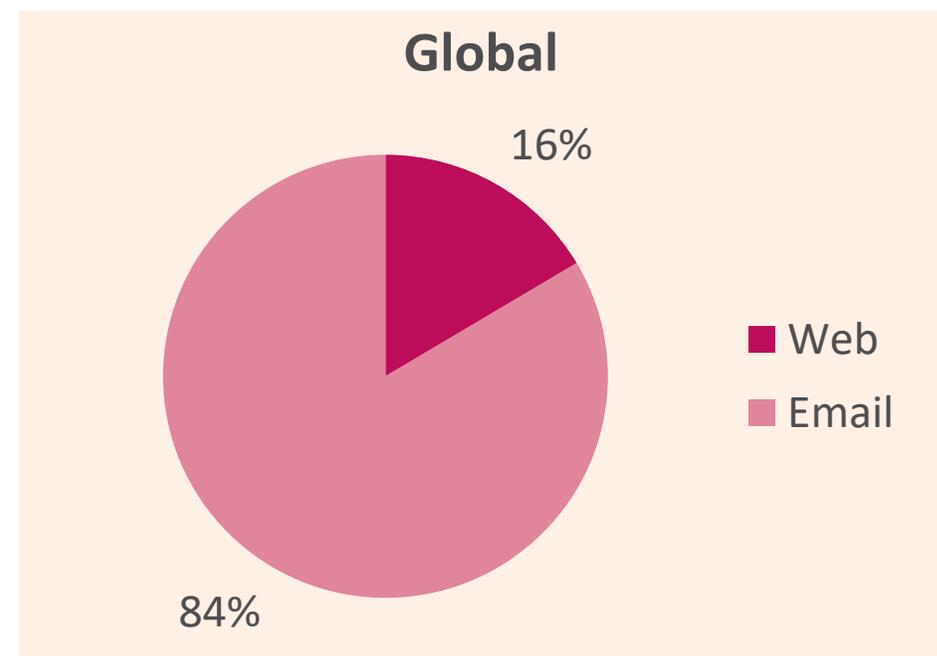


ВЕКТОРЫ АТАК В РФ ЗА ПОСЛЕДНИЕ 30 ДНЕЙ - ЭЛЕКТРОННАЯ ПОЧТА!

Russia



Global



ВИДЫ ФИШИНГА



Скам

Мошенничество, которое нацелено на быстрое получение денег обманным путём.

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.

Вишинг

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

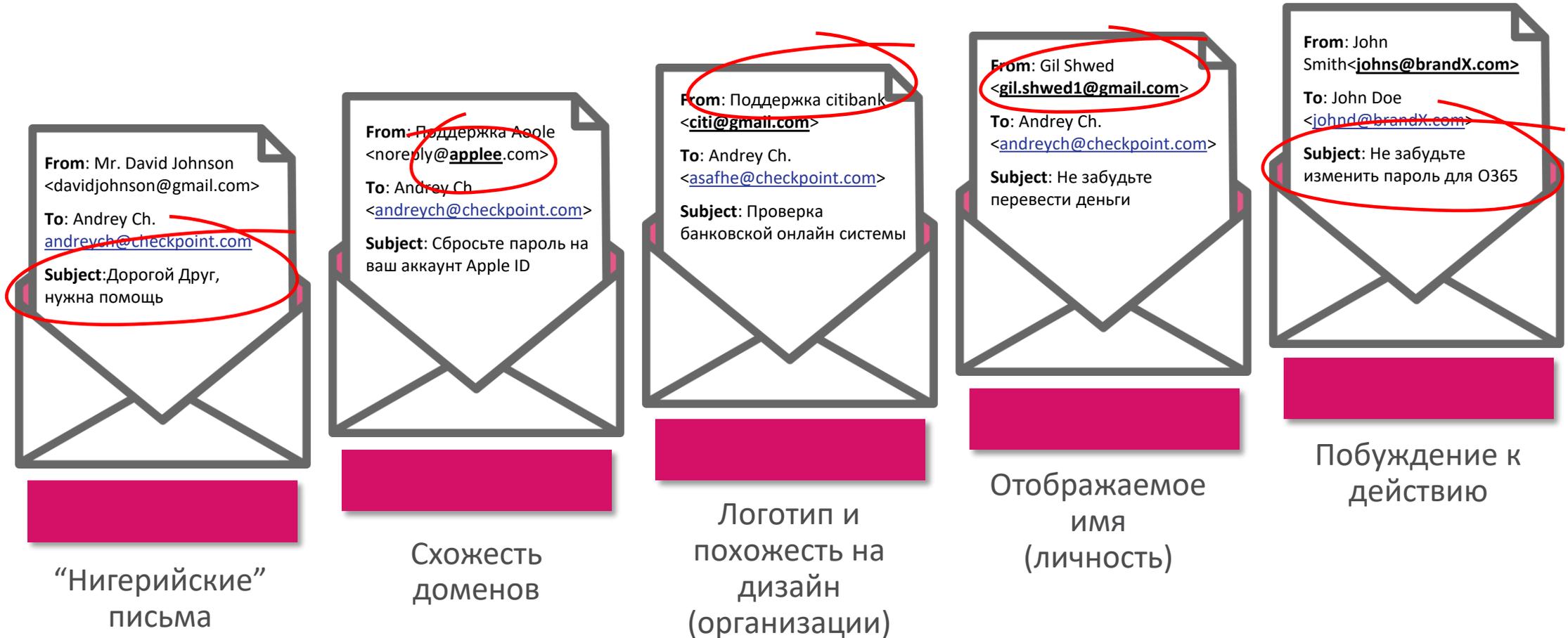
Смишинг

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.

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.



Уважаемый [REDACTED]

Отдел по работе с клиентами Сбербанка требованиями Федерального закона «О полученных преступным путем и фидуциарных обязательствах Банка России «Об идентификации получателей в целях предотвращения преступным путем, и фидуциарные должны предоставить информацию согласно доступной в Личном Кабинете по ссылке

[Форма «Информационные сведения Клиента»](#)

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]



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)

Министерство РФ
и России

судебному делу №21365. Вам, на вас должен быть вызван на судебное заседание по адресу (ч.2 ст. 168 ГПК РФ) электронный адрес был предоставлен в электронном виде услуг и документов, вы можете оставить свои комментарии. Подробности в архиве

Исполнитель Курицын В. А.

Долженности можно по [ссылке](#)

срок за 2015 год и ранее

«на сумму налога», неуплата налога, либо к уголовной ответственности. Пожалуйста погасите

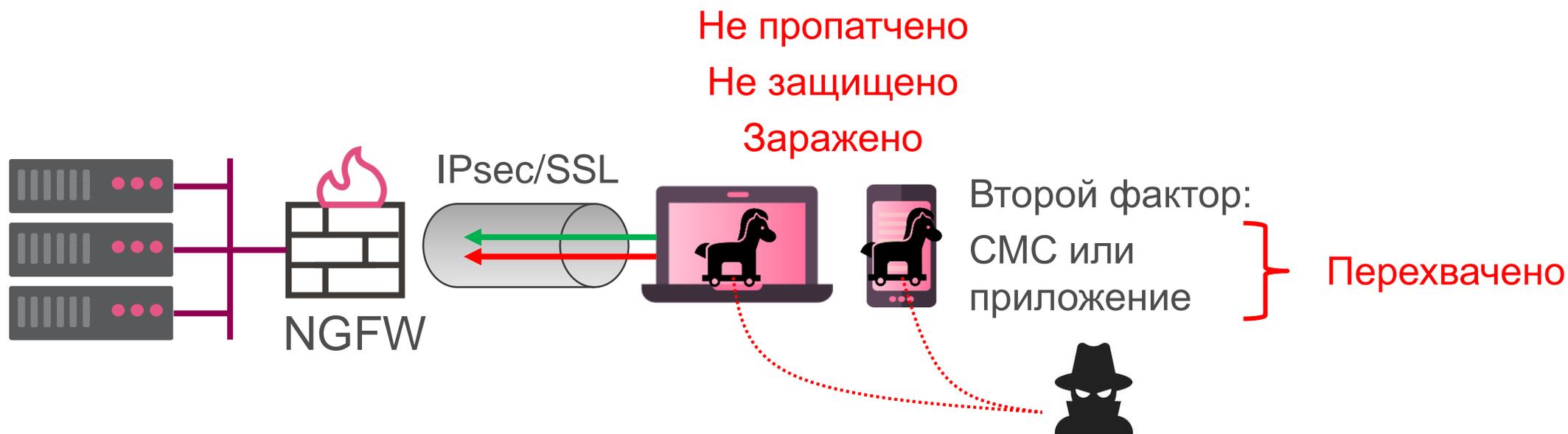
АТАКИ МОГУТ БЫТЬ МАКСИМАЛЬНО ТАРГЕТИРОВАННЫМИ

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:

- 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

Rampant Kitten

September 18, 2020

НЕСМОТРЯ НА ОБУЧЕНИЕ, ПОЛЬЗОВАТЕЛИ ПОПАДАЮТ НА УДОЧКУ ЗЛОУМЫШЛЕННИКОВ

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



Вредоносы «Резюме»

Reply Reply All Forward IM

Thu 19/3/2020 14:31

 Annie Baker <Baker12@aoll.com >
Job Application

To Martha Hunter

 Annie's Resume.doc
38 KB

Good Morning,

My name is Annie and I am looking for a job.
Please see my resume attached. The password is: 199

Looking forward to your reply.

Annie Baker



Фишинг «Срочно!»

File Message Developer Tell me what you want to do...

Fri 2018-09-14 23:21

Mail Administrator <kania@indonesian-aerospace.com >
Mailbox De-activation Notice

To

Deactivation Notice

We have received a request to delete your account. Your account will be removed from the site shortly and will be permanently deleted within 24hrs.

(Note: Please ignore this message if the request was from you. If you wish to cancel this request, do so immediately by verifying your details.)

[Verify Now](#)

If you have additional questions, please contact customer service.

Thanks,
Mail Administrator.

01

МЕТАДАННЫЕ

Проверить отправителя

DNS

База данных

Имперсонализация

From: Msoutlookmoc.kooltuo.ecivres@94	Is Deleted: Not deleted
To: John Doe	User Mailbox: john.d@cloudsec.onmicrosoft.com
Subject: john.d@cloudsec.onmicrosoft.com	Is Read: Unread
Content type: Password Reset Required	Sender is external: Yes
Email received: HTML	Any recipient is external: No

81.80 KB 1 file attached

test41.pdf
81.80 KB

Dear John

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 7/18/2018. The action requested is as follows:

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

New password should meet the password criteria:

*at least 8 characters.

*contain at least one capital letter

*contain at least one small letter

*contain at least special character

*don't use the last 3 password used before.

*don't include the first 2 characters from your user name

example of good password: A@qr*981

The link above expires after 24 Hours. If you don't change your password before then, your Outlook Web App account locked for security.

Thank you,
Maintenance and Operations.

Source: Email Security Team.

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

From: Msoutlookmoc.kooltuo.ecivres@94
To: [John Doe](#)
Subject: [john.d@cloudsec.onmicrosoft.com](#)
Content type: Password Reset Required
Email received at: HTML
10:51:45 2018-7-18

Is Deleted: Not deleted
User Mailbox: [john.d@cloudsec.onmicrosoft.com](#)
Is Read: Unread
Sender is external: Yes
Any recipient is external: No

81.80 KB 1 file attached

 test41.pdf
81.80 KB

Dear John

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 7/18/2018. The action requested is as follows:

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

New password should meet the password criteria:

*at least 8 characters.

*contain at least one capital letter

*contain at least one small letter

*contain at least special character

*don't use the last 3 password used before.

*don't include the first 2 characters from your user name

example of good password: A@q*981

The link above expires after 24 Hours. If you don't change your password before then, your Outlook Web App account locked for security.

Thank you,
Maintenance and Operations.

Source: Email Security Team.

02

ВЛОЖЕНИЯ

Проверить файлы

ANTI-VIRUS

THREAT EMULATION

THREAT EXTRACTION

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

From: Msoutlookmoc.kooltuo.ecivres@94
To: [John Doe](#)
Subject: [john.d@cloudsec.onmicrosoft.com](#)
Content type: Password Reset Required
Email received at: HTML
10:51:45 2018-7-18

Is Deleted: Not deleted
User Mailbox: [john.d@cloudsec.onmicrosoft.com](#)
Is Read: Unread
Sender is external: Yes
Any recipient is external: No

81.80 KB 1 file attached

 test41.pdf
81.80 KB

Dear John

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 7/18/2018. The action requested is as follows:

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

New password should meet the password criteria:

*at least 8 characters.

*contain at least one capital letter

*contain at least one small letter

*contain at least special character

*don't use the last 3 password used before.

*don't include the first 2 characters from your user name

example of good password: A@q*981

The link above expires after 24 Hours. If you don't change your password before then, your Outlook Web App account locked for security.

Thank you,
Maintenance and Operations.

Source: Email Security Team.

03

ССЫЛКИ

Репутация и схожесть

Сведения о домене

Проверить в момент клика

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

From: Msoutlookmoc.kooltuo.ecivres@94
To: [John Doe](#)
Subject: [john.d@cloudsec.onmicrosoft.com](#)
Content type: Password Reset Required
Email received at: HTML
10:51:45 2018-7-18

Is Deleted: Not deleted
User Mailbox: [john.d@cloudsec.onmicrosoft.com](#)
Is Read: Unread
Sender is external: Yes
Any recipient is external: No

81.80 KB 1 file attached

test41.pdf
81.80 KB

Dear John

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 7/18/2018. The action requested is as follows:

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

New password should meet the password criteria:

- *at least 8 characters.
 - *contain at least one capital letter
 - *contain at least one small letter
 - *contain at least special character
 - *don't use the last 3 password used before.
 - *don't include the first 2 characters from your user name
- example of good password: A@qr*981

The link above expires after 24 hours. If you don't change your password before then, your Outlook Web App account locked for security.

Thank you,
Maintenance and Operations.

Source: Email Security Team.

04

ЯЗЫК

Проверить заголовок и тело

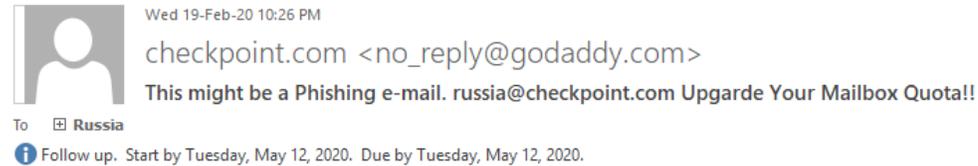
Сигнатуры фраз

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



PHISHING ALERT!

For your own protection, it is not recommended to click on links in this email or open any attachment.

Check Point Anti-Phishing has detected that this email was sent by a malicious user.

Report not Phishing

Mail Quota: (98% Full)

Hello russia@checkpoint.com

Your email quota has reached 98% and will soon exceed its limit.

Follow the URL below to upgrade your quota to **25GB** for free to avoid loss of email data.

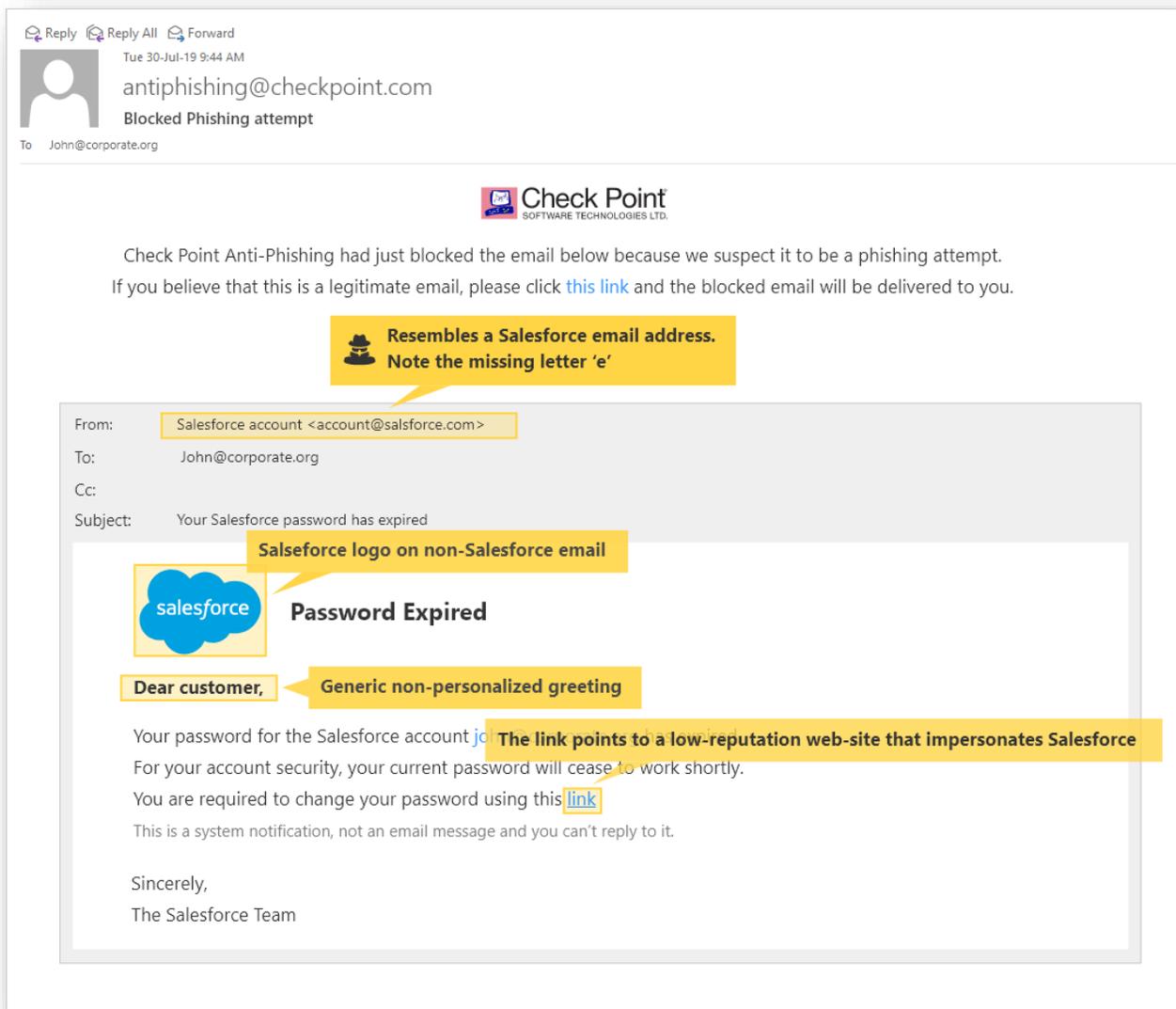
[Upgrade Email Quota](#)

Source: **checkpoint.com Administrator**

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



Блокируем продвинутый фишинг нулевого дня С помощью машинного обучения



Reply Reply All Forward
Tue 30-Jul-19 9:44 AM
antiphishing@checkpoint.com
Blocked Phishing attempt
To John@corporate.org

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point Anti-Phishing had just blocked the email below because we suspect it to be a phishing attempt. If you believe that this is a legitimate email, please click [this link](#) and the blocked email will be delivered to you.

Resembles a Salesforce email address. Note the missing letter 'e'

From: Salesforce account <account@salsforce.com>
To: John@corporate.org
Cc:
Subject: Your Salesforce password has expired

Salsforce logo on non-Salesforce email

salesforce
Password Expired

Dear customer, **Generic non-personalized greeting**

Your password for the Salesforce account [john@corporate.org](#) has expired. **The link points to a low-reputation web-site that impersonates Salesforce**
For your account security, your current password will cease to work shortly.
You are required to change your password using this [link](#)
This is a system notification, not an email message and you can't reply to it.

Sincerely,
The Salesforce Team



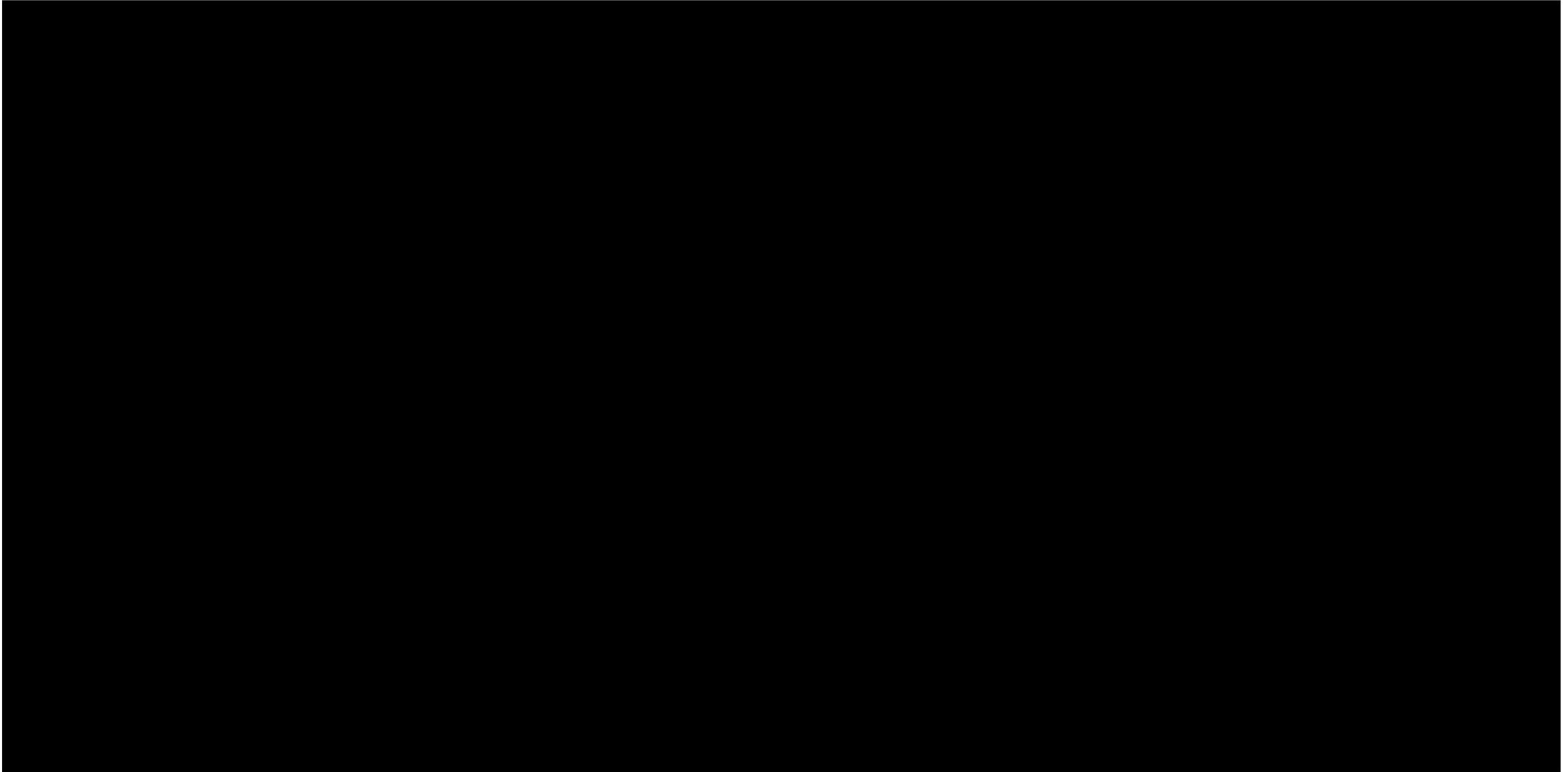
300+
индикаторов
в модели
ML/AI

Обучаем пользователей,
на что обращать внимание

Проактивная очистка и быстрая доставка документов пользователям

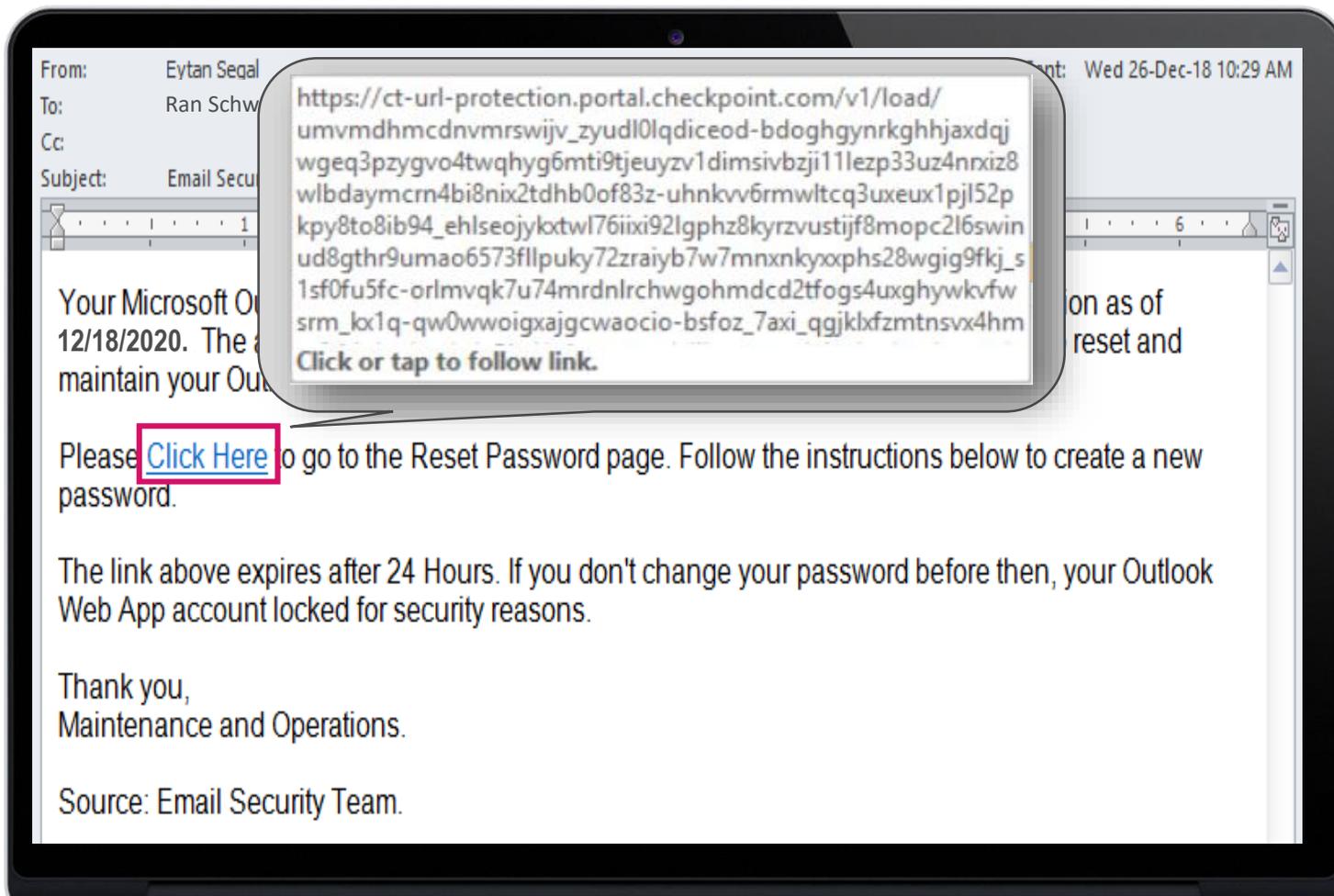


Инспекция вложений, защищенных паролем



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!)

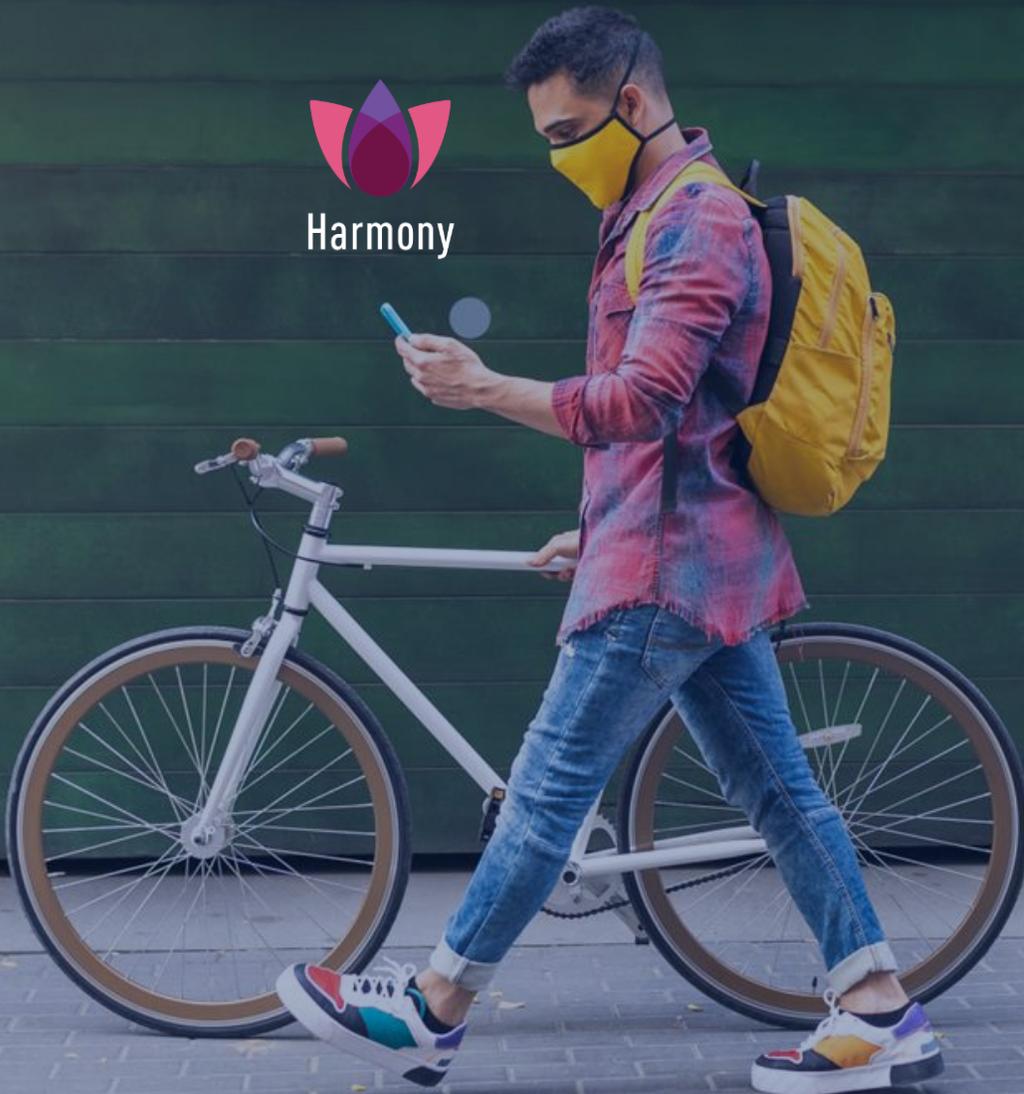
- **Будьте осторожны с подозрительными письмами, побуждающими Вас к немедленным действиям.**
- **Не переходите по ссылкам, не кликайте на подозрительные объекты.**
- **Будьте осторожны с вложениями, открывайте только те, которые ждали.** Во вложениях также будьте осторожны с ссылками.
- **Сверяйте адрес 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.



Harmony



Сергей Забула | szabula@checkpoint.com

Никита Турков | nikitat@checkpoint.com