АНТИФИШИНГ

ГОДОВОЙ ОТЧЕТ О ЗАЩИЩЕННОСТИ
СОТРУДНИКОВ ЗА 2021 ГОД

Люди как часть стратегии
эшелонированной защиты
информации в 2022 году

Введение в проблему

Человеческий фактор — по-прежнему одна из главных проблем современной информационной безопасности, а социальная инженерия – основной инструмент мошенников.

У большинства компаний к 2022 году уже появились все лучшие средства защиты и стандартизированные процессы безопасности, но для борьбы с современными цифровыми атаками и предотвращения инцидентов технических средств и стандартных процессов недостаточно.

Требуется дополнительный уровень защиты, основу которого составляют люди — рядовые сотрудники, разработчики ПО и даже клиенты организации.

Введение в проблему

Для 42% атак-вымогателей первоначальный доступ был получен благодаря фишингу, столько же пришлось на RDP-атаки через слабые пароли, которые тоже устанавливают люди.

Инцидент с уязвимостью в системе подачи заявок на кредит привел к утечке данных 104 тысяч клиентов банка Дом.РФ. В общем доступе оказался полный набор персональных данных для оформления потребительского кредита: Ф.И.О., дата рождения, сумма кредита, номер телефона, почтовый ящик, паспортные данные, ИНН, СНИЛС, домашний адрес, адрес места работы, должность, размер дохода. Этих данных хватит, чтобы мошенники могли оформить кредит на любого человека и получить от его имени деньги.

Причина инцидента и уязвимости — недостаток знаний и навыков по безопасной разработке у сотрудников, ответственных за разработку ПО.

По данным ЦБ РФ за 2021 год в России было совершено более миллиона операций без согласия клиентов финансовых организаций. Объём таких операций превысил 13,5 млрд рублей. По сравнению с аналогичными показателями предыдущего года количество и объём не согласованных операций увеличились на 33,8 и 38,8% соответственно.

Приёмы и методы социальной инженерии оставались основным инструментом, с помощью которого злоумышленники похищали средства физических и юридических лиц. Доля операций с использованием социальной инженерии составила почти 50%, а средняя сумма одного хищения с помощью таких приёмов возросла.

Одним из ярких инцидентов с применением методов социальной инженерии стала атака на профессора психологии НИИ им. Сербского — Аллу Аведисову.

Мошенник позвонил профессору и представился сотрудником отдела безопасности Росбанка и заявил, что на ее имя попытались получить кредит в 1 млн рублей. Чтобы защититься, профессору нужно было срочно снять со счёта все свои сбережения и передать их «сотруднику банка» на ответственное хранение. Общая сумма ущерба составила более 14 млн рублей.

АНТИФИШИНГ

В отчете о защищенности сотрудников за 2021 год мы постарались описать:

1. Как именно реализация техник злоумышленников на этапе проникновения в сеть зависит от действий людей.
2. Какие инциденты происходили в 2021 году в компаниях из разных отраслей из-за небезопасных действий людей с участием сотрудников разных должностей.
3. Какие приемы фишинга были самыми опасными для сотрудников.
4. Как измерить защищенность сотрудников и киберустойчивость организации, и как системно улучшать эти показатели с помощью методологии Антифишинга.
5. Что сделать в первую очередь для повышения защищенности своих сотрудников и организации от цифровых атак в реалиях 2022 года.

Структура отчета

1 В первом разделе отчета мы проанализировали связь действий людей с техниками на этапе проникновения по самой актуальной классификации MITRE ATT&CK.

2 Во втором разделе мы изучили и разобрали поведение людей на примере пяти реальных цифровых атак в 2021 году.

3 В третьем разделе мы оценили защищенность сотрудников в зависимости от отраслей, отделов и ролей в компании на основе статистики поведения более чем 21 тысячи сотрудников в более чем 40 тысячах имитированных атак за 2021 год.

4 В четвертом разделе мы оценили технические факторы, которые влияют на успех цифровых атак против сотрудников: каналы, по которым доставлялись атаки, а также зависимость действий сотрудников от типа вложений и других факторов.

5 В пятом разделе мы оценили психологические факторы, которые наиболее сильно влияют на небезопасное поведение — источники атак, персонификацию, использование в атаках эмоций и психологических усилителей — и разобрали три самые эффективные имитированные атаки Антифишинга 2021 года.

6 В шестом разделе мы рассмотрели показатели, отражающие эффективность процесса обучения сотрудников вопросам безопасности и тренировки их навыков по методологии и на базе платформы «Антифишинг» спустя 9 месяцев после первой атаки: снижение количества небезопасных действий и рост числа сообщений сотрудников об атаках.

7 В седьмом разделе мы дали рекомендации по обучению людей защите от цифровых атак: с каких шагов стоит начать прямо сейчас, как сформировать группы риска, что делать с сотрудниками, которые не проходят курсы вовремя или ведут себя небезопасно.

Источники данных

Отчет составлен на основе обезличенных данных от наших клиентов, которые согласились предоставить данные, а также на базе открытых источников и собственных исследований компании Антифишинг.

40 000
имитированных фишинговых атак за 2021 год

> 21 000
сотрудников

37
компаний

Основные выводы

до 100%

насколько небезопасные действия людей влияют на успех техник MITRE ATT&CK на этапе проникновения

в 96%

случаев реальных атак каналом доставки была электронная почта

30% сотрудников открывали фишинговые письма

21% из них совершали другие опасные действия

Психологические факторы, которые используются в атаке и больше всего влияют на совершение опасных действий:

44% Невнимательность

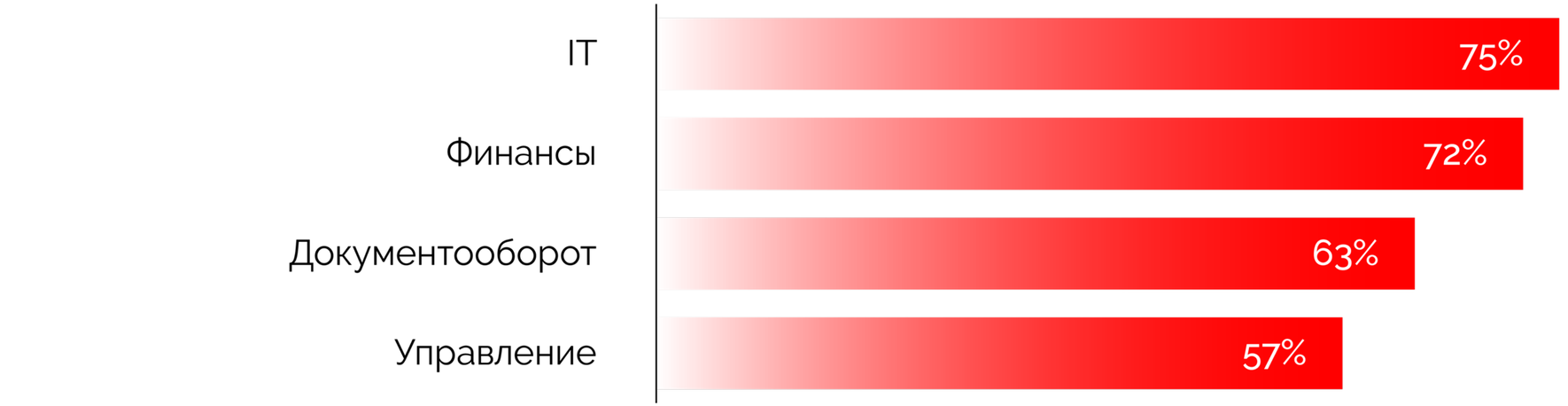
54% Авторитет

Наиболее опасным типом вложения являются DOCX-файлы. В 15% имитированных атак с ними совершаются небезопасные действия

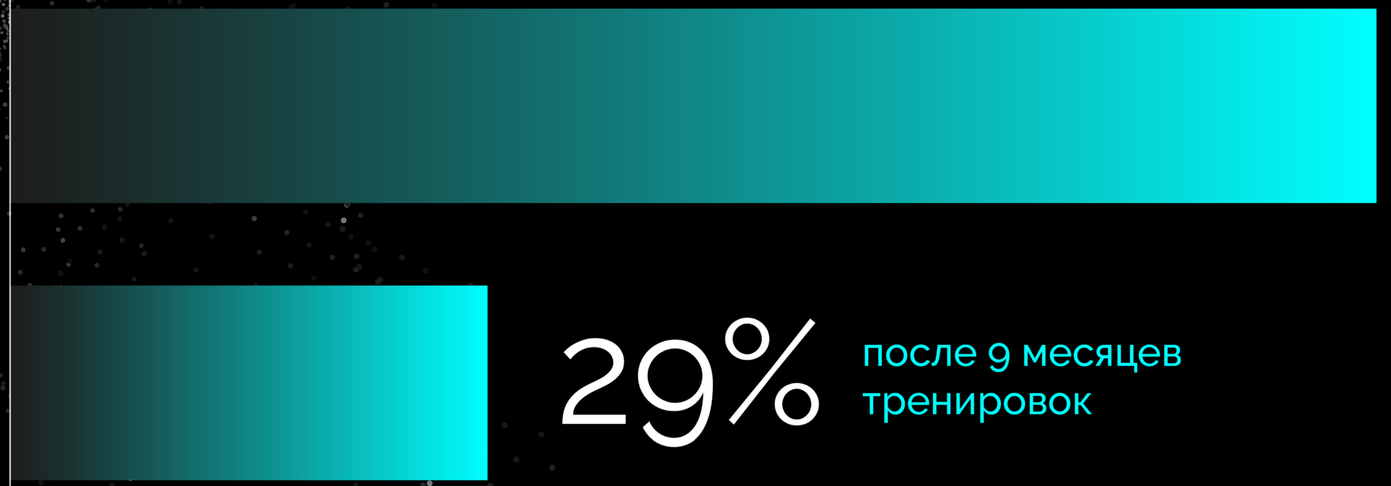
Наиболее уязвимы к фишингу (% небезопасных действий):

Сотрудники компаний из сферы

Сотрудники из отделов



Доля открытых писем



83% после первой атаки

29% после 9 месяцев тренировок

в 3 раза

сократился процент открытий фишинговых писем

≈ в 6 раз

сократился процент перехода на фишинговый сайт

Доля сотрудников, сообщивших о фишинговых письмах

Тренировка навыков помогает формировать желаемое поведение, полезное для защиты организации от цифровых угроз. Если вначале от сотрудников не поступало сообщений об атаках, то через 9 месяцев тренировок о фишинге сообщали 66% всех сотрудников в выборке.

1 Статистика атак по классификации MITRE

Команды безопасности во всем мире традиционно используют матрицу MITRE ATT&CK для анализа и разбора актуальных техник, тактик и технологий, которые используют злоумышленники. Считается, что почти все техники связаны с техническими уязвимостями, недостатками конфигурации и методами атак.

Статистика атак по классификации MITRE

Мы проанализировали все техники на этапе проникновения — Initial Access по классификации MITRE ATT&CK и разобрались, как действия людей связаны с каждой техникой.

В результате выяснилось, что 9 из 9 техник Initial Access по классификации MITRE ATT&CK реализуются полностью или частично из-за недостатка знаний или навыков по информационной безопасности.

Для сравнения техник по степени влияния человеческого фактора мы предложили индекс Антифишинга: экспертную оценку и расчет в процентном выражении, насколько успех каждой техники зависит от небезопасных действий людей.

Индекс Антифишинга — степень влияния человеческого фактора, — может различаться в диапазоне от 100% при фишинге до 20% в случае использования уязвимостей публичных приложений.

T1189

Теневая загрузка (Drive-by Compromise)

Бухгалтер компании искала информацию на специализированном форуме для бухгалтеров.

Этот веб-сайт был скомпрометирован злоумышленниками, они разместили на нем файлы под видом шаблонов бухгалтерских документов.

Бухгалтер загрузила данный файл себе, открыла его, и после этого на ее компьютер было установлено вредоносное ПО. С его помощью злоумышленник получил доступ к компьютеру бухгалтера и похитил денежные средства.

Публичный кейс по описанному сценарию атаки.

Индекс Антифишинга: 50%

T1190

Эксплоиты публичных приложений (Exploit Public-Facing Application)

Сотрудники отдела IT не устанавливали обновления безопасности для Atlassian Jira.

Злоумышленники использовали неисправленные уязвимости веб-сервера организации и установили троян удаленного доступа в систему организации. Это позволило им получить полный доступ ко всем задачам и исходным кодам продуктов компании.

Индекс Антифишинга: 20%

T1133

Внешние службы удаленного доступа (External Remote Services)

Сотрудник использовал RDP-соединение для доступа к рабочему компьютеру из дома. При этом пароли от личной электронной почты и пароль для доступа совпадали. Пароль был скомпрометирован и попал в базу утекших паролей.

Злоумышленники используя эти данные получили доступ к сети организации и установили программу для шифрования, запросив выкуп.

Индекс Антифишинга 50%

T1200

Подключение дополнительных устройств (Hardware Additions)

Злоумышленник проник в здание организации под видом курьера и подключил нетбук к локальной сети организации. Затем он собрал информацию о сети, серверах и рабочих станциях, используемых для осуществления платежей, и перехватил данные для входа на них.

Далее на зараженных компьютерах запустил вредоносное ПО, с помощью которого были совершены переводы денежных средств.

Индекс Антифишинга 50%

T1566 Фишинг (Phishing)

.001 Целевой фишинг с вложением (Spearphishing Attachment)

Сотрудник отдела IT получил письмо с приглашением на участие в конференции с описанием и референсами во вложении.

Он открыл файл, после чего вредоносная программа запустилась на ПК сотрудника, и мошенники получили доступ к корпоративной сети компании.

.002 Целевой фишинг со ссылкой (Spearphishing Link)

Сотрудник отдела IT получил письмо с приглашением на участие в конференции с описанием и референсами во вложении.

Он открыл файл, после чего вредоносная программа запустилась на ПК сотрудника, и мошенники получили доступ к корпоративной сети компании.

.003 Целевой фишинг через сторонние сервисы (Spearphishing via Service)

Злоумышленник создал поддельный аккаунт в социальной сети LinkedIn и связался через нее с сотрудником компании под видом представителя конкурирующей фирмы.

Он предложил сотруднику аналогичную должность с окладом больше текущего и для ознакомления с условиями отправил ему на личную почту файл с описанием вакансии.

Сотрудник открыл данное письмо на рабочем компьютере и после открытия вложения на компьютере было установлено вредоносное ПО.

Это позволило атакующему получить доступ в сеть компании и зашифровать данные.

Публичный кейс по описанному сценарию атаки.

Индекс Антифишинга **100%**

T1091

Распространение через съемные носители (Replication Through Removable Media)

Злоумышленники рассылали компаниям по почте красивые коробки-подарки от лица Amazon, в которых были поздравительная открытка и USB-устройство.

Сотрудник подключал полученный девайс к ПК, устройство выполняло атаку типа BadUSB, в ходе которой устройство использовало HID, регистрировало себя как клавиатуру и передавало серию предварительно заданных нажатий клавиш машине пользователя.

Эти нажатия клавиш запускали команды #PowerShell, которые загружали и устанавливали различный вредоносный софт, действовавший как бэкдор для доступа к инфраструктуре компании.

Публичный кейс по описанному сценарию атаки.

Индекс Антифишинга **100%**

T1199

Доверительные отношения (Trusted Relationship)

Системный администратор предоставил доступ стороннему внешнему подрядчику, обслуживающему СКУД, к внутренней сети компании.

Действительные учетные записи, используемые подрядчиком для доступа к внутренним сетевым системам, были скомпрометированы и использованы для сбора и передачи клиентских данных злоумышленникам.

Индекс Антифишинга **50%**

T1195 Компрометация цепочки поставок (Supply Chain Compromise)

.001 Компрометация программных зависимостей и инструментов разработки (Compromise Software Dependencies and Development Tools)

Разработчик получил проект и начал разработку ПО с использованием открытого исходного кода с GitHub.

Данный код изначально содержал часть вредоносного кода, добавленного злоумышленниками.

В итоге заказчик получил ПО с уязвимостями, которые позволили злоумышленнику похитить клиентские данные.

.002 Компрометация цепочки поставок ПО (Compromise Software Supply Chain)

Злоумышленники скомпрометировали разработчика известного прикладного программного обеспечения и внесли изменения в выпускаемое ПО до его получения конечным потребителем.

В результате данные компании, пользующейся данным ПО, были похищены и был запрошен выкуп за их неразглашение.

.003 Компрометация цепочки поставок комплектующих (Compromise Hardware Supply Chain)

Злоумышленники модифицировали аппаратные компоненты сетевых маршрутизаторов до их получения конечным потребителем.

Сотрудники компании установили данные устройства в свою сеть, не выполнив физический осмотр оборудования на предмет возможного несанкционированного доступа.

В итоге злоумышленники получили доступ к сети компании и использовали ее ресурсы, установив криптомайнер.

Индекс Антифишинга 50%

T1078 Существующие учетные записи (Valid Accounts)

.001 Учетные записи по умолчанию (Default Accounts)

Сотрудники компании установили сетевые накопители в свою инфраструктуру.

Данные устройства поставляются с предустановленной комбинацией имени пользователя и пароля, которые не были изменены после установки. Это позволило атакующим получить доступ к данным организации.

Индекс Антифишинга **100%**

.002 Доменные учетные записи (Domain Accounts)

Администратор компании не использовал многофакторную аутентификацию (MFA) для учетной записи администратора домена.

После компрометации логина и пароля этой учетной записи злоумышленники получили полный доступ в сеть компании и зашифровали данные, запросив выкуп.

Индекс Антифишинга **100%**

T1078 Существующие учетные записи (Valid Accounts)

.003 Локальные учетные записи (Local Accounts)

На всех компьютерах компании для учетной записи локального администратора были установлены одинаковые пароли.

Компрометация одного из сотрудников позволила злоумышленникам получить доступ ко всем компьютерам компании, повысить привилегии и привела к уничтожению данных.

Индекс Антифишинга **100%**

.004 Облачные учетные записи (Cloud Accounts)

В компании использовали облачный почтовый сервер, при этом не была настроена многофакторная аутентификация для облачных привилегированных учетных записей.

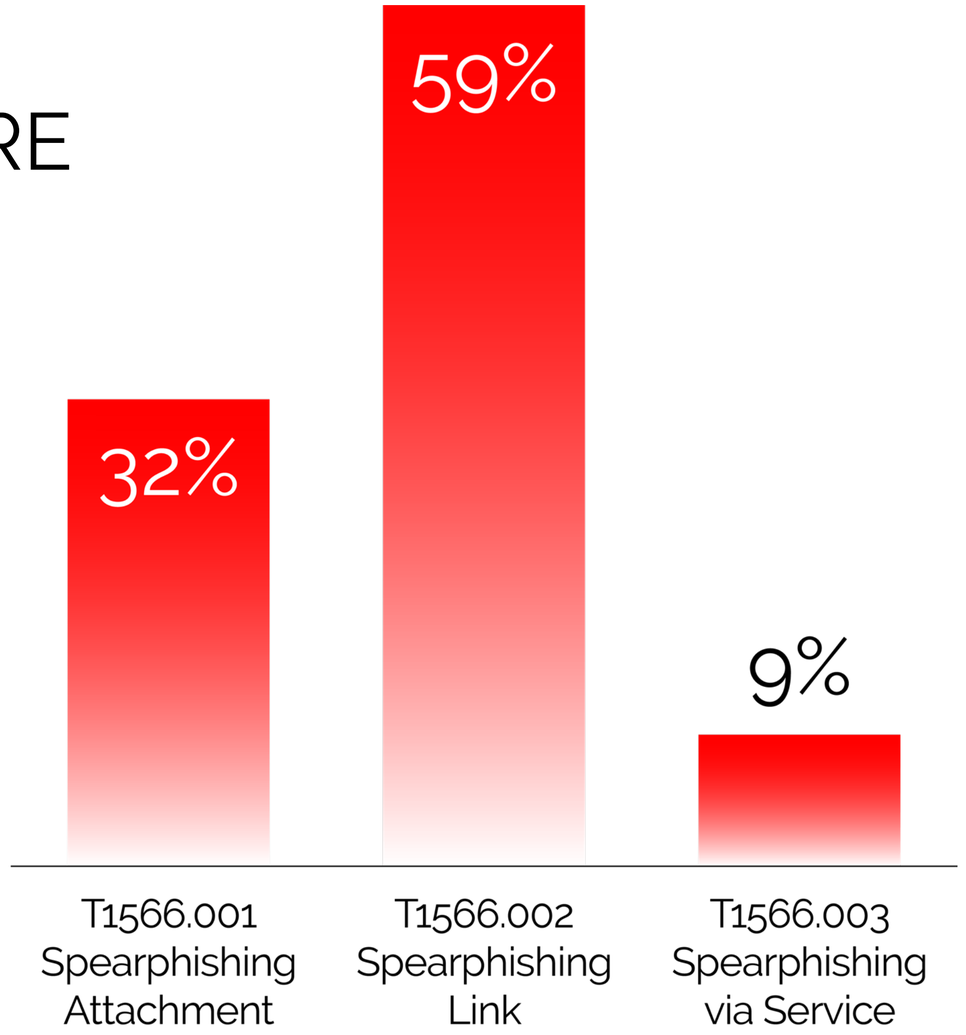
Компрометация такой записи позволила атакующим получить полный доступ к корпоративной электронной почте.

Индекс Антифишинга **50%**

Статистика атак по классификации MITRE

То, что считается классической техникой атаки на человека — фишинг — только одна из девяти техник проникновения в базе MITRE. Однако, как показывают наши примеры, мошенники используют человеческий фактор в каждой из перечисленных техник.

За год мы разобрали порядка 100 инцидентов, связанных с цифровыми атаками на людей. Согласно нашей статистике, на атаки с использованием различных техник фишинга (T1566) приходится:



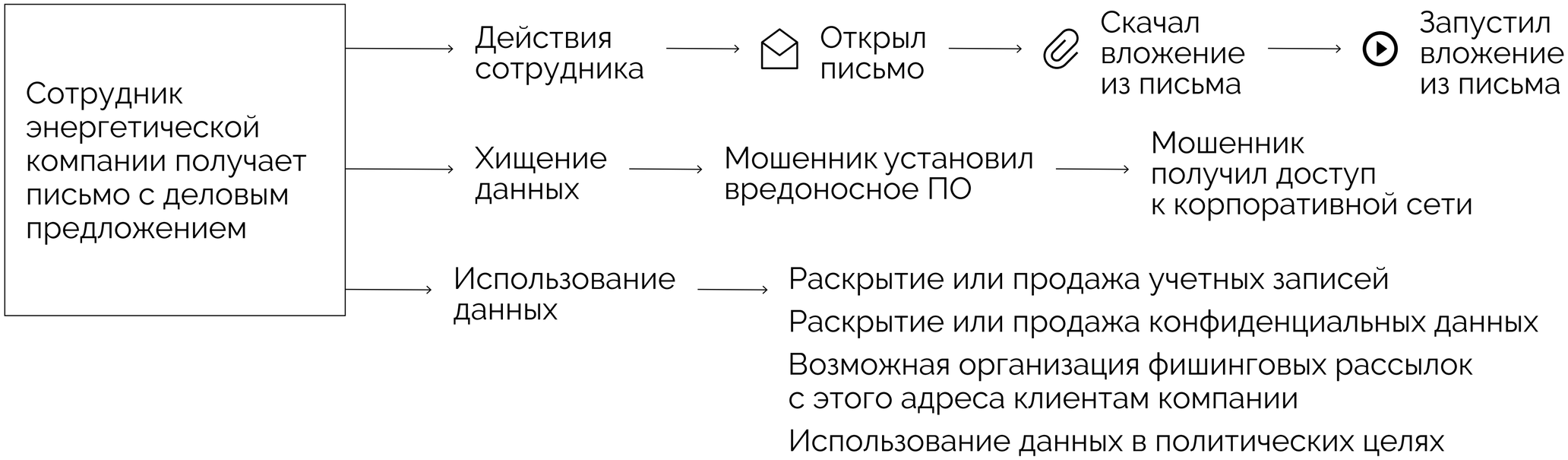
2 Разбор пяти цифровых атак на людей в 2021 году

На пяти примерах мы разобрали, как происходят фишинговые атаки и как именно ведут себя в таких ситуациях люди, занимающие различные должности. Атаки выбраны из базы знаний Антифишинга для демонстрации разнообразия возможных сценариев. Для каждого случая мы показываем, какие технические и психологические векторы используются злоумышленникам, к каким небезопасным действиям они подталкивают людей и каковы потенциальные последствия успешных атак.

1. Атака на компании энергетического сектора

Любопытство | Желание помочь | Невнимательность

Авторитет | Срочность



Организаторы глобальной фишинговой кампании атаковали крупные бизнесы из разных сфер, прежде всего энергетические компании и их поставщиков. Сотрудникам направлялись письма с предложением о партнерстве якобы от другой фирмы из этой же отрасли. Для убедительности текст письма был составлен в стиле деловой переписки и содержал отсылки к реальным проектам, связанным с деятельностью атакуемой компании. Приложение к письму (образ диска или архив) содержало исполняемый файл. Нажатие на него запускало вредоносную программу, позволяющую злоумышленникам похищать информацию с компьютера жертвы.

Mon 3/15/2021 8:56 PM

RASHID MAHMOOD <support@rcamanagement.es>

EPC for BAB SIMGAP EOR Pilot - Upgradation of Bab Project - RFQ for Solid FITTINGS PIPES & FLANGES.

To [redacted]@gsconst.co.kr

Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.
Outlook blocked access to the following potentially unsafe attachments: 17776-PIP-014_Rev-A-MTO Solid CRA Fittings Pipes and flanges For Bab Upgradation Project Xerox Scan_2021161134248.img.

Dear Sir / Madam,

China Petroleum Engineering & Construction Corporation (CPECC), have been invited to bid for the Bab Upgradation Project.

For the above said PROJECT, and as an ADCO approved vendor for the subject package you are hereby invited to submit your Technical & Commercial offer, in United States Dollars (USD) or in United Arab Emirates Dirham (AED), on or before the **21-Mar-2021** in accordance and total compliance with the instructions and specifications.

Your acknowledgement and Intention to Bid must be communicated to CPECC by return email by within two days from this email.

If your proposal contains any suggested improvements or deviates in any way from the RFQ documents the same should be highlighted and mentioned in vendor proposal cover letter.

Important Points for Compliance.

1) Please submit both Technical and Commercial offer separately.

2) MTO attached for pricing. (Please give us offer for all the items)

3) Your prices must be on CFR or DDU Abu Dhabi basis.

4) Prices validity must be 30 or more days.

5) Please provide optional prices separately if any.

6) Please submit ICV certification if applicable.

7) Please provide ADNOC approval document.

PLEASE DOWNLOAD SPECIFICATIONS FROM THE ATTACHED FILE

Best Regard,

RASHID MAHMOOD

Project Buyer

BAB Integrated Facilities Project

中国石油工程建设有限公司海湾地区公司

Right-clic

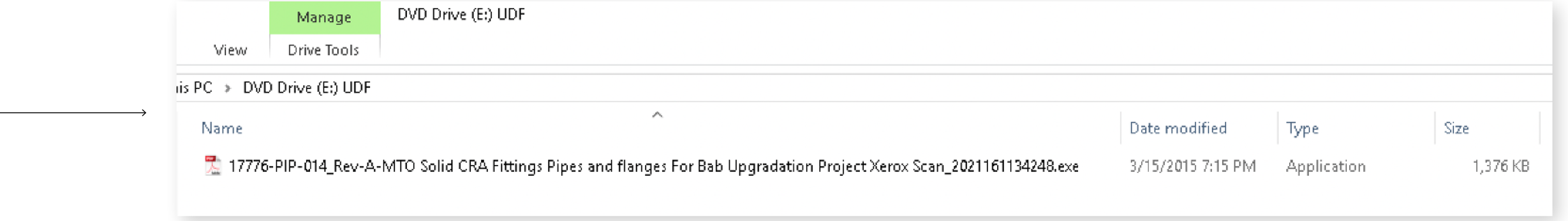
CHINA PETROLEUM ENGINEERING & CONSTRUCTION CORPORATION

Email. rashid.mahmood@cpecc.ae Website. www.cpecc.ae

Office Tel: Direct 971 (0)2-201-3412 Ext. 412 Fax. 971 (0)2-678-7799

Mobile 971 (0) 56-9900694

Файл образа подключенного диска с вредоносным двоичным кодом Snake Keylogger, маскирующимся под PDF



2. Атака от имени лондонской Школы востоковедения и африканистики

Любопытство | Желание помочь | Невнимательность | Авторитет

Специалисту по Ближнему Востоку приходит приглашение на online-мероприятие

→ Действия сотрудника → Открыл письмо → Перешел по ссылке из письма → Ввел данные учетной записи

→ Хищение данных → Мошенник получил данные учетной записи электронной почты

→ Использование данных → Сбор разведывательных данных из электронной почты жертвы в политических целях, в т.ч. организации саботажей, несанкционированных митингов

Возможная организация фишинговых рассылок с этого адреса

Заведомо ложное использование информации

Раскрытие данных спецслужбам других стран

Подрыв деятельности организации

Злоумышленники маскировались под сотрудников лондонской Школы востоковедения и африканистики (SOAS). Они рассылали избранным жертвам – исследователям и журналистам, занимающимся ближневосточной тематикой – письма с персонализированной ссылкой на фишинговую форму регистрации на online-мероприятие Школы. Целью этого было похищение учетных данных жертв для авторизации в Google, Microsoft, Facebook и Yahoo. Злоумышленники также предлагали обсудить приглашение по телефону. Фишинговая форма регистрации была размещена на легитимном, но скомпрометированном сайте радио SOAS.

Поддельное приглашение на конференцию

SOAS University of London

SOAS RADIO

To Dr. [redacted]
The Director [redacted]

Subject: Invitation to The Centre for International Studies and Diplomacy Webinar (CISD)

Dear Dr. [redacted]

You are cordially invited to participate as main speaker in the **Centre for International Studies and Diplomacy Webinar** on **March 11-12, 2021** at the **SOAS University of London**.

The subject of the conference is: " **The US Security Challenges in the Middle East**"

We host about 50 participants who are political influencers, high profile professors and decision makers all around the world.

The conference registration steps:

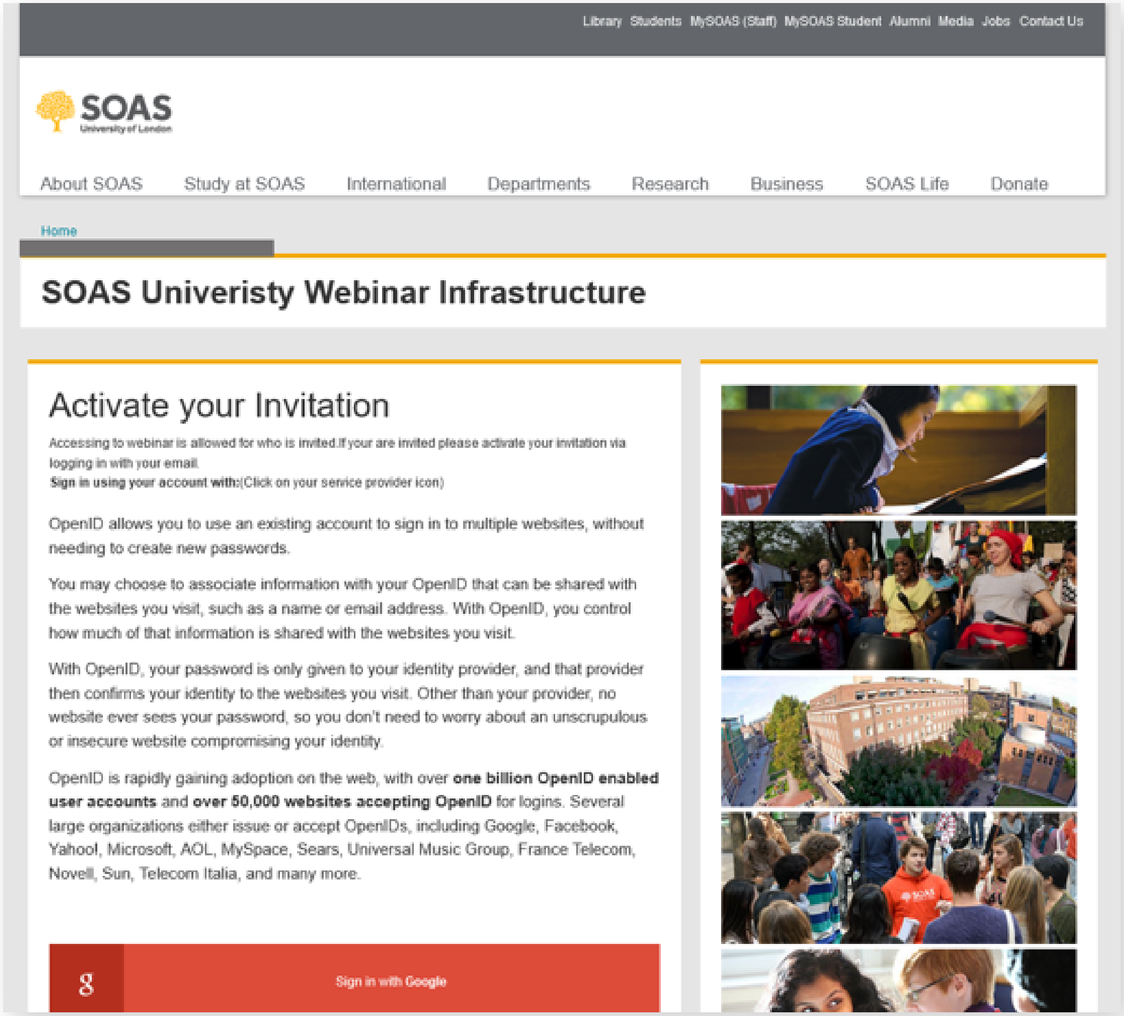
1) Get the registration link
2) Automatic creation of participants' profiles in the SOAS system for further coordination
3) Registering the bank account information of the participants for Honorarium
4) Receiving central topics
5) Coordinating the IT SOAS team to hold a test webinar
6) Holding webinars online
7) Paying honorarium and sending appreciation letters to the participants
8) Membership of participants in specialized working groups for further cooperation if the participants are satisfied

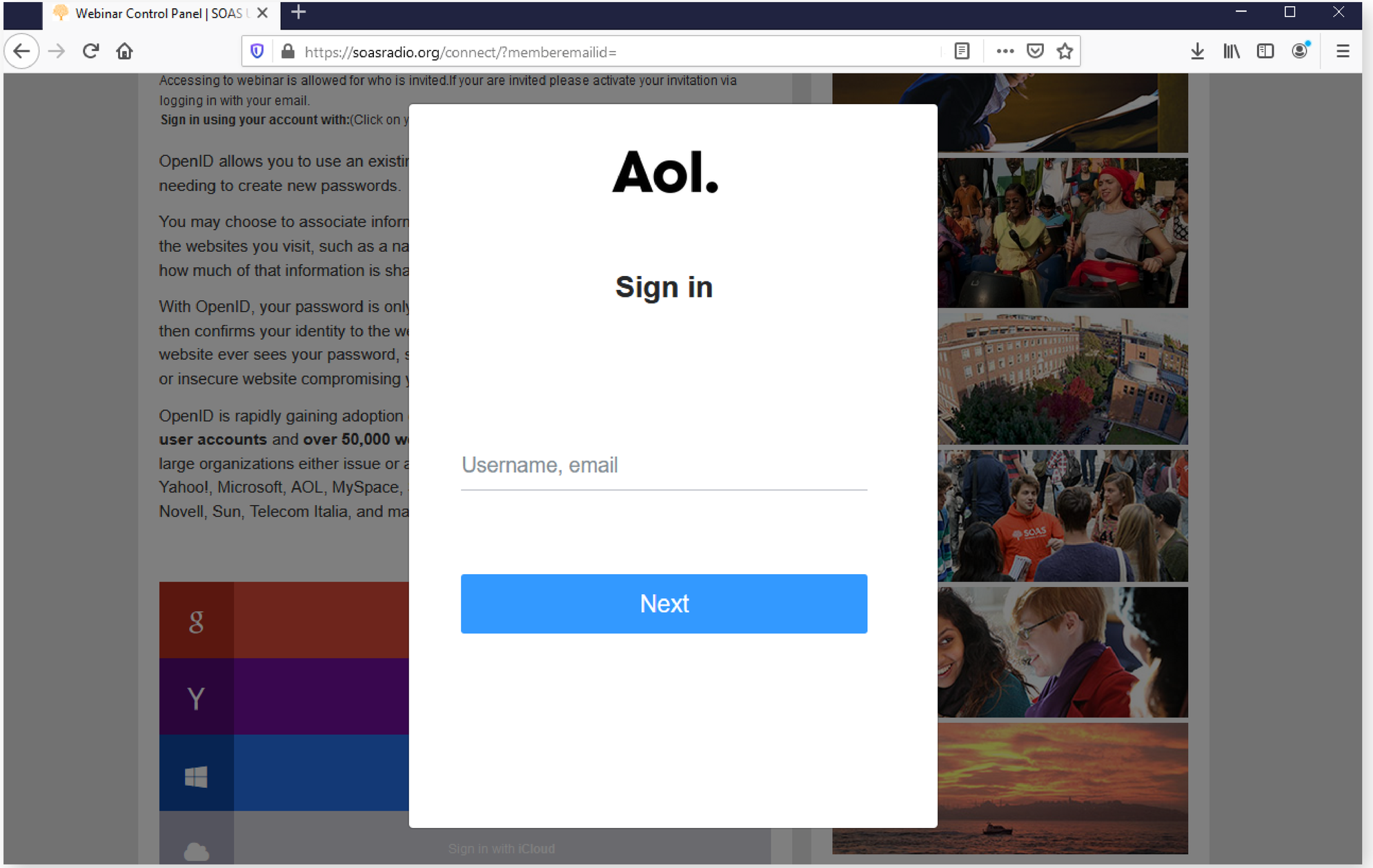
We will keep you updated on the agenda and speakers as they are confirmed. We hope you will forward your personal support to our efforts with CIDS and look forward to receiving your response about completing your registration.

On Behalf of the Organizers,

Dan Plesch

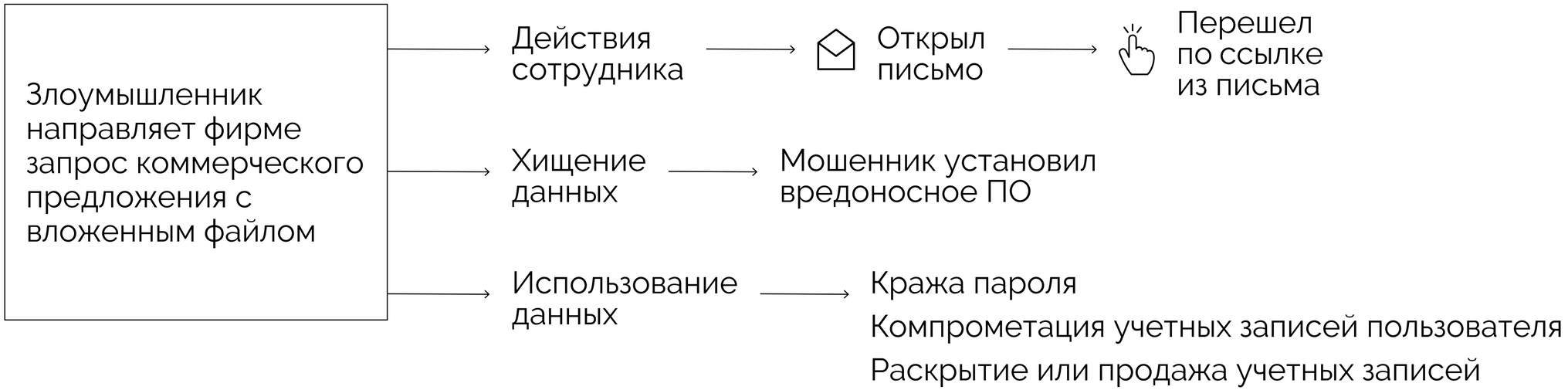
Ссылка вела на «Панель управления вебинаром» на законном, но взломанном веб-сайте, принадлежащем исследовательскому учреждению SOAS Лондонского университета




Webinar Control Panel | SOAS
https://soasradio.org/connect/?memberemailid=
Accessing to webinar is allowed for who is invited.If your are invited please activate your invitation via logging in with your email.
Sign in using your account with:(Click on y
OpenID allows you to use an existi
needing to create new passwords.
You may choose to associate inform
the websites you visit, such as a na
how much of that information is sha
With OpenID, your password is onl
then confirms your identity to the w
website ever sees your password, s
or insecure website compromising y
OpenID is rapidly gaining adoption
user accounts and over 50,000 w
large organizations either issue or a
Yahoo!, Microsoft, AOL, MySpace,
Novell, Sun, Telecom Italia, and ma
Aol.
Sign in
Username, email
Next
Sign in with iCloud

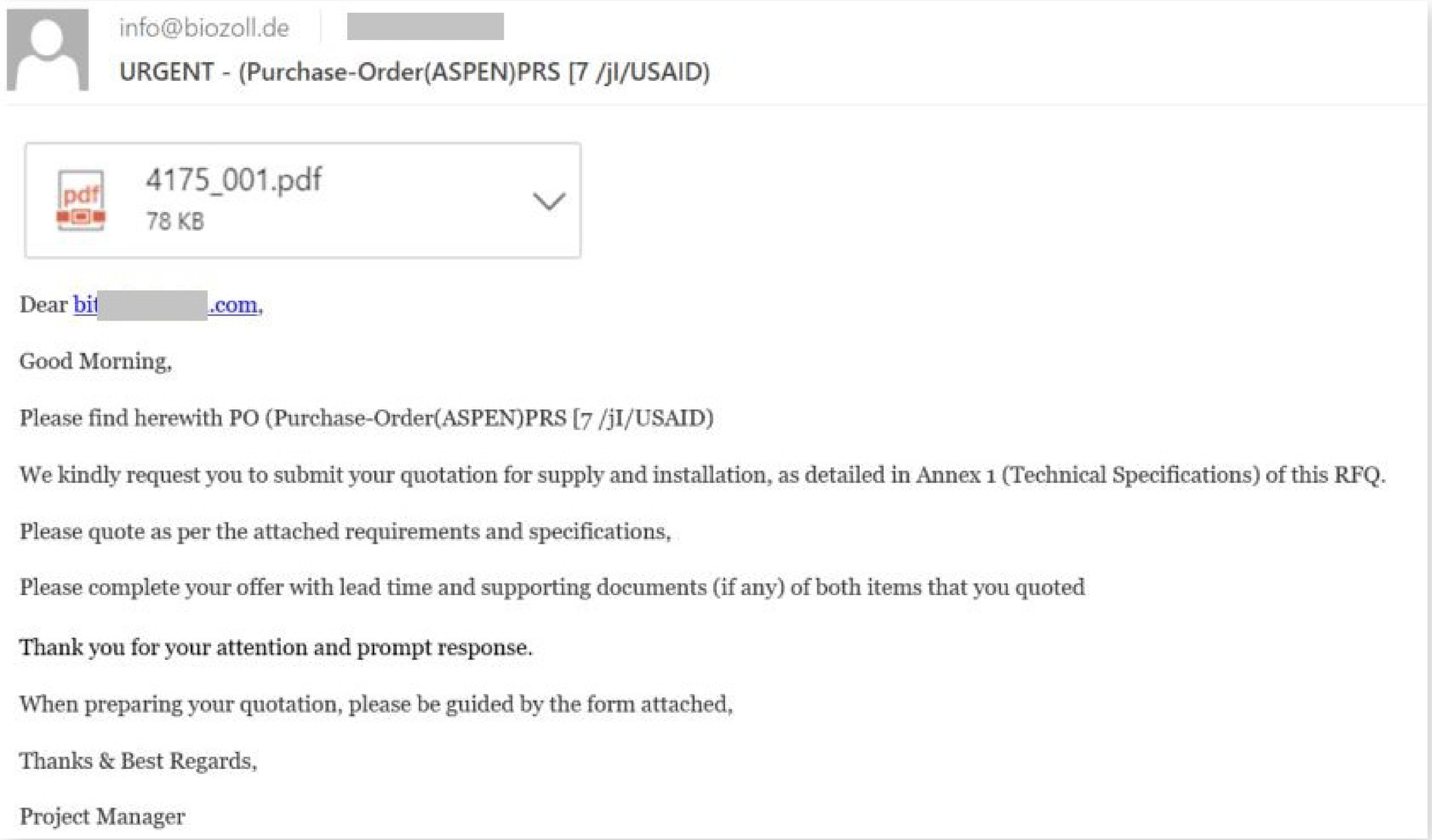
3. Атака с использованием замаскированной ссылки на вредоносную программу

Любопытство | Жадность | Желание помочь | Невнимательность



Злоумышленники прислали фишинговое письмо компании, предоставляющей промышленные услуги и торгующей оборудованием, и запросили коммерческое предложение. В качестве «приложения» получателю был направлен PDF-файл якобы с руководством по составлению такого запроса. Однако вместо прикреплённого файла в письмо была вставлена картинка со ссылкой на вредоносную программу. При нажатии на неё на компьютер жертвы скачивался троян-шпион, способный похищать пароли и другие данные.

Пример письма якобы с вложением



info@biozoll.de

URGENT - (Purchase-Order(ASPEN)PRS [7 /jI/USAID)

4175_001.pdf
78 KB

Dear bi[redacted].com,

Good Morning,

Please find herewith PO (Purchase-Order(ASPEN)PRS [7 /jI/USAID)

We kindly request you to submit your quotation for supply and installation, as detailed in Annex 1 (Technical Specifications) of this RFQ.

Please quote as per the attached requirements and specifications,

Please complete your offer with lead time and supporting documents (if any) of both items that you quoted

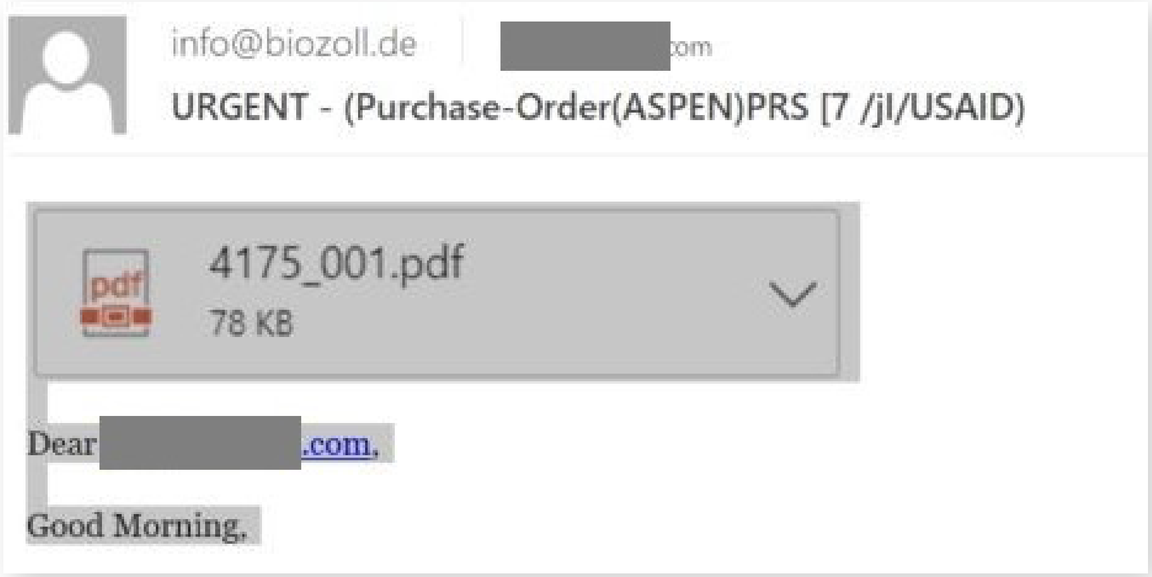
Thank you for your attention and prompt response.

When preparing your quotation, please be guided by the form attached,

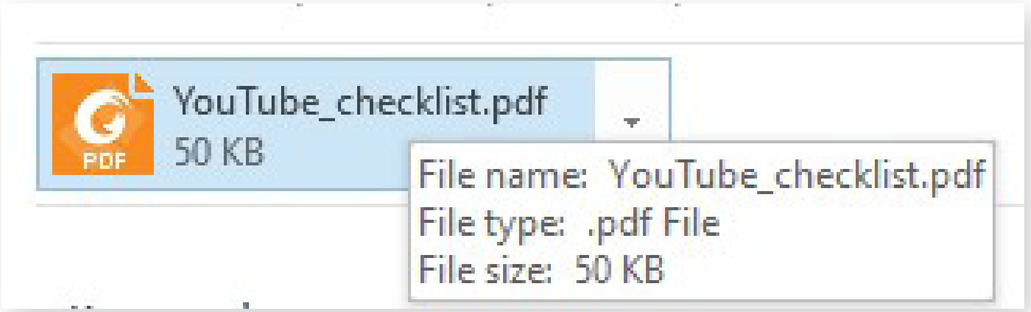
Thanks & Best Regards,

Project Manager

На самом деле это не вложение,
а картинка в теле письма, под которой
находится ссылка для загрузки трояна



Так выглядит настоящее вложение



4. Атака под видом письма от сервиса для электронной подписи

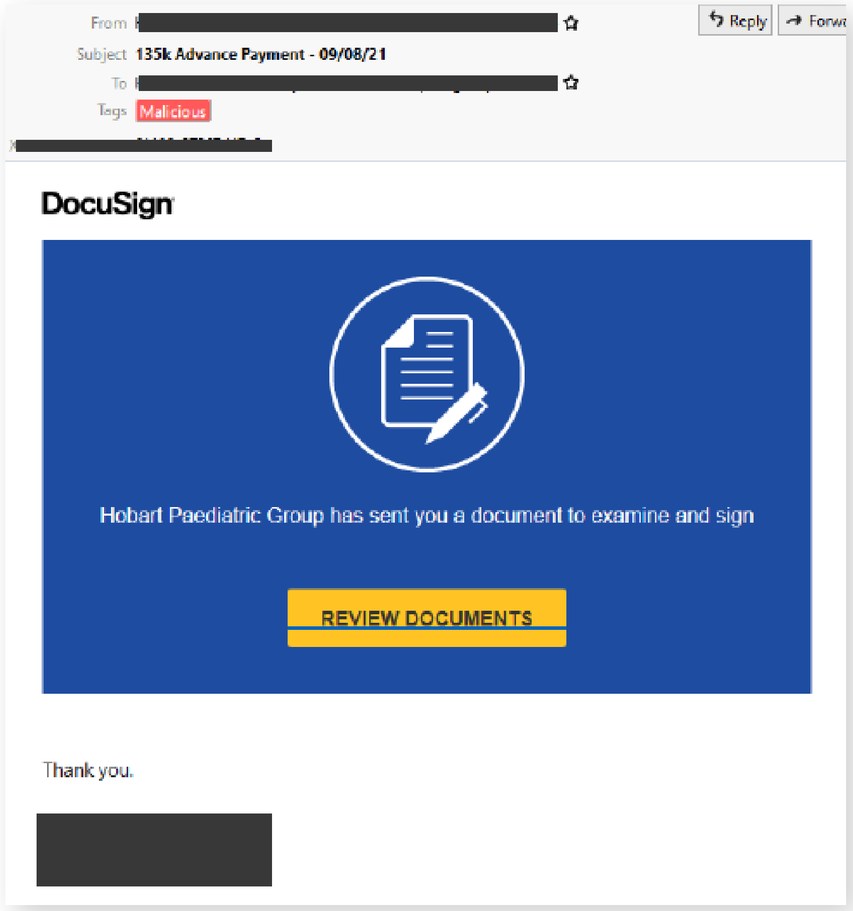
Любопытство | Желание помочь | Невнимательность | Авторитет

Жертве предлагается подписать документ с помощью сервиса электронной подписи

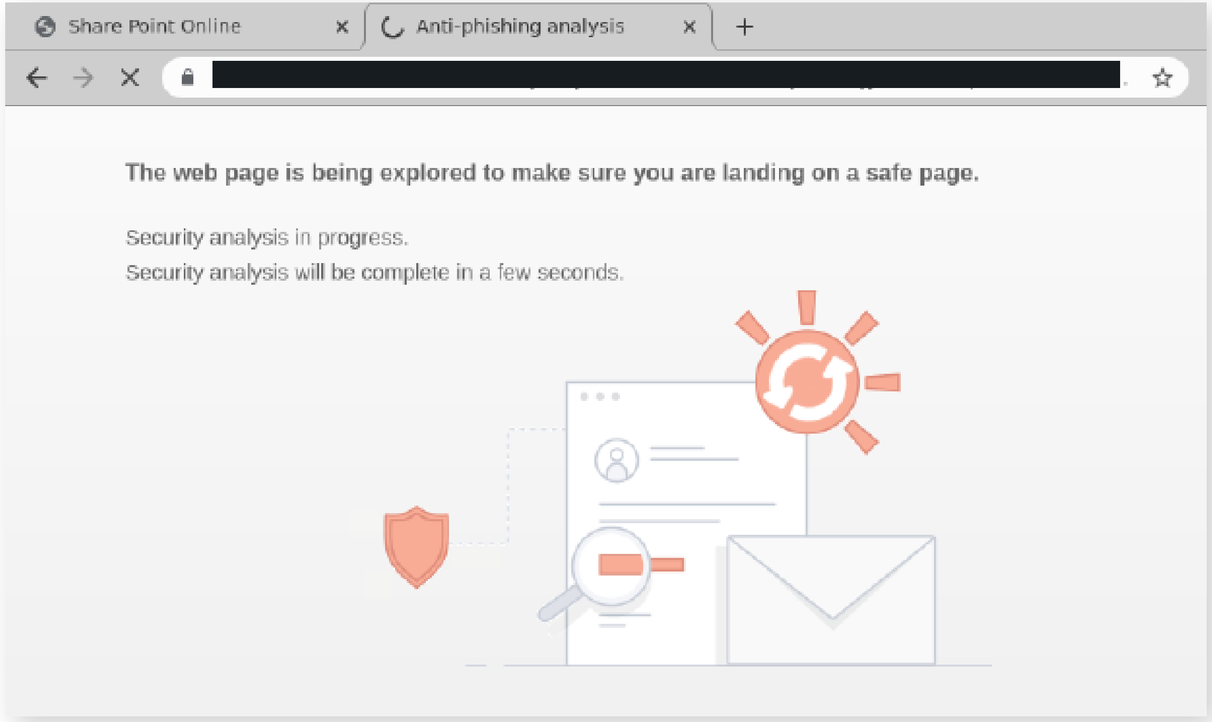
- Действия сотрудника → Открыл письмо → Перешел по ссылке из письма → Ввел данные учетной записи
- Хищение данных → Мошенник получил данные учетной записи электронной почты
- Использование данных →
  - Раскрытие или продажа учетных записей
  - Раскрытие или продажа конфиденциальных данных третьим лицам
  - Возможная организация фишинговых рассылок с этого адреса

В ходе атаки жертвы получали письмо со ссылкой на документ на сервисе DocuSign, который используется сотнями миллионов клиентов как инструмент для электронной подписи. Письма рассылались под видом известного поставщика медицинских услуг. При переходе по ссылке жертва сначала попадала на промежуточную страницу, подражающую известному сервису по проверке на фишинг. На итоговой странице использовались логотипы Adobe и Microsoft. Атака была нацелена на получение адресов электронной почты и логинов жертв, а также потенциально могла быть использована для загрузки вредоносного ПО.

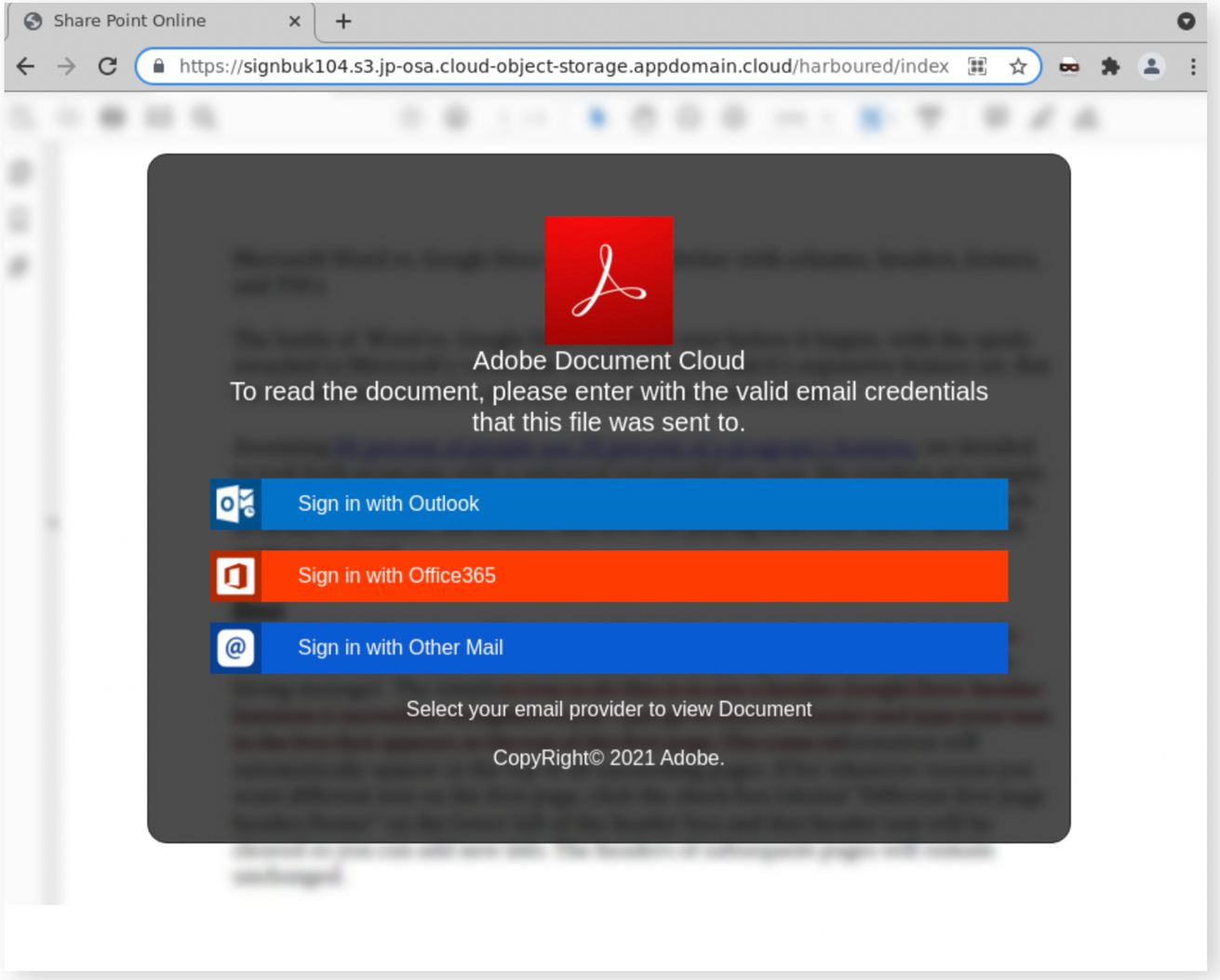
Пример письма

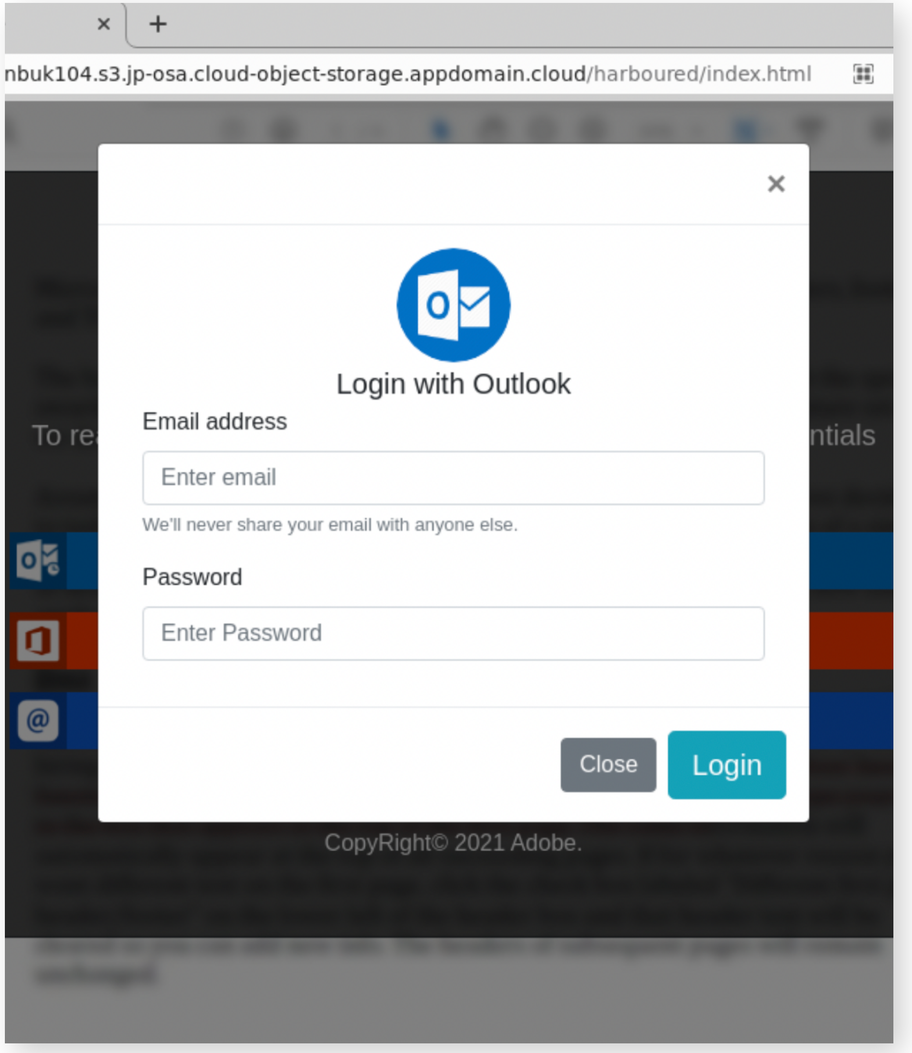


Для отвлечения внимания после перехода по ссылке открывалась промежуточная фишинговая страница, которая копирует известную антифишинговую и имитирует проверку ссылки из письма



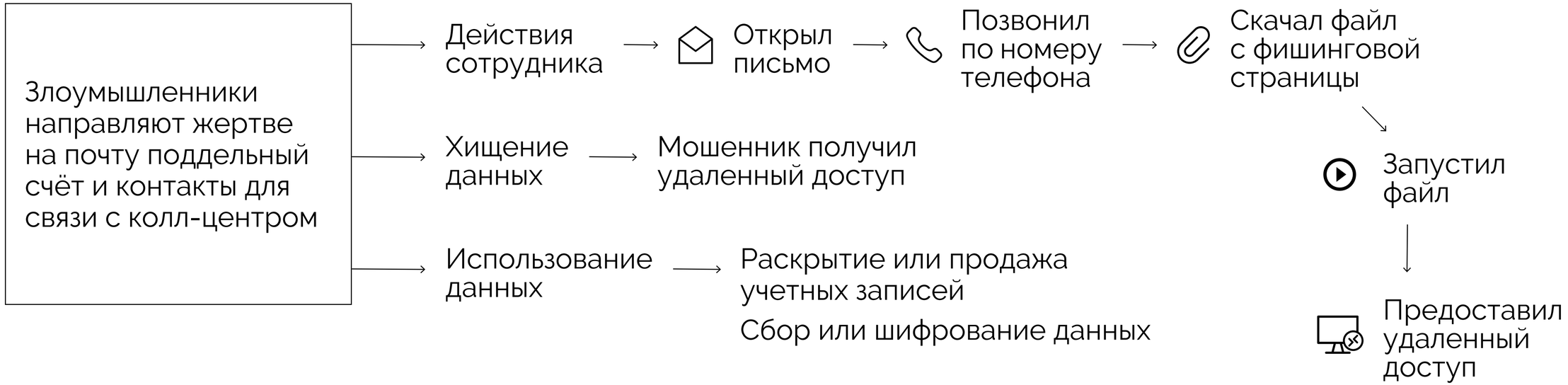
Конечная фишинговая страница





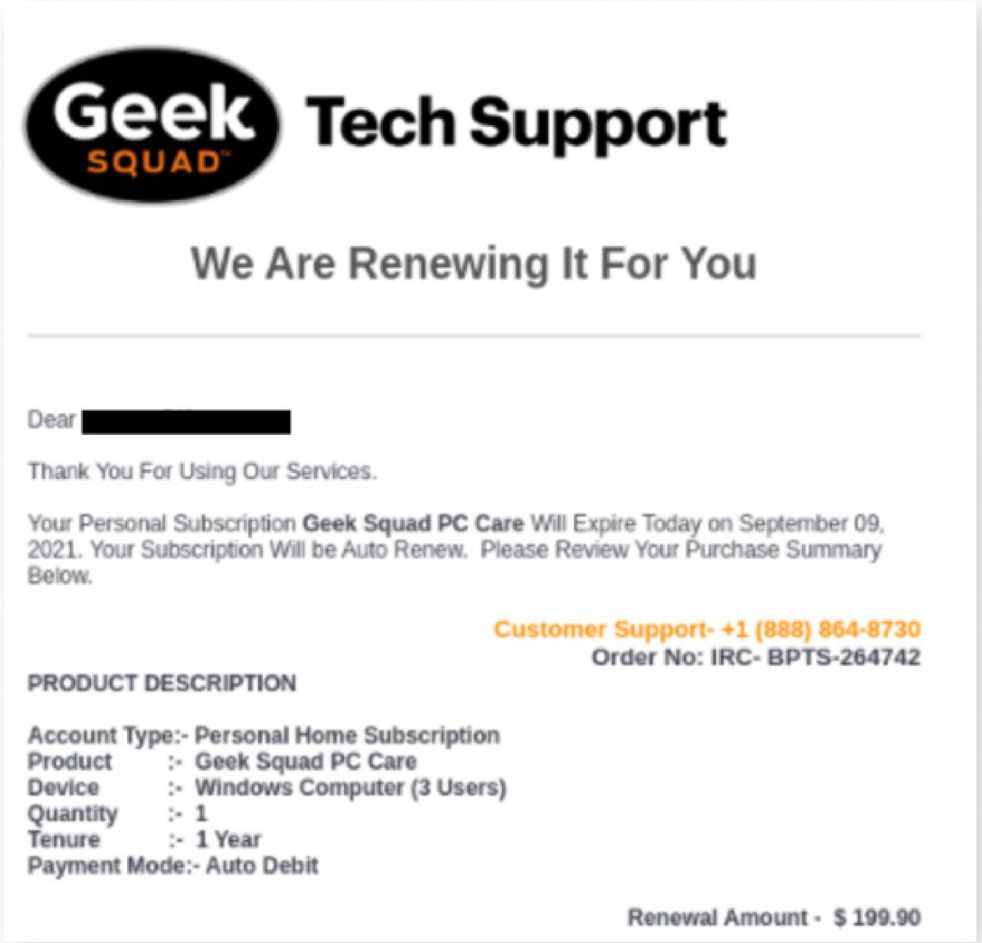
5. Атака фальшивой техподдержки

Раздражение | Страх | Любопытство | Жадность | Авторитет | Срочность



Мошенники, выдавая себя за представителей компании по оказанию компьютерных услуг Geek Squad, убеждали жертв позвонить в «колл-центр» и предоставить удаленный доступ к своим компьютерам. Жертва получала на электронную почту поддельный счет за подписку на несколько сотен долларов. Для отмены платежа предлагалось связаться с «техподдержкой» компании по указанному в письме телефону. Звонок поступал в организованный мошенниками колл-центр. Оператор в ходе беседы просил жертву перейти на поддельный сайт компании и затем скачать программу для удаленного доступа к компьютеру (легитимное ПО TeamViewer). После установки жертве предлагалось сообщить мошенникам пароль, таким образом передавая контроль над компьютером.

Примеры фишинговых писем



Geek SQUAD Tech Support

We Are Renewing It For You

Dear [redacted]

Thank You For Using Our Services.

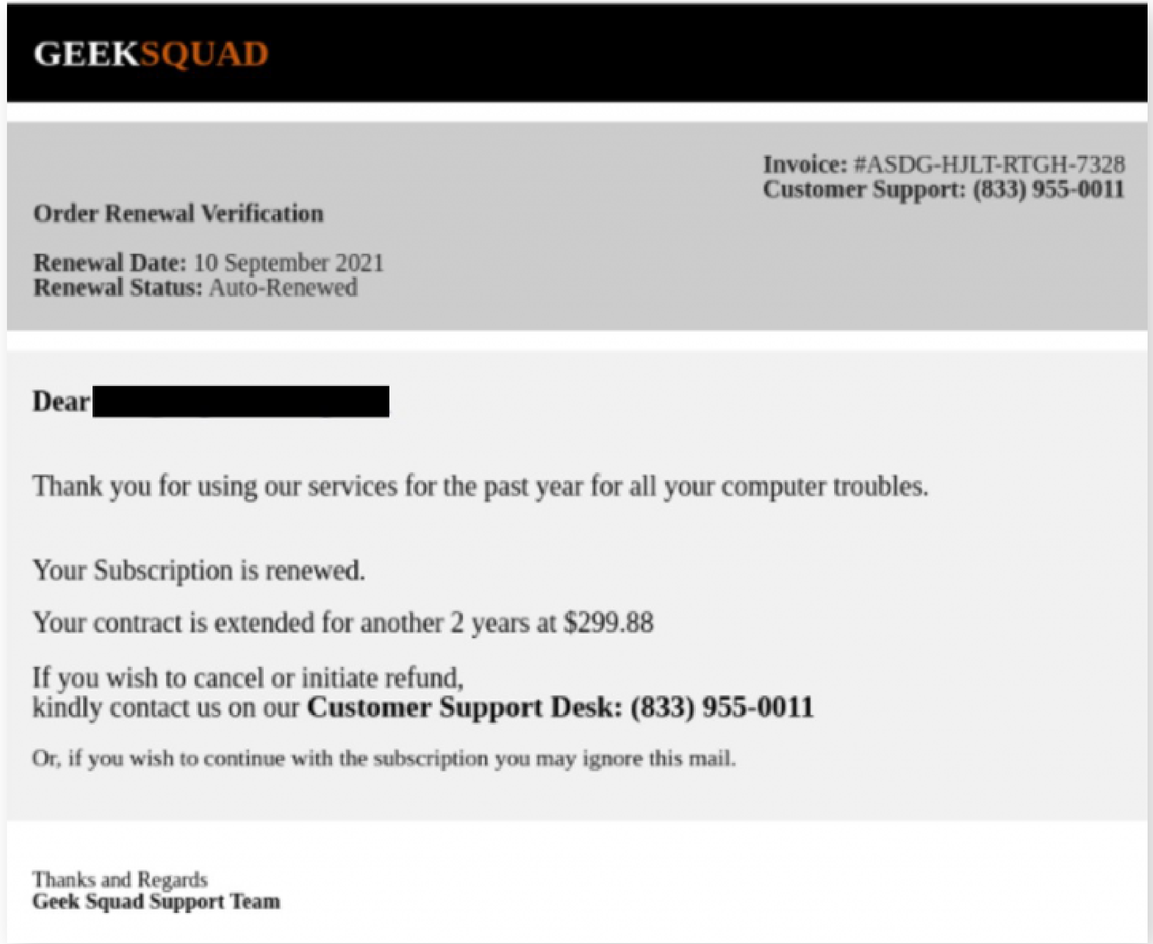
Your Personal Subscription **Geek Squad PC Care** Will Expire Today on September 09, 2021. Your Subscription Will be Auto Renew. Please Review Your Purchase Summary Below.

Customer Support- +1 (888) 864-8730
Order No: IRC- BPTS-264742

PRODUCT DESCRIPTION

Account Type:- Personal Home Subscription
Product :- Geek Squad PC Care
Device :- Windows Computer (3 Users)
Quantity :- 1
Tenure :- 1 Year
Payment Mode:- Auto Debit

Renewal Amount - $ 199.90



GEEKSQUAD

Invoice: #ASDG-HJLT-RTGH-7328
Customer Support: (833) 955-0011

Order Renewal Verification

Renewal Date: 10 September 2021
Renewal Status: Auto-Renewed

Dear [redacted]

Thank you for using our services for the past year for all your computer troubles.

Your Subscription is renewed.

Your contract is extended for another 2 years at $299.88

If you wish to cancel or initiate refund,
kindly contact us on our **Customer Support Desk: (833) 955-0011**

Or, if you wish to continue with the subscription you may ignore this mail.

Thanks and Regards
Geek Squad Support Team

Примеры фишинговых писем

GeekSquad

Payment receipt

Manage payment

You paid $359.56

to Geek SQUAD-Solutions (800) 890-9249 on September 09, 2021

Payment details

Invoice-no.	358218
Invoice amount	$359.56
Total amount	$359.56
Payment method	Online
Authorization ID	GYB02DT6119

Thank you,

Geek SQUAD-Solutions

(800) 890-9249

Hello Customer ,

Thank You for your payment. Your account has been debited with $398.49 for the Auto Renewable plan of your McAfee family. The charges might reflect within a few moments to 24 hours. For any query or assistance please reach out to us @ **+1 (918) 467-5100 / +1 (918) 467-5100.**

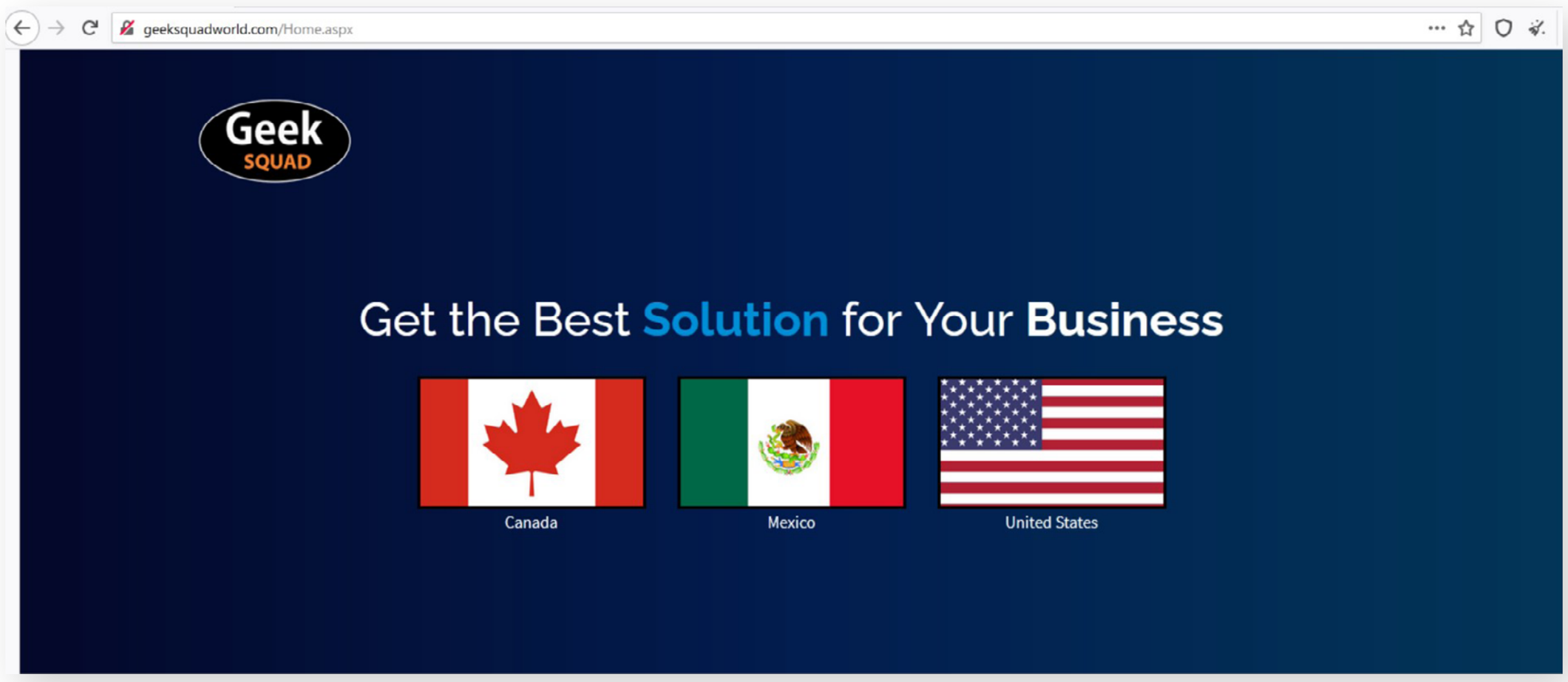
Invoice Number – UGDEZQ675

Product	Issue Date	Expiration Date	Qty	Amount
McAfee Security 360 Plan	Sep, 14, 2021	Sep, 13, 2026	1	$398.49

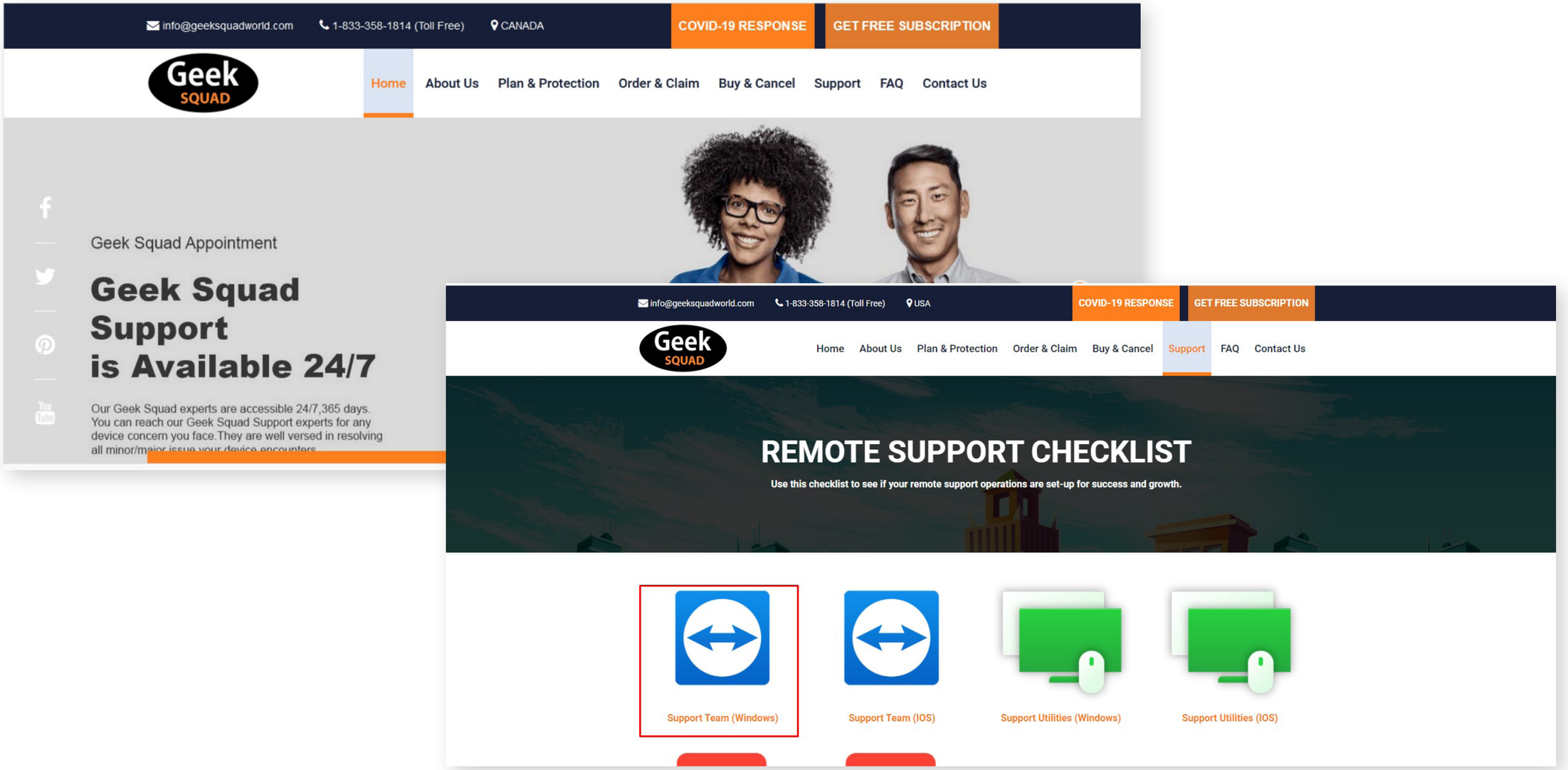
PC Solution

We are an associate of the Geek Squad.

Оператор колл-центра предложил перейти на сайт https://geekaquadworld.com/ для отмены подписки



Мошенники просят скачать и установить TeamViewer и сообщить данные для ввода



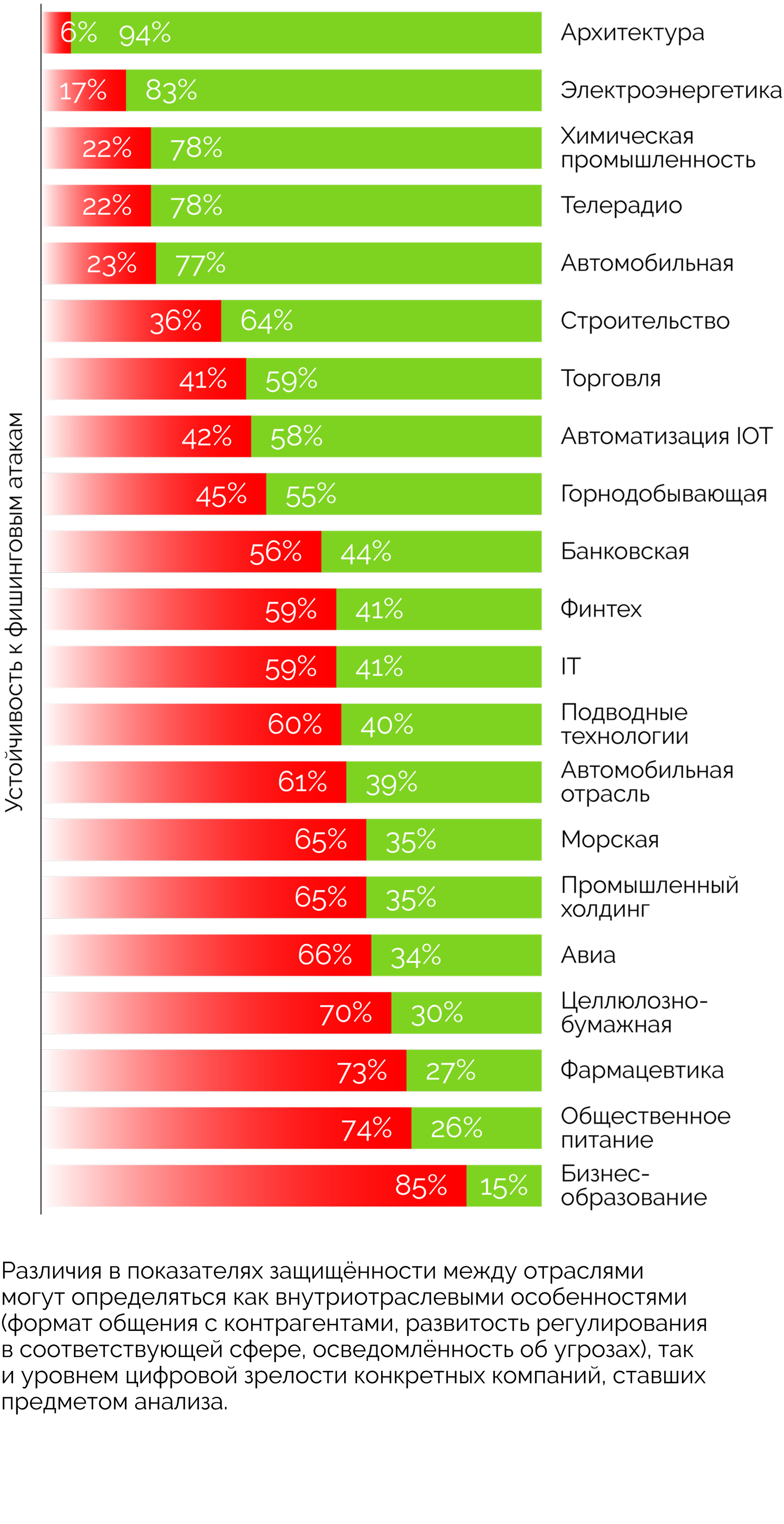
3 Общая статистика защищенности сотрудников

Зависимость защищенности сотрудников от отраслей, подразделений и ролей в компании.

Общая статистика защищенности сотрудников

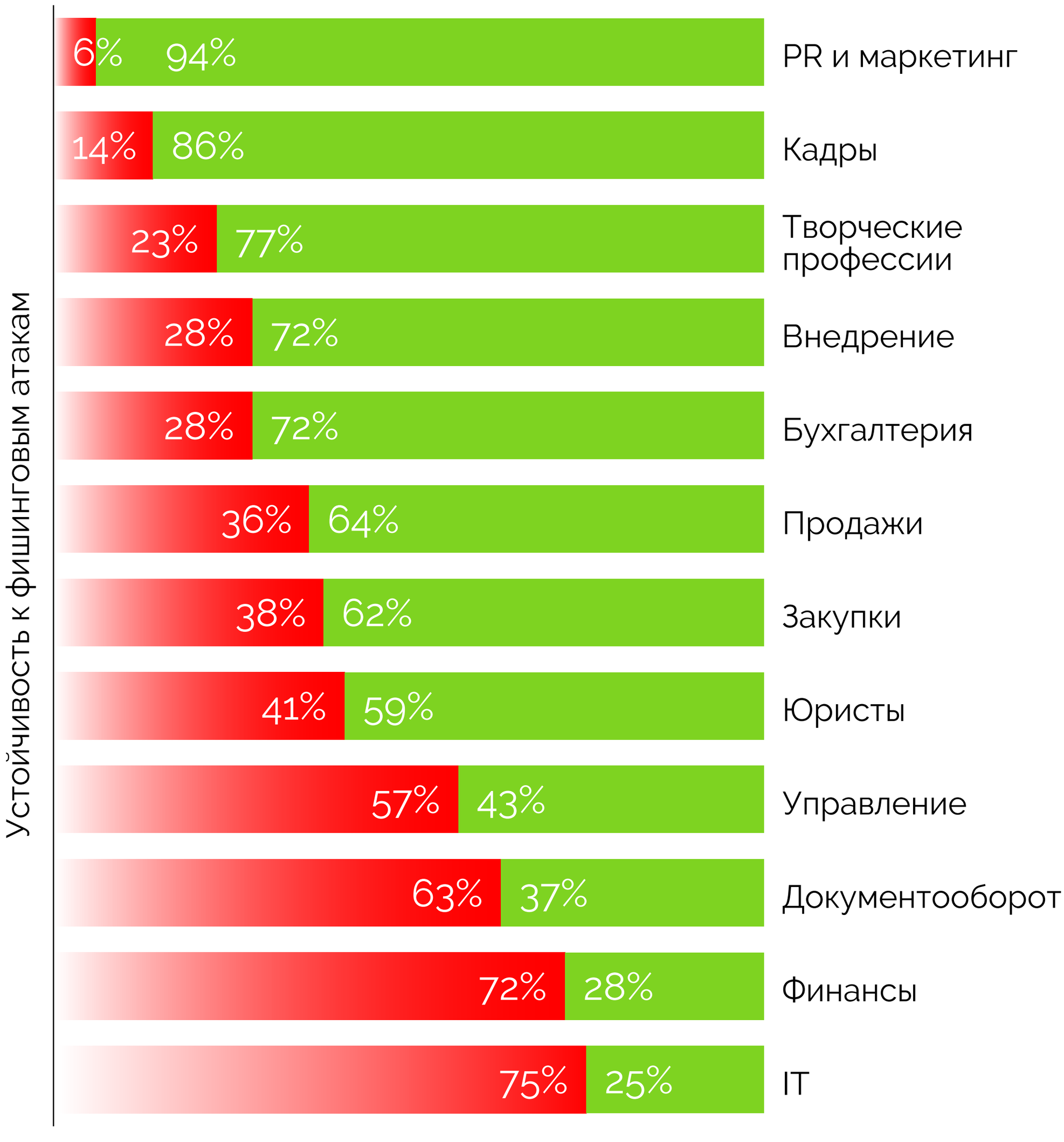
* Динамика указана в сравнении с 2020 годом

Общая статистика по отраслям



Различия в показателях защищённости между отраслями могут определяться как внутриотраслевыми особенностями (формат общения с контрагентами, развитость регулирования в соответствующей сфере, осведомлённость об угрозах), так и уровнем цифровой зрелости конкретных компаний, ставших предметом анализа.

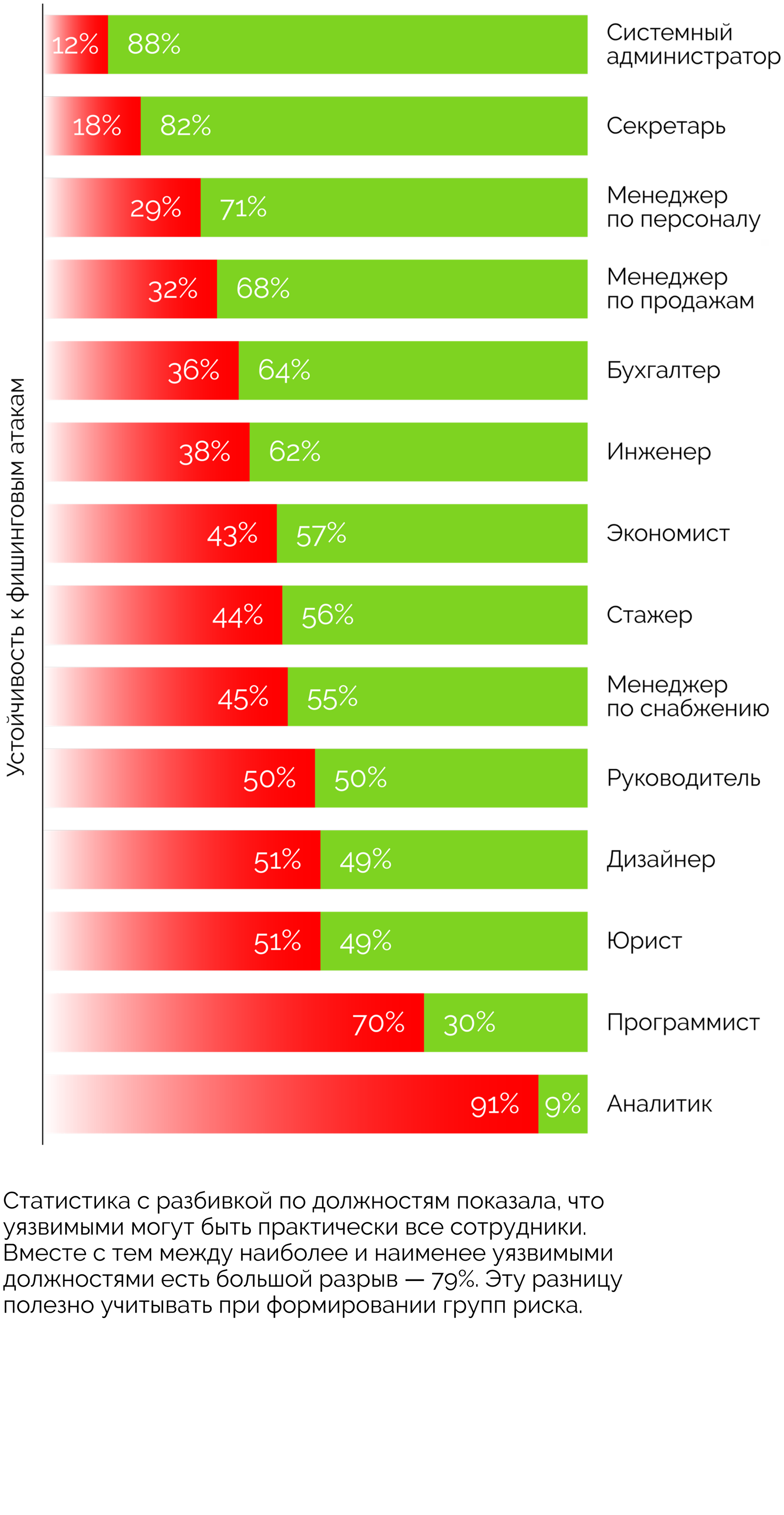
Общая статистика по подразделениям



Уязвимость перед фишингом может быть связана не только с недостаточной подготовленностью сотрудников, но также и со слабостями на уровне бизнес-процессов внутри организации и её отделов. Это зависит от инструментов и форматов внутренней и внешней коммуникации, использования программного обеспечения и интернет-сервисов, формальных и неформальных инструкций и других особенностей работы в командах.

Оценка степени уязвимости подразделений позволяет выявить слабые места организации. Однако этот показатель не стоит автоматически переносить на всех сотрудников конкретного подразделения, поскольку между ними может быть много индивидуальных различий. Также статистика не является универсальной и может варьироваться в разных организациях.

Общая статистика по должностям



Статистика с разбивкой по должностям показала, что уязвимыми могут быть практически все сотрудники. Вместе с тем между наиболее и наименее уязвимыми должностями есть большой разрыв — 79%. Эту разницу полезно учитывать при формировании групп риска.

4 Технические векторы атак

Каналы, по которым доставлялись реальные атаки в 2021 году

Согласно нашим исследованиям, в 2021 году основным каналом доставки фишинговых атак являлась электронная почта — на нее приходилось 96% случаев. В качестве других каналов использовались телефонные звонки, сообщения в мессенджерах и социальных сетях, однако чаще всего они выступали как второстепенные средства связи. В наиболее сложных атаках были задействованы сразу несколько каналов связи.

Популярность атак через электронную почту делает защиту от них приоритетной задачей.

* Данные из разбора 100 цифровых атак на компании за 2021 год.

Пример атаки с использованием нескольких каналов связи

Использование нескольких каналов может быть направлено на усиление атаки и дополнительное побуждение получателей к небезопасным действиям. Так, в ходе фишинговой кампании группировка Lazarus рассылала документы с вредоносным макросом через LinkedIn, Telegram, WhatsApp и корпоративную почту. В одном случае злоумышленники сначала связались с жертвой через LinkedIn, а затем направили на электронную почту письмо с предложением о работе от имени известной компании.

Шаг 1: Злоумышленники присылают сотрудникам вредоносные файлы с поддельным описанием вакансии. Файл может быть направлен как по электронной почте, так и в мессенджере. Заразив компьютеры жертв, злоумышленники собирают дополнительную информацию о компании.

Шаг 2. С помощью собранной информации злоумышленники расширяют поверхность атаки и связываются с другими сотрудниками компании. Разные каналы связи дополняют друг друга: после представления в LinkedIn злоумышленник направляет сотруднику электронное письмо с вредоносным файлом, а также продолжает общение в Telegram.

Senior Business Manager

Job Location: Washington, DC
Employment Type: Full Time
Clearance Level Must Currently Possess: None
Clearance Level Must Be Able to Obtain: None
Telecommuting Options: Some Telecommuting Allowed
Annual Salary: $72k - $120k

Job Description:

General Dynamics Mission Systems (GDMS) engineers a diverse portfolio of high technology solutions, products and services that enable customers to successfully execute missions across all domains of operation.

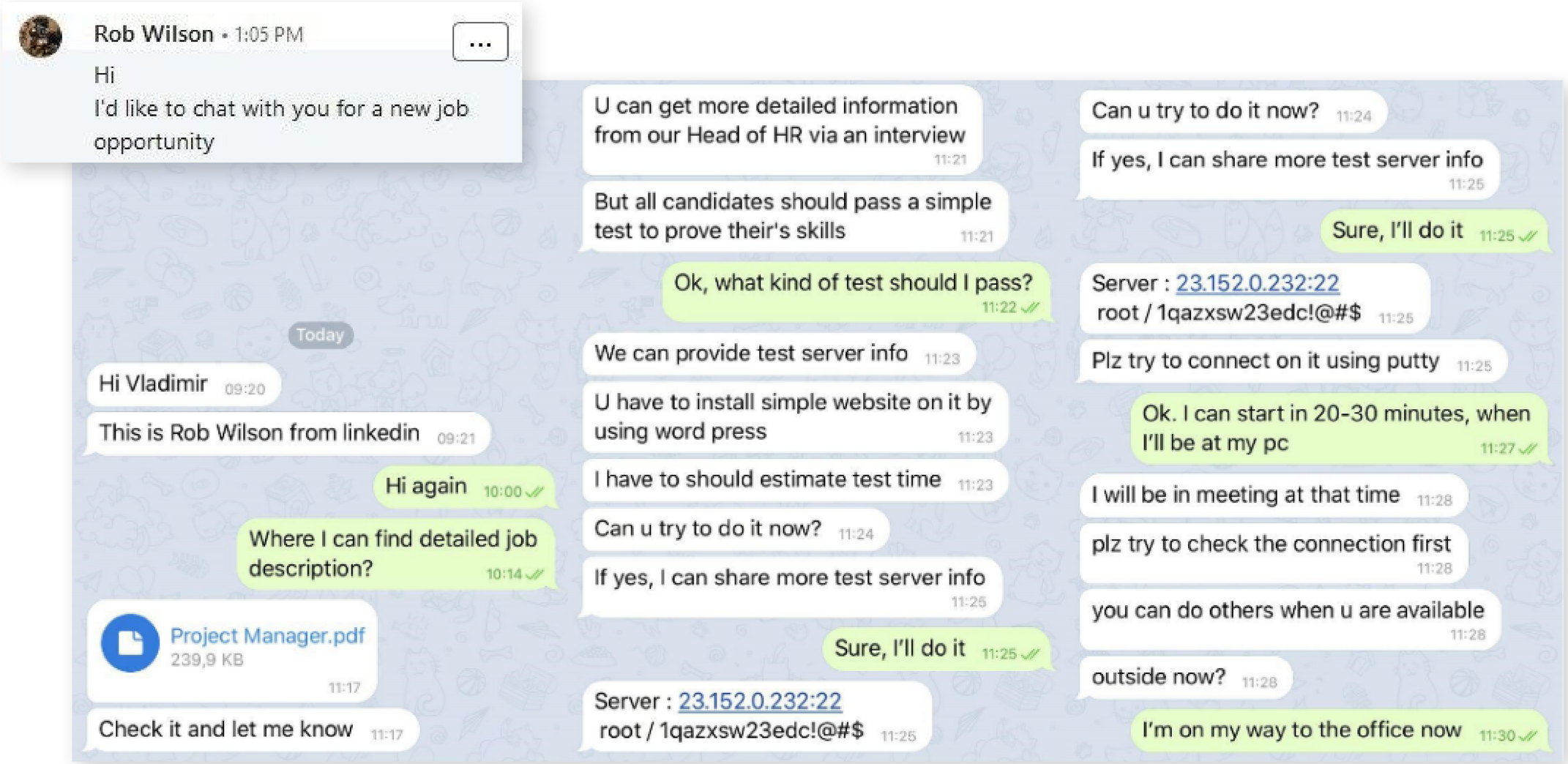
With a global team of 13,000+ top professionals, we partner with the best in industry to expand the bounds of innovation in the defense and scientific arenas.

Given the nature of our work and who we are, we value trust, honesty, alignment and transparency. We offer highly competitive benefits and pride ourselves in being a great place to work with a shared sense of purpose.

You will also enjoy a flexible work environment where contributions are recognized and rewarded. If who we are and what we do resonates with you, we invite you to join our high performance team!

Responsibilities:

Bachelor's degree in Senior Business Manager or a related specialized area or the equivalent experience is required plus a minimum of 10 years of relevant experience; or Master's degree

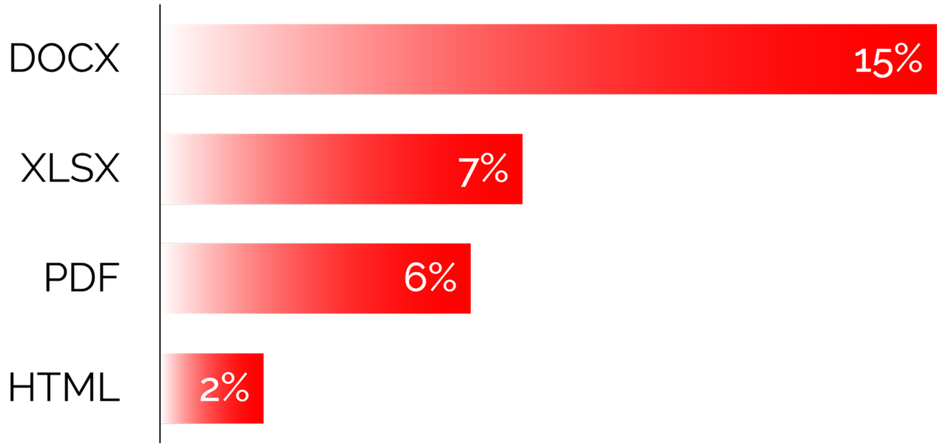

Rob Wilson • 1:05 PM
Hi
I'd like to chat with you for a new job opportunity
Today
Hi Vladimir 09:20
This is Rob Wilson from linkedin 09:21
Hi again 10:00
Where I can find detailed job description? 10:14
Project Manager.pdf
239,9 KB
11:17
Check it and let me know 11:17
U can get more detailed information from our Head of HR via an interview 11:21
But all candidates should pass a simple test to prove their's skills 11:21
Ok, what kind of test should I pass? 11:22
We can provide test server info 11:23
U have to install simple website on it by using word press 11:23
I have to should estimate test time 11:23
Can u try to do it now? 11:24
If yes, I can share more test server info 11:25
Sure, I'll do it 11:25
Server : 23.152.0.232:22
root / 1qazxsw23edc!@#$ 11:25
Can u try to do it now? 11:24
If yes, I can share more test server info 11:25
Sure, I'll do it 11:25
Server : 23.152.0.232:22
root / 1qazxsw23edc!@#$ 11:25
Plz try to connect on it using putty 11:25
Ok. I can start in 20-30 minutes, when I'll be at my pc 11:27
I will be in meeting at that time 11:28
plz try to check the connection first 11:28
you can do others when u are available 11:28
outside now? 11:28
I'm on my way to the office now 11:30

Действия сотрудников с разными типами вложений

DOCX

15%

Вложения, которые чаще всего открывали сотрудники в имитированных фишинговых атаках, — это файлы с расширением docx.



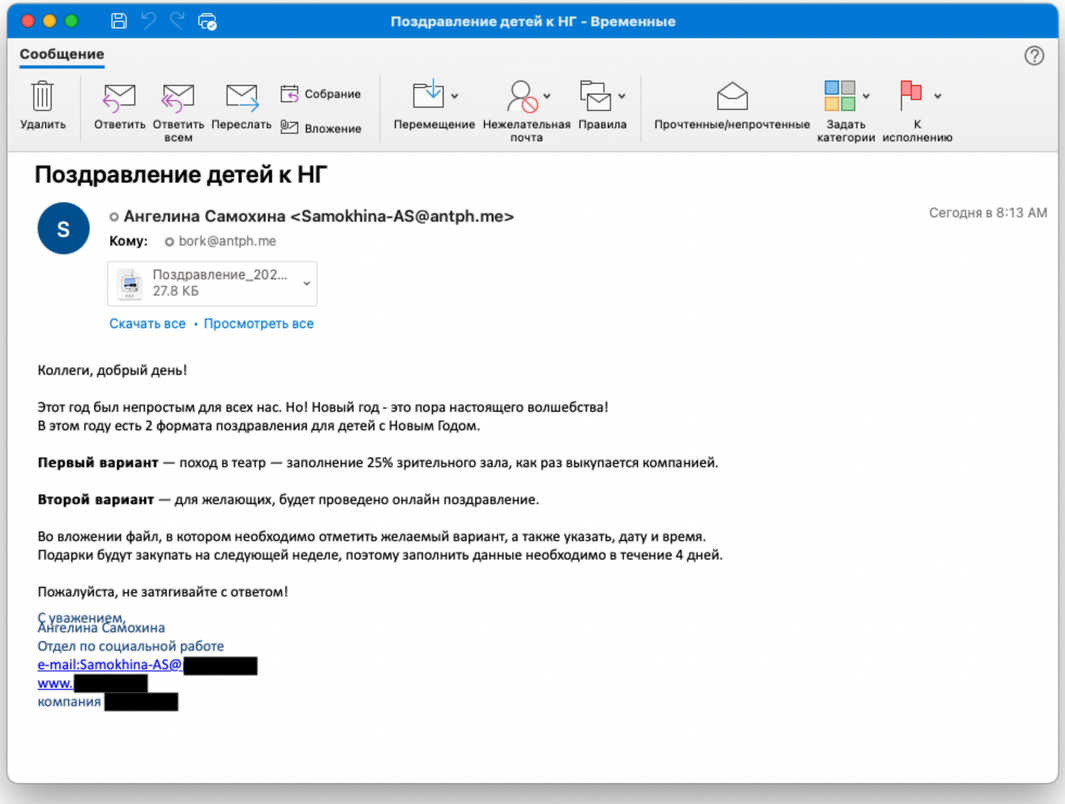
Использование при тренировке документов этого и других популярных у злоумышленников форматов помогает отрабатывать навыки на ситуациях, с которыми сотрудники могут столкнуться в реальности.

Один из приёмов, применявшихся специалистами Антифишинга и увеличивших количество небезопасных действий с документами форматов docx и xlsx, — побуждение исправить ошибку. В тексте письма получателю в максимально нейтральной форме предлагается проверить данные во вложенном файле. Внутри документа нарочно допущена ошибка, что подталкивает сотрудника нажать на кнопку «Разрешить редактирование» и тем самым запустить вредоносную программу.

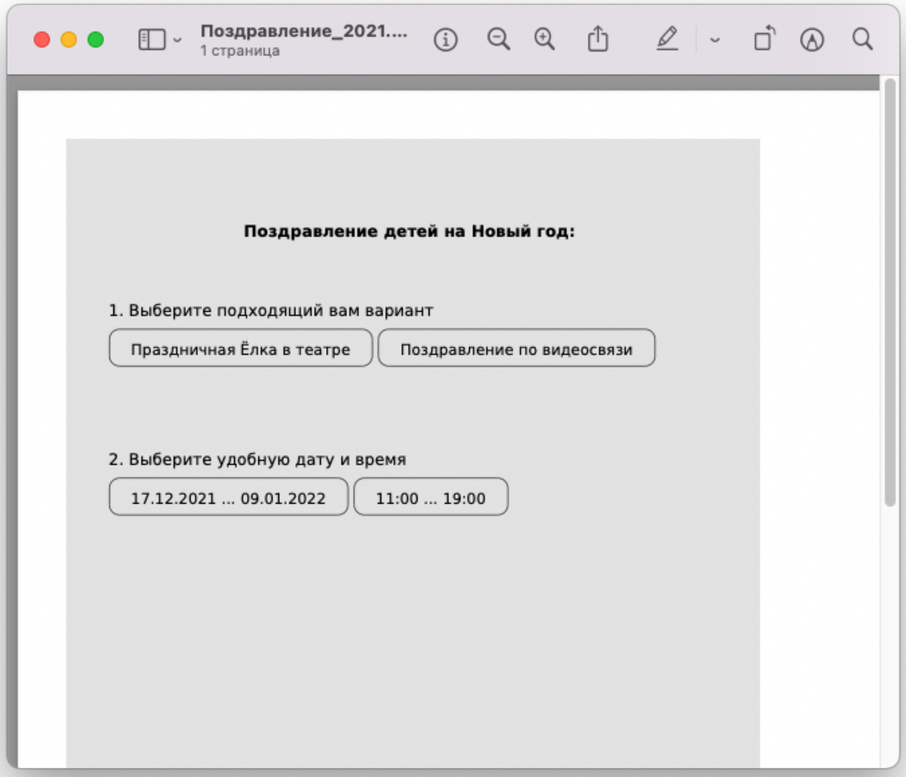
Высокий показатель небезопасных действий с такими вложениями показывает, что доверие к файлу во многом зависит не от его типа, а от содержимого письма, способности злоумышленников усыпить бдительность получателя.

Пример имитированной атаки с вложенным файлом Microsoft Office Word

Сотрудник получает рассылку от имени коллеги с просьбой в ближайшее время выбрать формат поздравления его детей.



При попытке заполнить вложенный документ сотрудник запустит загрузку вредоносного файла на свой компьютер.



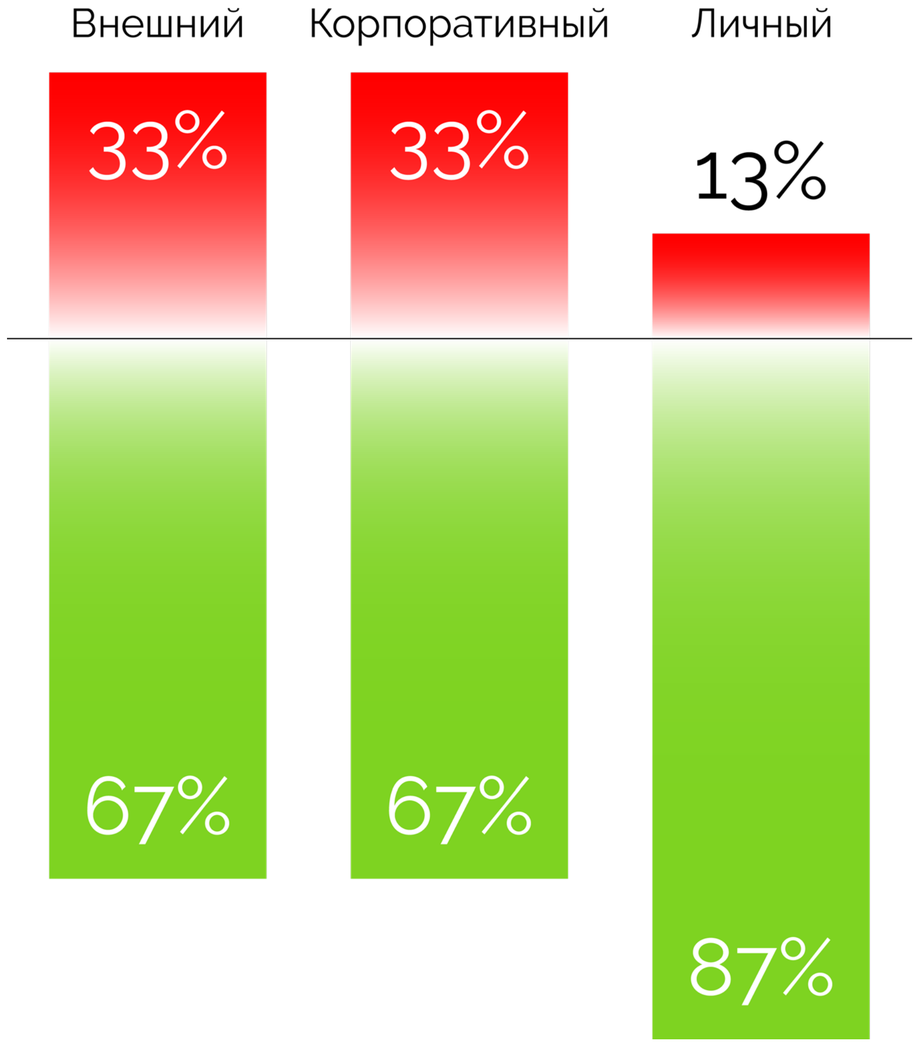
5 Психологические векторы атак

Эксперты Антифишинга развивают собственную классификацию цифровых атак на сотрудников, в основе которой – влияние психологических векторов атак на действия людей. Она описывает эмоции и другие приемы социальной инженерии, которые используют мошенники в реальных атаках.

Влияние источника атаки на её эффективность

Мы использовали классификацию, чтобы сравнить разные психологические векторы в имитированных атаках за 2021 год и выявить те, которые наиболее эффективно побудили получателей совершить небезопасные действия. Процентное значение обозначает долю от общего количества успешных атак, в которых использовалась та или иная эмоция, или усилитель.

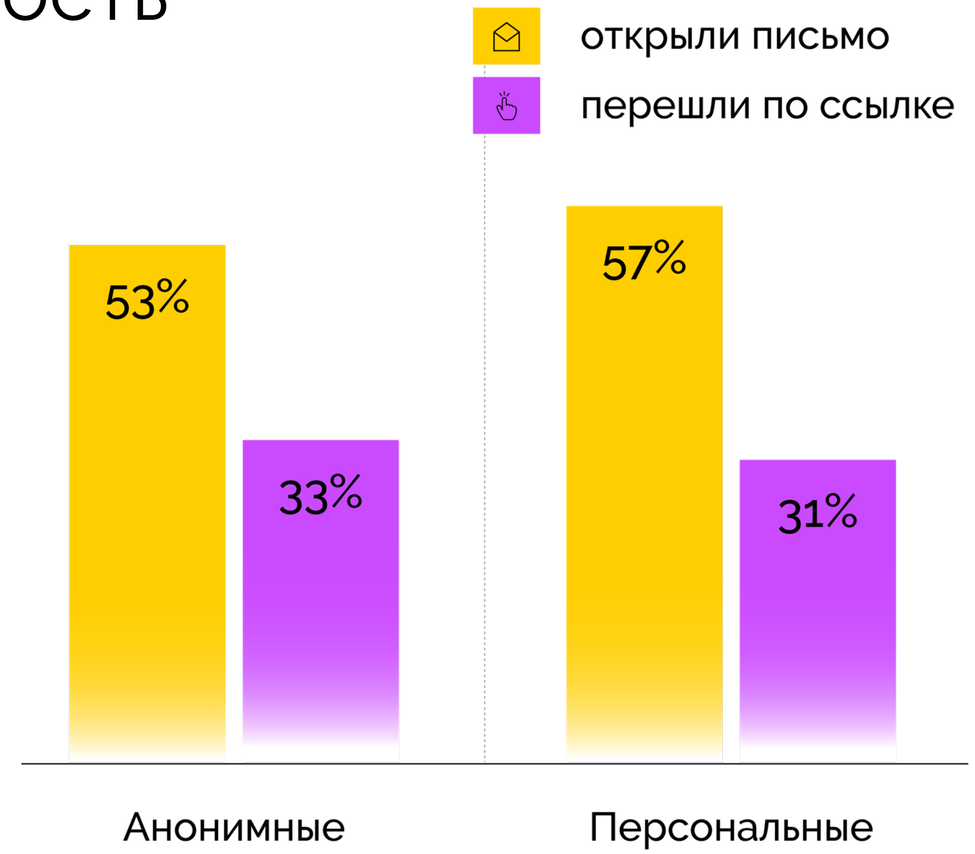
Атаки, проводившиеся от внешнего и корпоративного источника, оказались более эффективными с точки зрения побуждения получателей к небезопасным действиям, чем личные письма. При этом заметной разницы в эффективности между корпоративными и внешними атаками не выявлено.



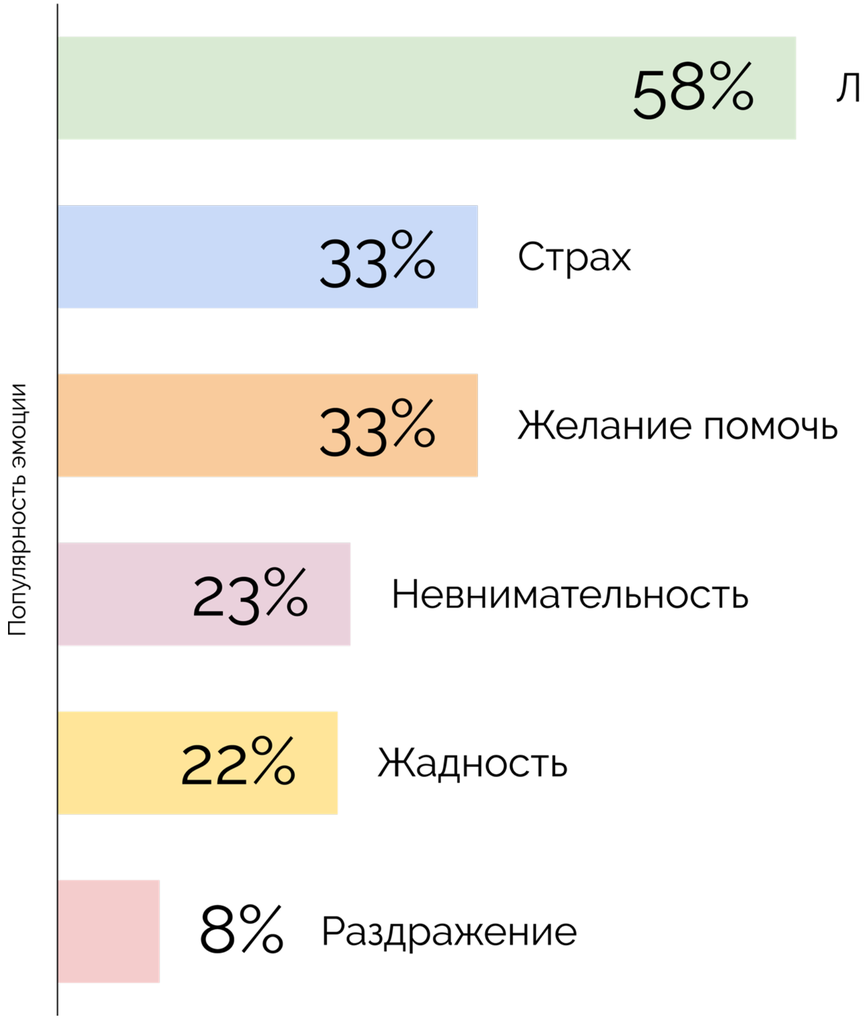
Эффективность атаки не обязательно зависит от источника. Если речь идёт о целевой атаке, содержание письма так или иначе будет адаптировано под получателя и будет выглядеть значительно более правдоподобно, чем массовая рассылка. В имитированных атаках специалисты Антифишинга составляют шаблоны писем под конкретную организацию с учётом информации о клиенте, собранной из открытых источников.

Влияние персонификации атаки на ее эффективность

Персонифицированные атаки представляли наибольшую опасность для сотрудников по сравнению с анонимными, однако разница между ними оказалась незначительной. Письма, в которых использовалось личное обращение, побудили получателей к небезопасным действиям в 57% случаев, а не содержащие имени — в 53%.



Влияние эмоций в атаке



Мы выявили, что наиболее часто встречающийся психологический вектор в успешных имитированных атаках — любопытство. 58% писем, побудивших сотрудников в небезопасным действиям, вызывали эту эмоцию. Соответственно, любопытство чаще других эмоций использовалось в связке с другими векторами.

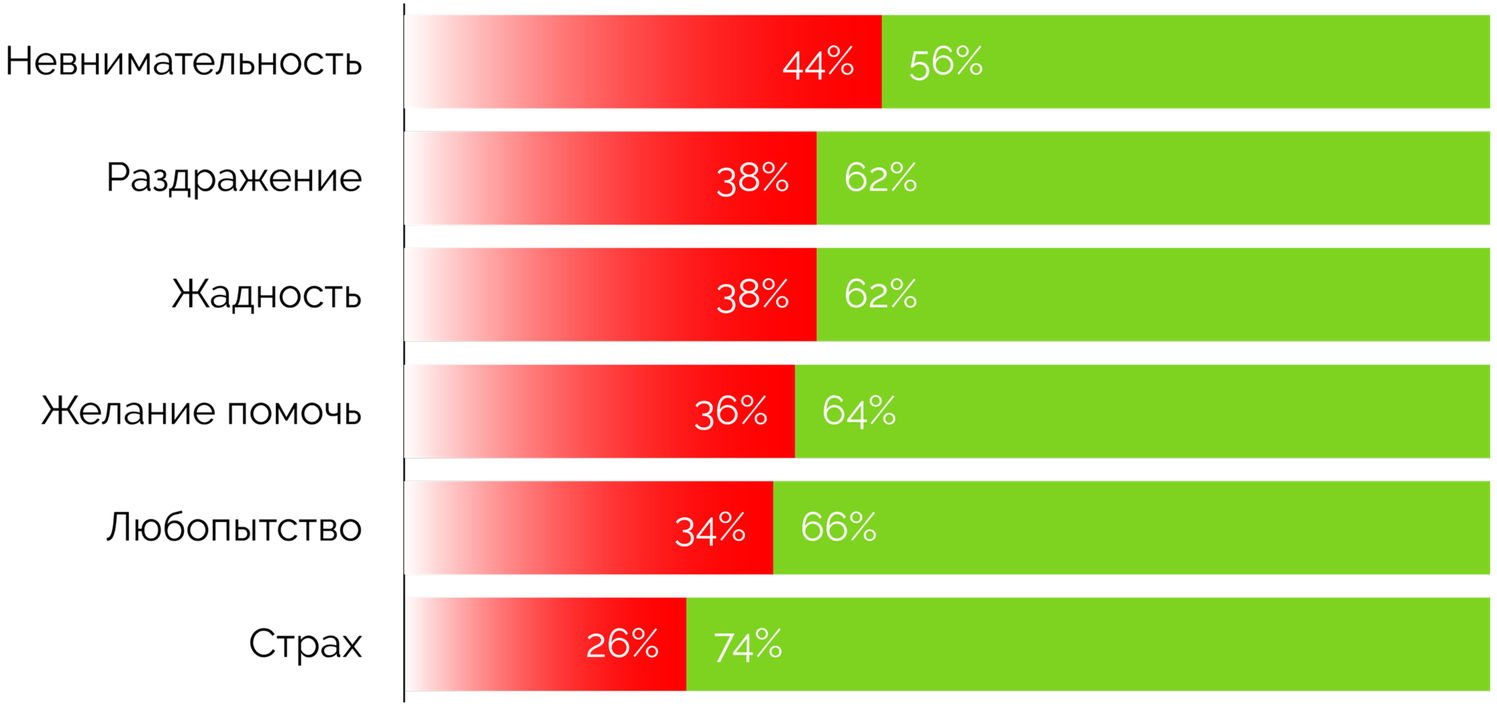
Любопытство в данном случае — это когнитивное искажение, которое можно охарактеризовать как ощущение упущенной выгоды. Получив письмо, сотрудник думает: «Если я сейчас не отреагирую, я что-то потеряю». При этом речь может идти не только о материальной потере, но и об упущенной ценной информации.

Эффективность психологических векторов

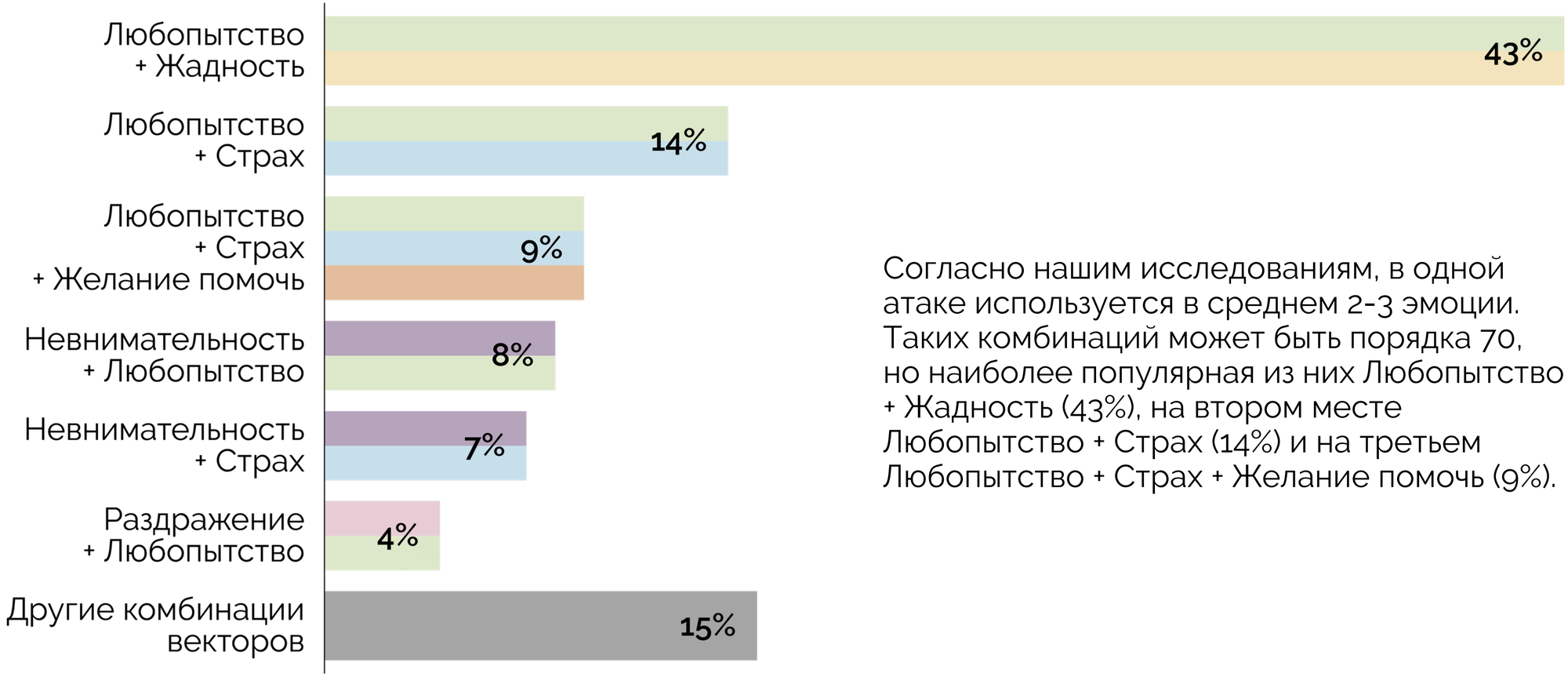
Одним из самых эффективных векторов оказалась Невнимательность.

Невнимательность — это состояние. Из чего можно сделать вывод, что при целевых атаках ошибки и неточности с большой долей вероятности могут быть не замечены сотрудником.

Наиболее эффективными векторами с точки зрения побуждения к небезопасным действиям оказались Невнимательность (44%), Раздражение (38%), Жадность (38%). Разница между эффективностью различных эмоций варьируется в пределах 12%.

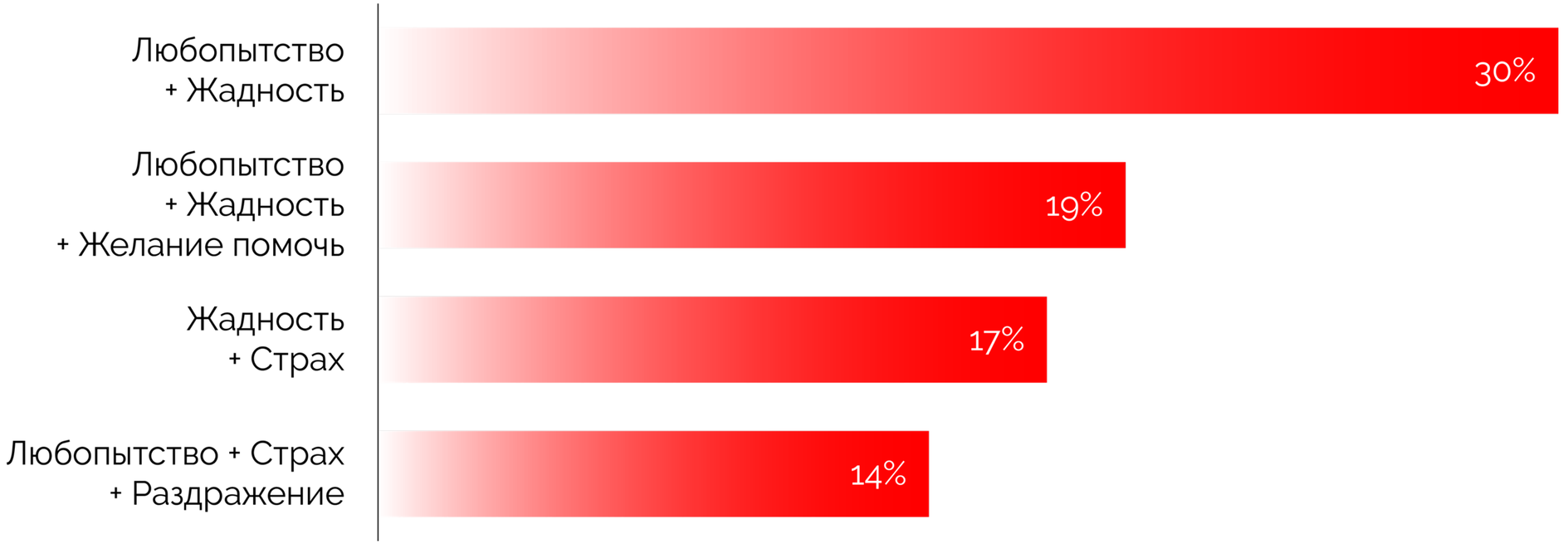


Влияние комбинаций векторов в атаке



Согласно нашим исследованиям, в одной атаке используется в среднем 2-3 эмоции. Таких комбинаций может быть порядка 70, но наиболее популярная из них Любопытство + Жадность (43%), на втором месте Любопытство + Страх (14%) и на третьем Любопытство + Страх + Желание помочь (9%).

Эффективность комбинаций векторов



Сравнение атак по комбинациям эмоций показало, что самая популярная связка Любопытство + Жадность одновременно оказалась и наиболее опасной (30% небезопасных действий). Следом по эффективности идёт похожая комбинация Любопытство + Жадность + Желание помочь (19%)

Влияние усилителей в атаке

Письма, направленные якобы от авторитетного источника, побуждали к небезопасным действиям 20% сотрудников. Фактор срочности сработал в 25% случаев.

Наиболее эффективным оказалось сочетание двух этих усилителей — 30%.

Усилители или психологические катализаторы повышают эффективность атак за счет дополнительной апелляции к эмоциям людей.

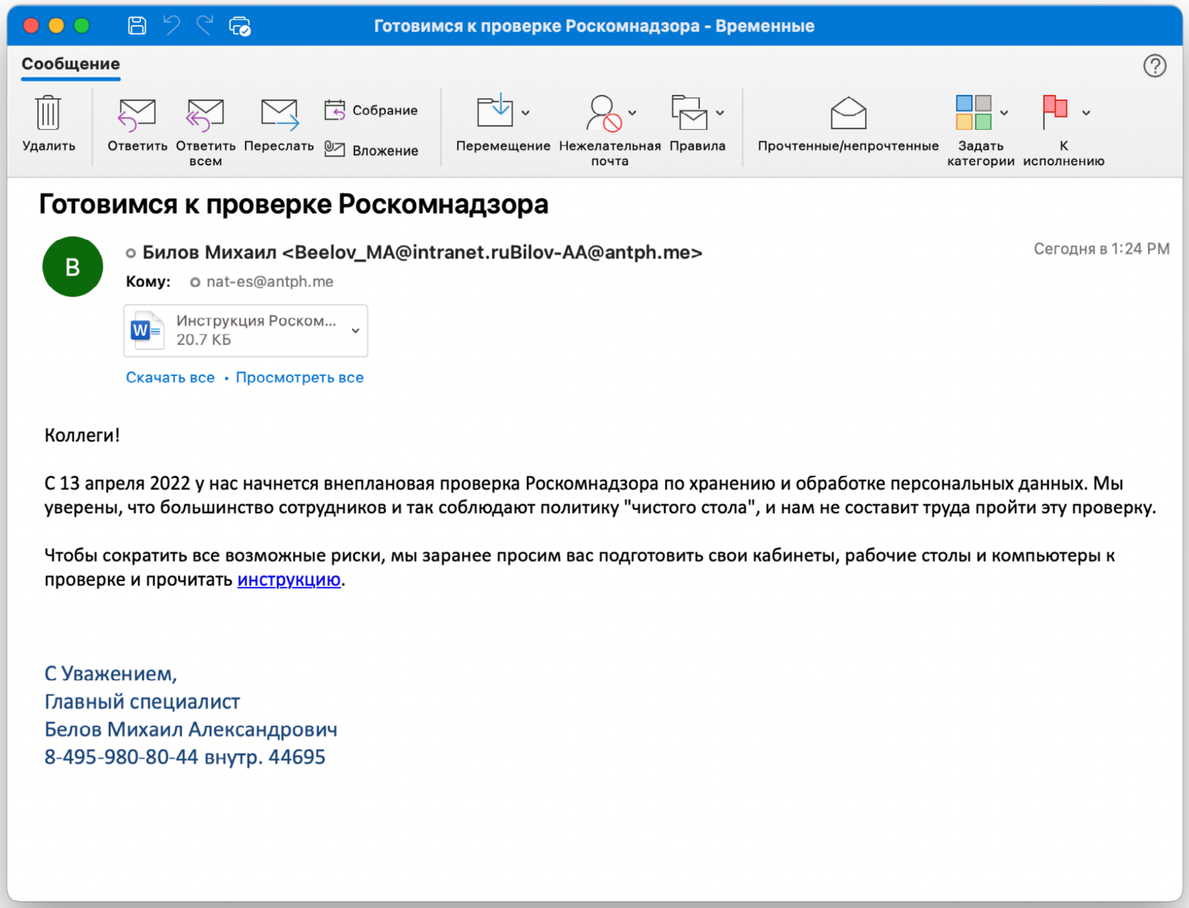
Три самые опасные имитированные атаки в 2021 году

В 2021 году мы поставили клиентам около 700 шаблонов имитированных атак. Из них мы отобрали три самых эффективных, которые чаще остальных провоцировали сотрудников на небезопасные действия.

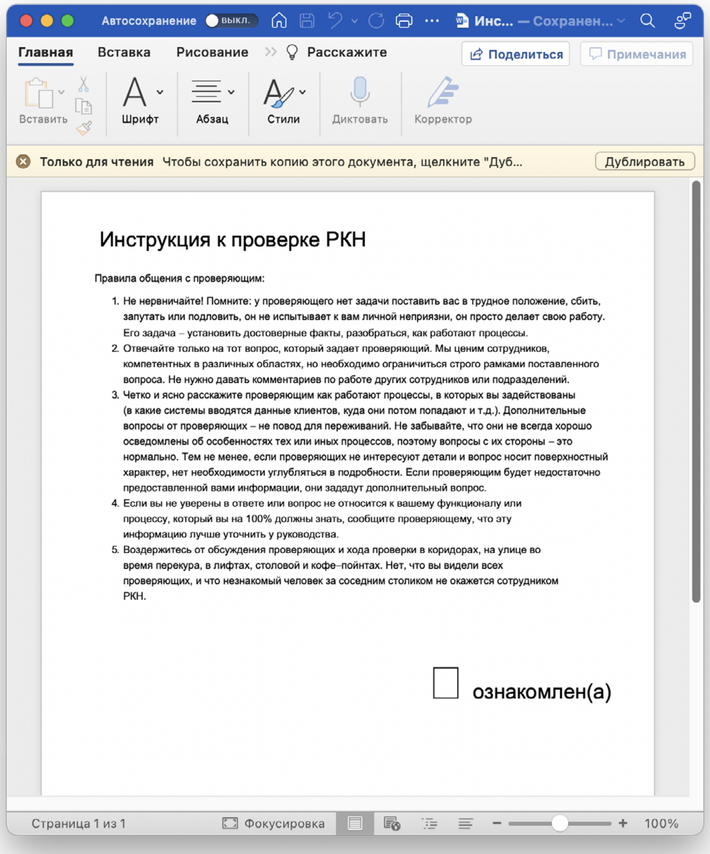
Проверка Роскомнадзора

Корпоративная | Страх | Раздражение

Письмо якобы от коллеги, который сообщает о необходимости подготовиться к проверке Роскомнадзора.



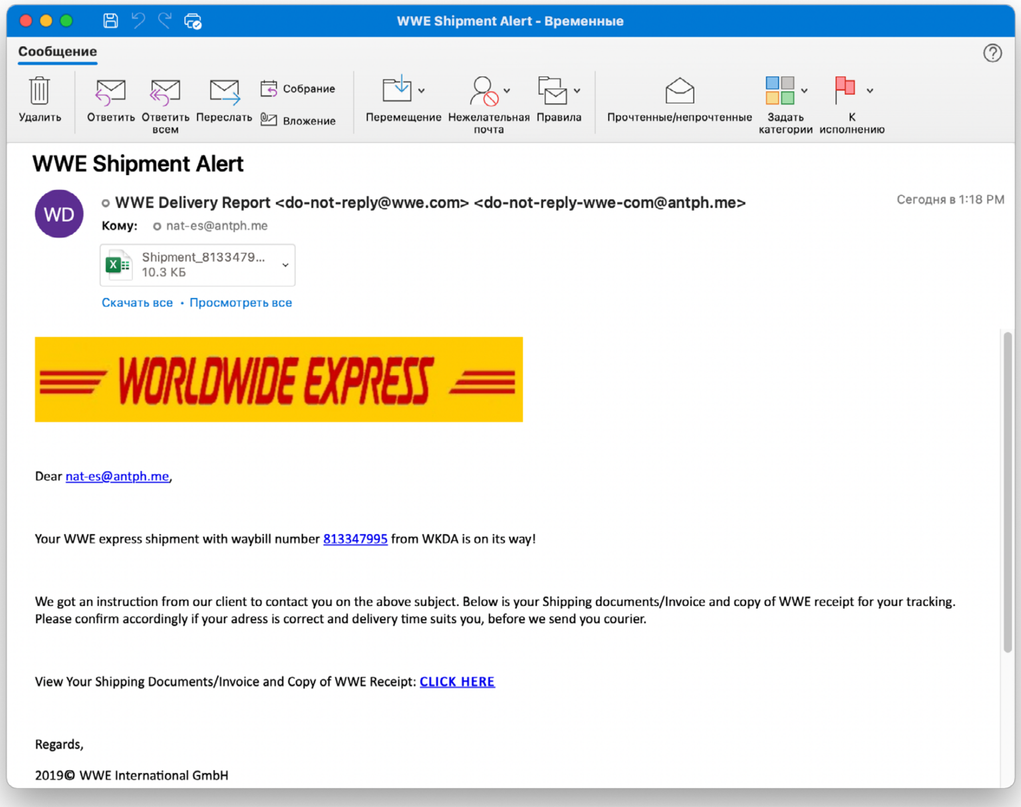
Чтобы поставить отметку об ознакомлении с «инструкцией», сотрудник будет вынужден отключить безопасный режим.



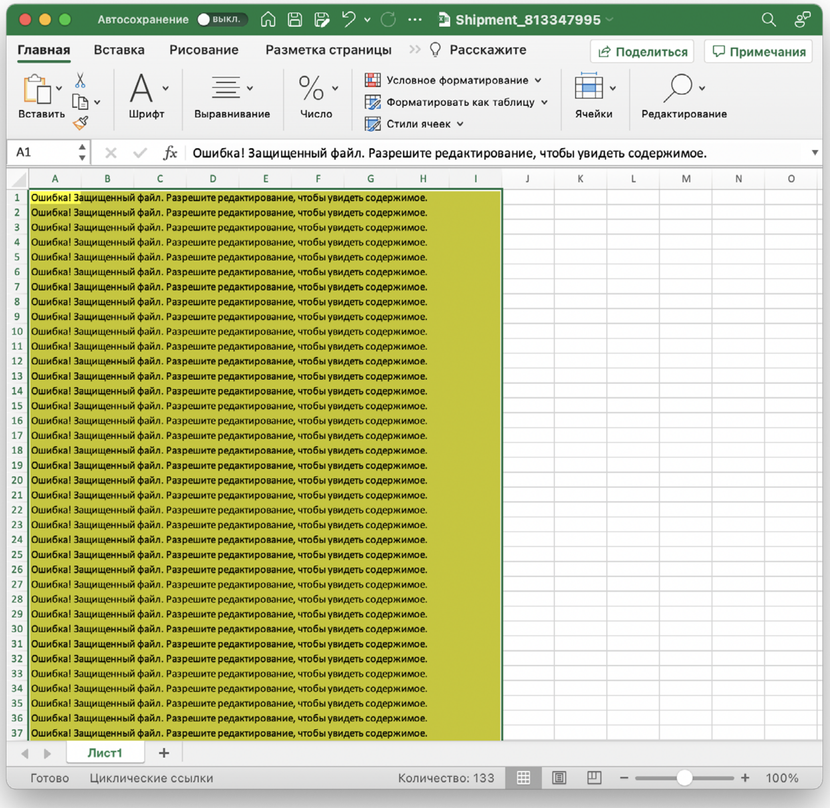
Экспресс-доставка

Внешняя | Желание помочь | Жадность | Любопытство | Авторитет | Срочность

Письмо сообщает получателю о доставке документов бандеролью на его имя.



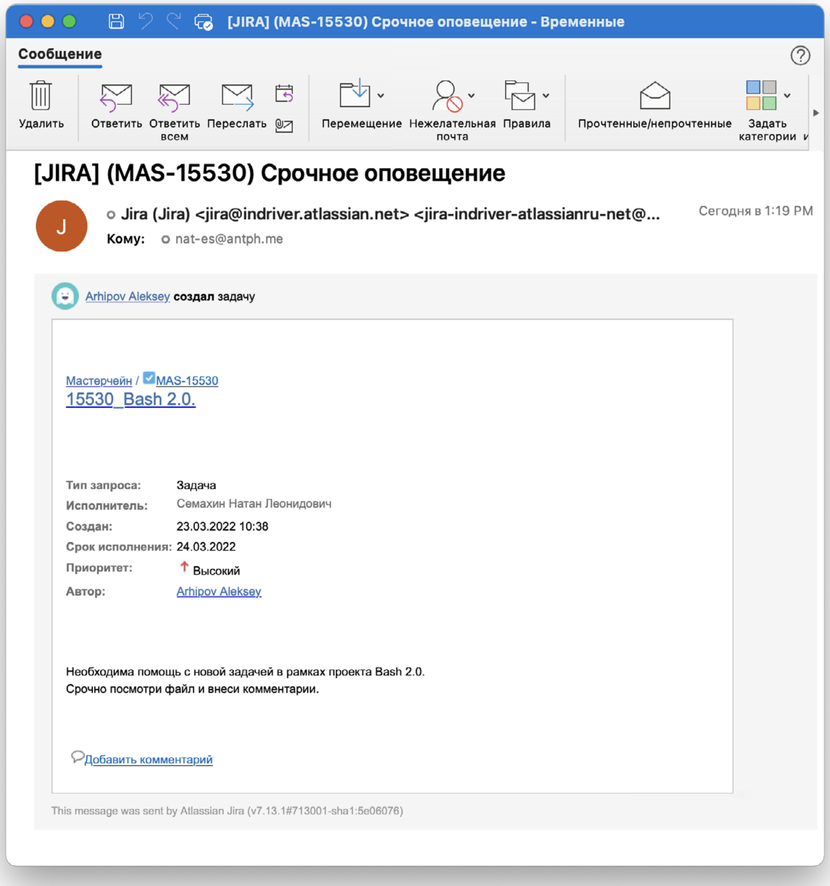
Во вложении вместо данных сотрудник видит надпись «Разрешить редактирование, чтобы увидеть содержимое», и отключает защищенный режим.



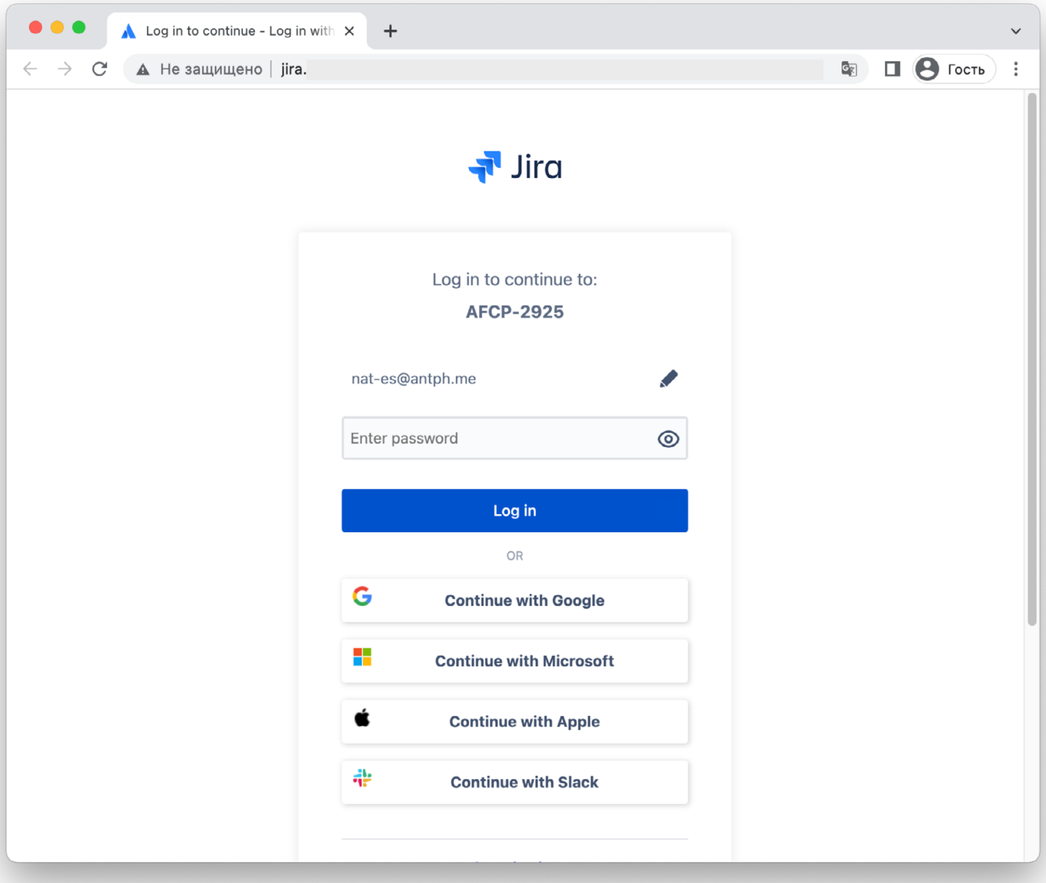
Задача в Jira

Корпоративная | Любопытство | Желание помочь | Срочность | Авторитет

В письме-уведомлении из Jira получатель видит просьбу якобы от коллеги помочь с новым проектом.



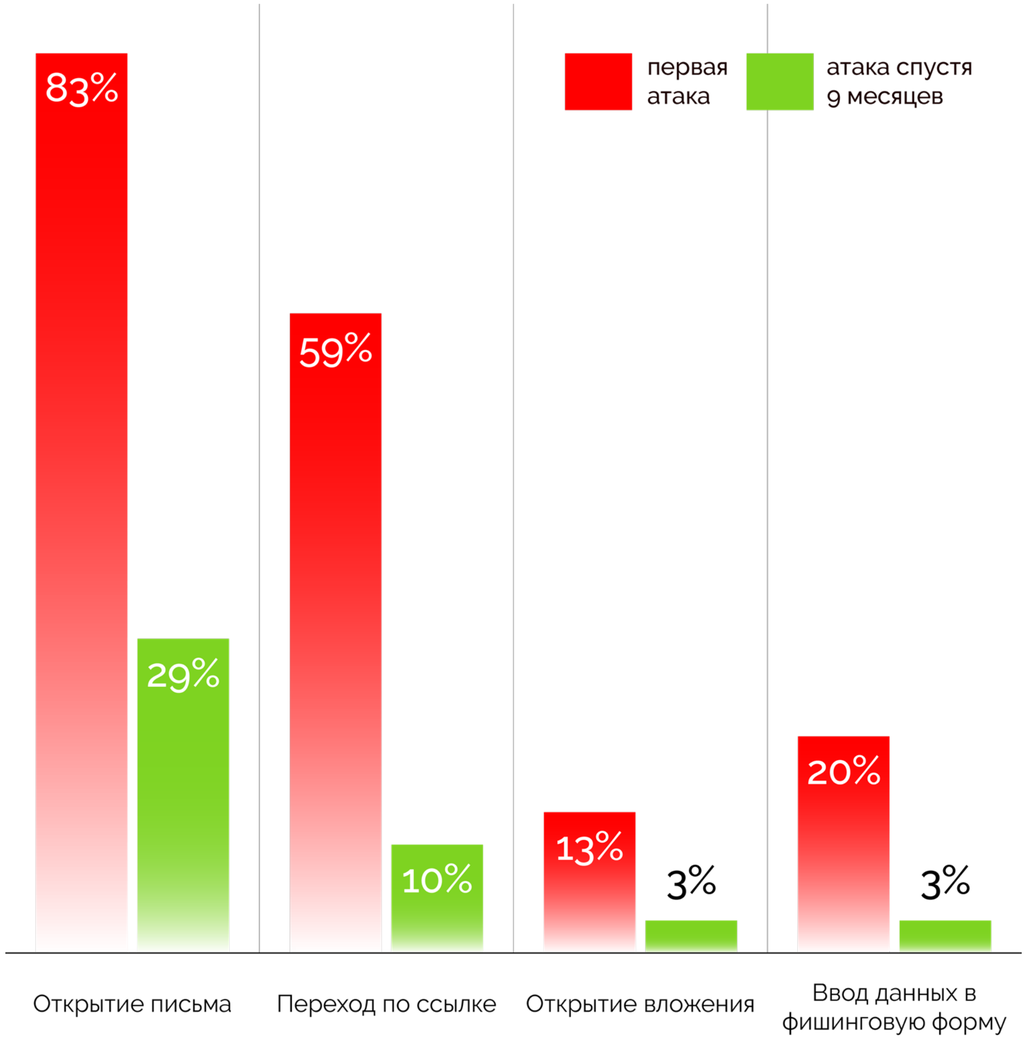
При переходе по ссылке сотрудник попадает на фишинговую форму авторизации в Jira, и вводит свой пароль.



6 Эффективность Антифишинга

На основе методологии и платформы «Антифишинг» мы оценили эффективность обучения и постоянных тренировок с помощью имитированных атак. Наш подход поможет специалистам по информационной безопасности и руководству понять, как измерить устойчивость сотрудников перед цифровыми угрозами, и как улучшить этот показатель в своей организации.

Небезопасные действия



Ключевой результат тренировки навыков — снижение количества небезопасных действий сотрудников с фишинговыми письмами. В рамках тренировки проводится несколько имитированных атак.

Для оценки эффективности мы сравнили показатели по четырём видам небезопасных действий спустя 9 месяцев после начала регулярной тренировки навыков через имитированные атаки среднего уровня сложности. Сравнение по выборке атак одинаковой сложности позволило точнее выявить изменение поведения сотрудников.

Тренировка позволила снизить количество открытий фишинговых писем с 83% до 29%. Также меньше сотрудников стали совершать другие небезопасные действия: переходы по ссылке, заполнение фишинговых форм и открытие вложенных файлов.

Методичный и непрерывный процесс обучения способствует росту безопасного поведения лучше, чем отдельные мероприятия, организуемые раз в год или реже.

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 регулярного проведения имитированных атак среднего уровня сложности. Если перед началом обучения и тренировки сообщений о подозрительных письмах не поступало, то спустя в среднем 9 месяцев о фишинговых письмах сообщали 66% сотрудников. Таким образом, тренировки помогают мотивировать сотрудников к действиям, повышающим защиту компании.

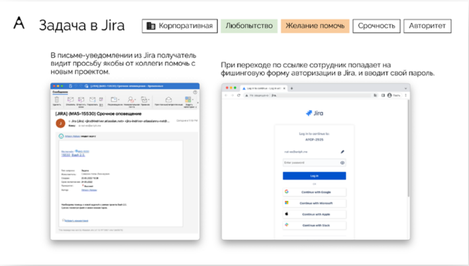
7 Рекомендации по обучению людей

Чек-лист: что сделать уже на этой неделе для защиты от цифровых атак на сотрудников и клиентов

1 Имитируйте атаки на сотрудников с векторами

Любопытство | Страх | Желание помочь

2 Покажите сотрудникам разборы атак и опасные триггеры в письмах



См. слайд 62

3 Назначьте сотрудникам базовый учебный курс по защите от цифровых атак

4 Проведите тестирование, чтобы закрепить и проверить знания

5 Настройте еженедельные информационные оповещения для сотрудников и клиентов об актуальных цифровых атаках

Как сформировать группы риска

Компании со штатом более тысячи сотрудников часто задаются вопросами: кого обучать в первую очередь? Какая категория сотрудников относится к самой уязвимой? И как ее определить? Мы рекомендуем разделить сотрудников на следующие группы и обучать их в таком порядке.

В первую очередь:

- Сотрудники с высоким уровнем доступа ко внутренним ресурсам/системам компании (Администраторы сети, Системные инженеры и т.п.).
- Сотрудники, которые работают с внешними контрагентами (Отдел продаж, Отдел закупок и т.п.).
- Топ-менеджеры.

Во вторую очередь:

- Сотрудники, для которых интернет является основным инструментом работы.
- Сотрудники с уровнем доступа выше среднего ко внутренним ресурсам/системам компании (Техническая поддержка и т.п.).

В третью очередь:

- Сотрудники, у которых есть доступ в интернет, но для которых он не является основным инструментом работы.
- Сотрудники с низким уровнем доступа ко внутренним ресурсам/системам компании.

Группа на повышенном контроле:

- Сотрудники, которые в первой тестовой атаке совершили все типы небезопасных действий.
- Сотрудники, которые не прошли обучение вовремя.

Не реже чем 1 раз в 6 месяцев проводите пересмотр групп риска, при необходимости редактируйте группы (перераспределяйте сотрудников по результатам обучения и тренировки навыков). Оптимально актуализировать группы: раз в квартал.

Что делать с сотрудниками, которые не проходят обучение вовремя

В каждой компании есть сотрудники, которые не понимают и не осознают важность обучения вопросам безопасности. Они постоянно откладывают прохождение курсов и тестов, ссылаясь на высокую занятость, загруженность рабочими задачами и нехватку времени. Вот как мы рекомендуем поступать в таких случаях:

1. Убедитесь, что сотрудник имеет достаточную мотивацию: он знает зачем нужно проходить обучение, почему сейчас это важно, какие есть риски, и как это может повлиять на его жизнь.

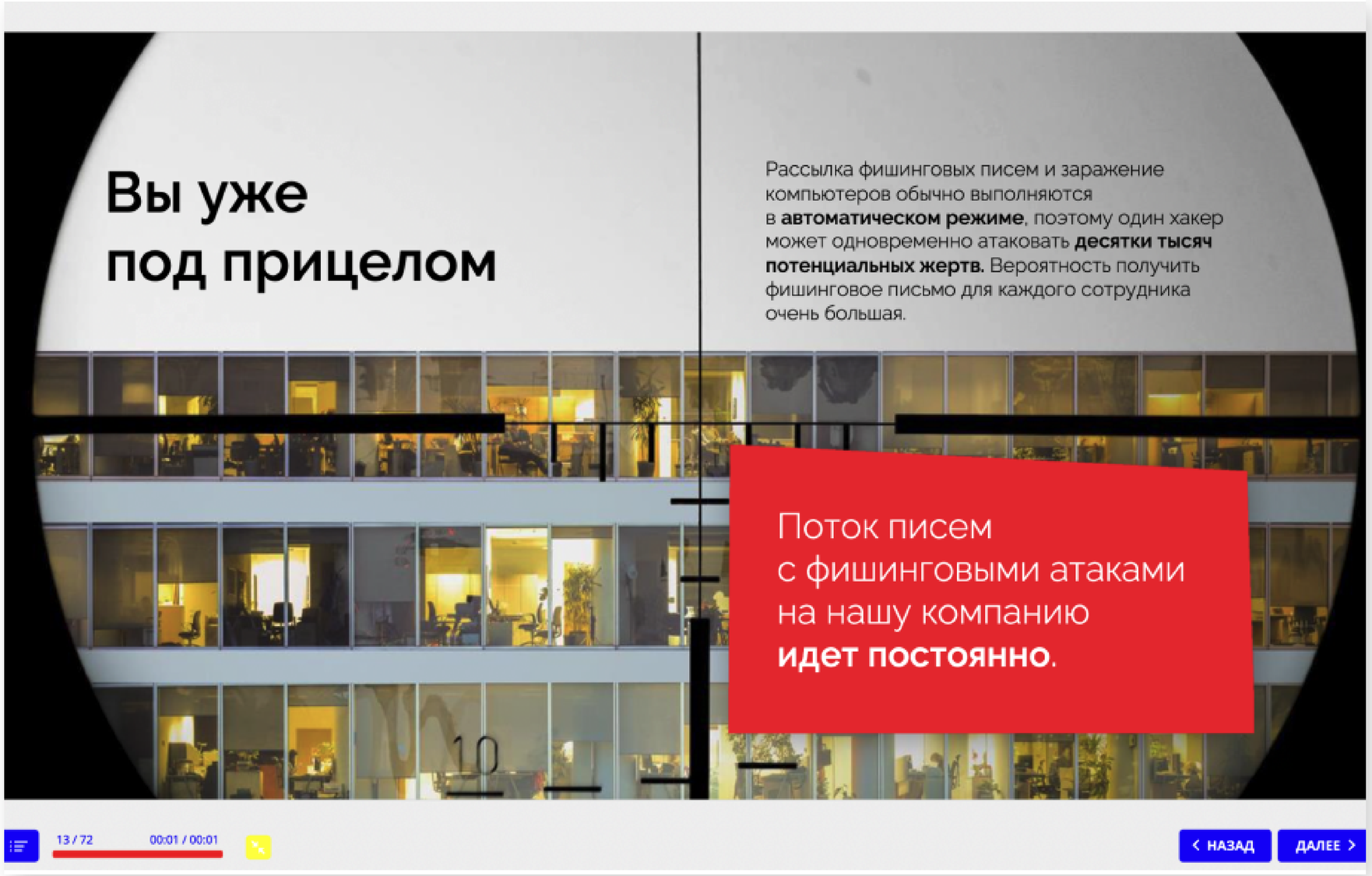
2. Важно, чтобы сотрудник знал, как именно он может помочь защитить компанию, и к чему может привести несоблюдение правил безопасности конкретно им. В этом помогут наши материалы для информационной рассылки перед началом внедрения процессов повышения осведомленности, обучения и тренировки навыков по безопасности.

3. Если сотрудник не прошел курс вовремя — отправьте напоминание.

4. Если после одного напоминания ситуация не изменилась — инициируйте беседу сотрудника с HR-службой или руководителем отдела, в котором он работает.

5. Если беседа не принесла результатов — назначьте административное наказание в соответствии с политикой компании.

Фрагмент обучающего курса



Что делать с разработчиками ПО и продуктовыми командами

Знания и навыки по безопасной разработке разработчиков ПО и продуктовых команд — то, что помогает бизнесу получать продукты без уязвимостей, рисков для репутации и в нужный срок.

Важно, чтобы команды безопасности могли выдавать не противоречивые и актуальные требования по безопасности приложений, а разработчики ПО и продуктовые команды точно знали, что им нужно делать в своих проектах.

Отслеживание изменений в стандартах и лучших практиках, исключение дублирований и противоречий в требованиях по информационной безопасности, а также способах их реализации — сложная аналитическая задача. Особое внимание следует уделять их применимости к различному программному обеспечению.

Чтобы упростить эту задачу, команда Антифишинга подготовила набор чек-листов для типовых приложений с набором требований, которые можно сразу подать на вход продуктовым командам. Для получения чек-листов по другим типовым приложениям напишите на почту, указанную ниже.

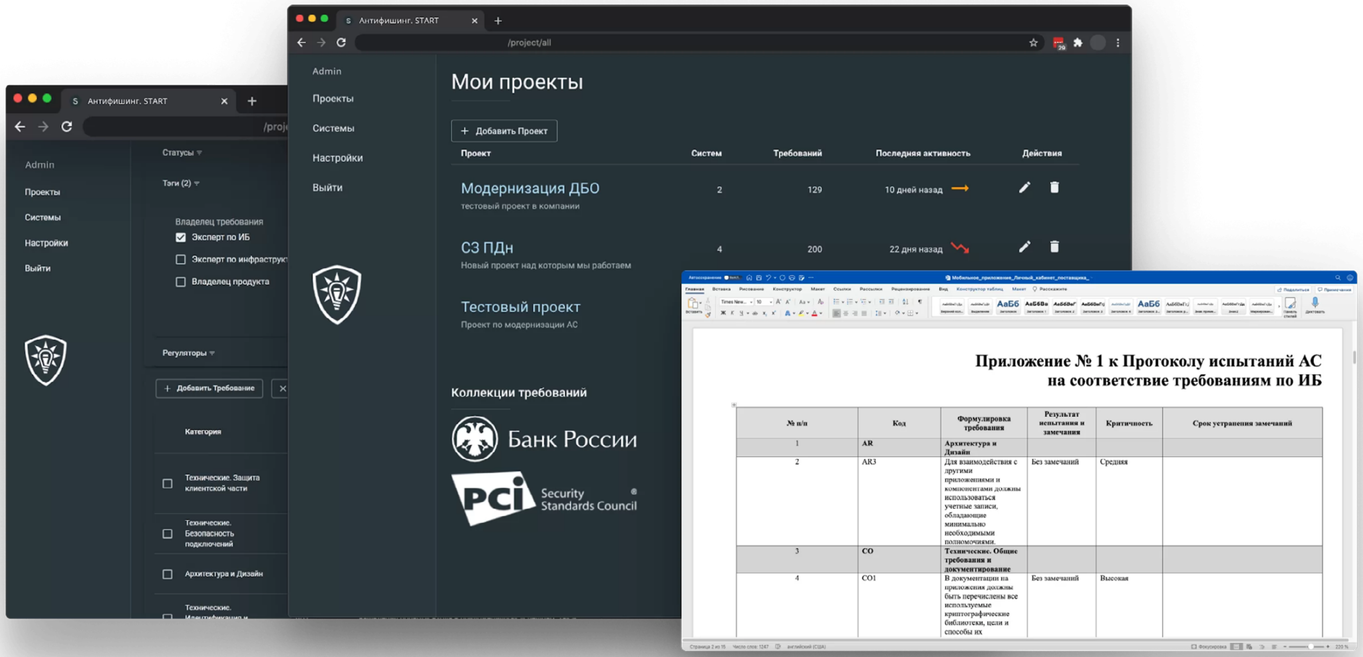
Чек-лист: требования по ИБ для мобильных приложений.

feedback@antiphish.ru.

Что делать с разработчиками ПО и продуктовыми командами

Для регулярного управления требованиями, знаниями и навыками разработчиков ПО и продуктовых команд используйте продукты класса ASRTM — Application security requirements and threat management.

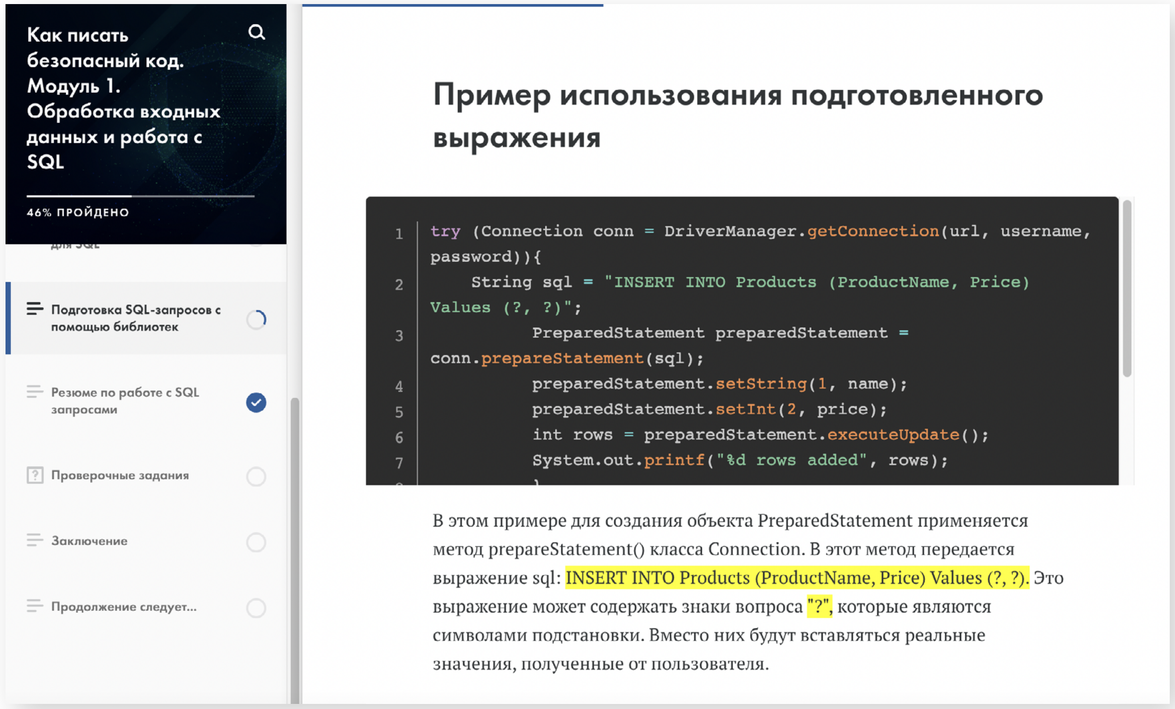
Для демонстрации Антифишинг. START как продукта класса ASRTM в рамках процессов DevSecOps напишите на sales@antiphish.ru.



Что делать с разработчиками ПО и продуктовыми командами

Для быстрого обучения основам безопасности приложений назначьте ключевых членов команд разработки на специализированные курсы.

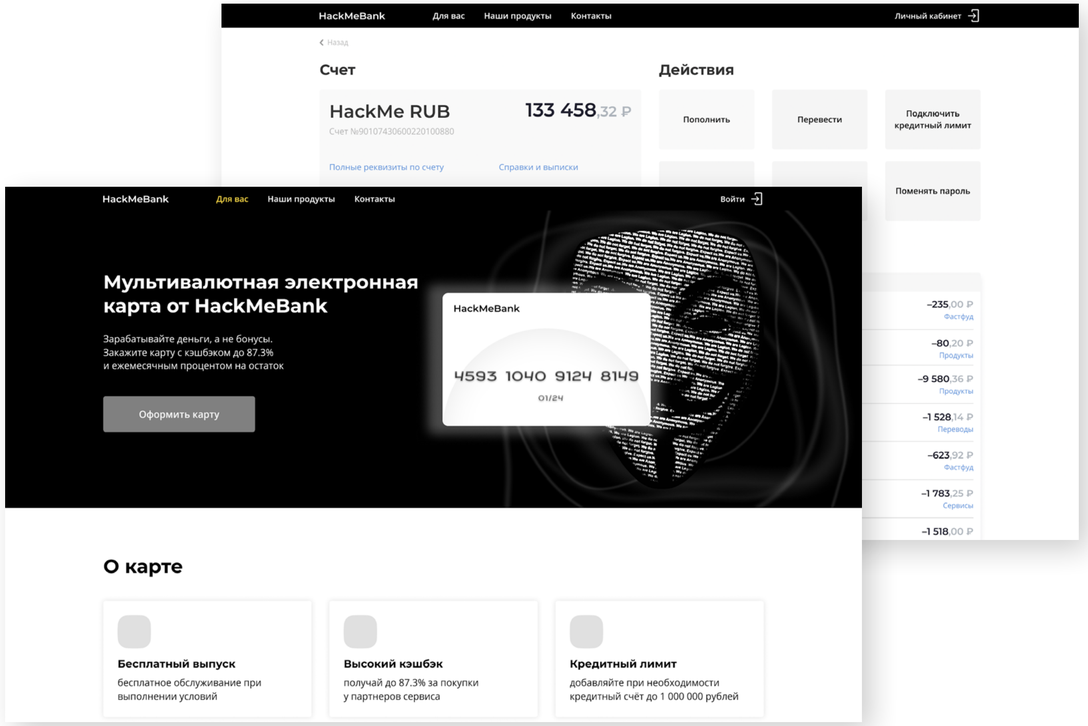
Для получения доступа к курсам по безопасной разработке Антифишинг. START. EDU напишите на feedback@antiphish.ru.



Что делать с разработчиками ПО и продуктовыми командами

Для мотивации команд разработки проведите активности в форме соревнований по поиску уязвимостей на примере реальных приложений и типовых систем, которые разрабатываются в каждой команде.

Для получения доступа к интерактивному CTF-тренажеру Антифишинг. START. CTF напишите на feedback@antiphish.ru.



Заключение

В 2021 году ЦБ РФ зафиксировал более 1 млн операций, совершённых без согласия клиентов финансовых организаций, — на треть больше чем в 2020-ом. По сравнению с предыдущим годом их объём увеличился на 38,8% и превысил 13,5 млрд рублей. Почти 50% операций без согласия клиентов были совершены с использованием приёмов и методов социальной инженерии.

Защита информации в современной организации определяется прежде всего знаниями и навыками сотрудников из разных подразделений, от секретарей до аналитиков и разработчиков ПО.

Обучение и непрерывная тренировка навыков на базе реальных примеров атак позволит сделать сотрудников активным участниками защиты организации от цифровых угроз и в итоге усилит технические средства обеспечения безопасности.

Насколько ваша компания защищена от целевых атак на сотрудников? Проверьте уже сейчас. Оставьте заявку, мы бесплатно проведём три учебные атаки и покажем слабые места в безопасности компании.

Напишите нам, если у вас есть комментарии и дополнения по отчету, или вы хотите заранее узнать и участвовать в будущих исследованиях Антифишинга.

feedback@antiphish.ru

Будем рады ответить на вопросы о применении методологии и платформы «Антифишинг» для обучения и непрерывной тренировки навыков ваших сотрудников.

sales@antiphish.ru

Подпишитесь на наш блог
и Телеграм-канал о фишинге
и других цифровых атаках
на людей. Мы регулярно
показываем, как человеческий
фактор влияет на
безопасность и рассказываем,
что с этим делать

blog.antiphish.ru

t.me/antph

В безопасности важен каждый.
Обучайте и тренируйте своих людей.

antiphish.ru