

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября



В ад без очереди

Тяжелые будни социальных инженеров

Сайма Челейкина

тимлид

Микаэл Хачатрян

Ведущий эксперт

Перспективный мониторинг



Основные работы

Ampire 360°



Почтовый
фишинг



Сторонние
каналы



Вишинг



ИИП



Распространение
USB



Обучение



Физ.
проникновение

Схема проведения работ

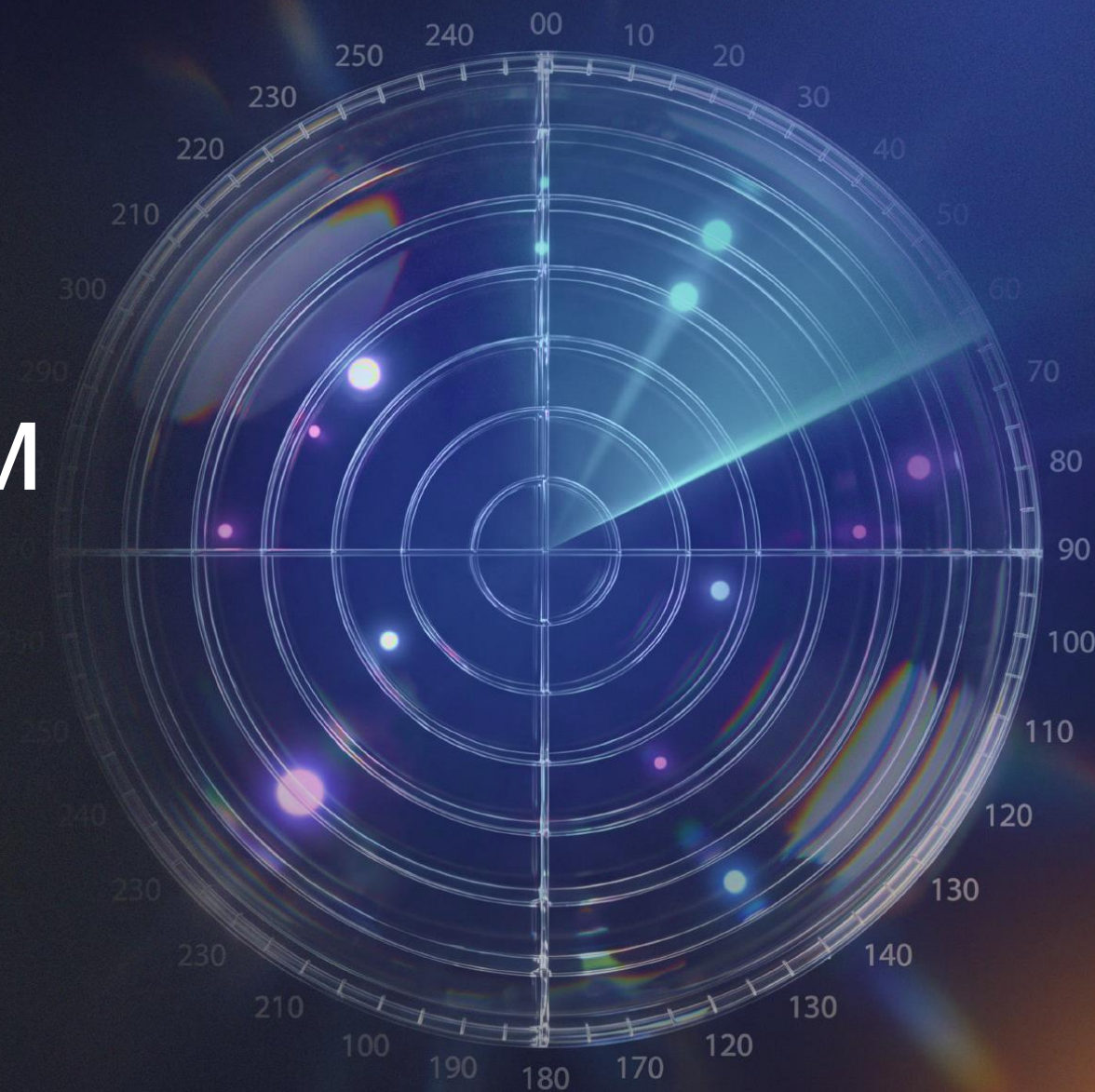


Примечание:

- ▶ Перед фишинговой рассылкой по целевому перечню адресов производится тестовая отправка письма заказчику для согласование формата и полезной нагрузки

Новогоднее чудо с привкусом плесени

История №1



Пример фишингового письма

Уважаемые коллеги!

Уходящий 2018 год был для нашего предприятия годом больших вызовов, упорной работы и важных побед. Каждый из вас внес огромный вклад в общий успех, и руководство искренне благодарит вас за преданность делу и профессионализм.

В преддверии Нового года мы запускаем праздничный проект – **«Фабрика желаний»**. Мы предлагаем каждому сотруднику поделиться своей заветной мечтой. Мы выберем **3 случайных заявки** и исполним их за счет бюджета компании. Имена победителей будут объявлены на праздничном новогоднем корпоративе.

Чтобы принять участие, перейдите на [портал проекта](#), авторизуйтесь под своей рабочей учетной записью и заполните короткую форму. Сбор заявок открыт **до 24 декабря**.

Анна Полякова
HR-департамент

Фабрика Желаний

Напишите свое новогоднее желание и компания его исполнит

Укажите ФИО *

Short answer text

Укажите электронную почту и номер телефона *

Short answer text

Укажите ваш отдел и должность *

Short answer text

Напишите своё новогоднее желание



Paragraph

Long answer text

Получение ответов

Пожертвуйте деньги в детский дом

1 response

Хочу набор конфет как в детстве

1 response

Новенькую кофемашину :))

1 response

Хочу новый bmw

1 response

Купите мне билеты в Барнаул, чтобы я могла навестить родственников на новогодние праздники, которых не видела 3 года

1 response

Хочу оплатить стоматолога и наконец-то вылечить два зуба, которые откладываю с лета

1 response

Подарите мне новое офисное кресло или новый ноутбук МОЩНЫЙ

1 response

Хочу пройти курс для повышения квалификации или сертификат

1 response

Мечтаю о годовом абонементе в фитнес-клуб с бассейном

1 response

Пора менять резину на машине а она щас дорогая

1 response

Помогите оплатить лечение больной мамы

1 response

Результаты рассылки

Email Sent



Email
Opened



Clicked Link



Submitted
Data



404: Выходной не найден

Ampire 360°

История №2

Пример фишингового письма



Чт 26.09.2019 13:24

Сокращенная рабочая неделя

 Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

Уважаемые коллеги!

Просьба ознакомиться с информацией отдела кадров. Согласно решению правительства, на предприятиях начнут испытывать 4-хдневную рабочую неделю. Как одна из компаний, входящих в национальный проект по повышению производительности, [REDACTED] добавлена в группу тестирования. В приложенном файле вы найдете новый график работы на 4-ый квартал. Просьба ознакомиться и распечатать заявление о согласии на участие в эксперименте. Более подробная информация в ближайшее время будет озвучена на общем собрании.

С уважением,

Отдел правового обеспечения и управления персоналом



График
работы.docx



Заявление.
docx

Образец лог-файла

```
kali@kali: ~  
File Edit View Search Terminal Help  
kali@kali:~$ tail -f /home/kali/scripts/parser_log  
Sep 26 13:28:55.434 17[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 13:29:14.102 17[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 13:30:02.851 17[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 13:32:41.119 17[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 13:35:10.552 17[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
  
Sep 26 14:12:33.004 213.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (iPhone; CPU iPhone OS 12_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Mobile/15E148 Safari/604.1  
Sep 26 14:15:44.218 213.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (iPhone; CPU iPhone OS 12_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Mobile/15E148 Safari/604.1  
Sep 26 14:28:02.105 213.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
  
Sep 26 16:45:11.882 178.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 16:48:19.901 178.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
Sep 26 16:50:02.115 178.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36  
  
Sep 26 16:52:44.348 94.[REDACTED] user [REDACTED] z.ru id 9d7HmGx launch the file. UA: Mozilla/5.0 (Linux; Android 9; SM-G960F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.92 Mobile Safari/537.36
```

Ответ пользователя



ошибка.png
37 KB



Добрый день!

Хотел принять участие в программе, но никак не удается открыть заявление, вылезает ошибка (скриншот приложил).
Пожалуйста, помогите открыть документ и распечатать заявление.

С уважением,



Загадочное исчезновение письма

Ampire 360°



LIVE

История №3

Пример фишингового письма

Тема: График отпусков на 2025 год

Коллеги, добрый день!

Теперь график отпусков будет формироваться через наш **корпоративный портал**.

Прошу **до 15 ноября (пятницы) 18:00** заполнить информацию о планируемом в **2025** году отпуске по **ссылке**.

Составление графика отпусков является **обязательным**.

Напоминаю, что:

- хотя бы одна из частей отпуска должна быть не менее 14 календарных дней (неразрывных);
- отпуск предоставляется в календарных днях, поэтому не забывайте включать выходные;
- дни отпуска должны быть согласованы с руководителем;
- новым сотрудникам ежегодный оплачиваемый отпуск предоставляется после 6 месяцев работы в компании;
- перенос отпуска возможен, если составить соответствующее заявление и согласовать с руководством.

Готова ответить на возникающие вопросы.

Таймлайн отправки письма

Timeline for [REDACTED]

Email: [REDACTED]

Result ID: tzT0TQB



Campaign Created

November 11th 2024 4:00:00 pm



Email Sent

November 11th 2024 4:00:01 pm



Email Opened

November 11th 2024 4:13:24 pm



Clicked Link

November 11th 2024 4:13:27 pm

 Windows (OS Version: 10)

 Firefox (Version: 155.0)



Submitted Data

November 11th 2024 4:13:34 pm

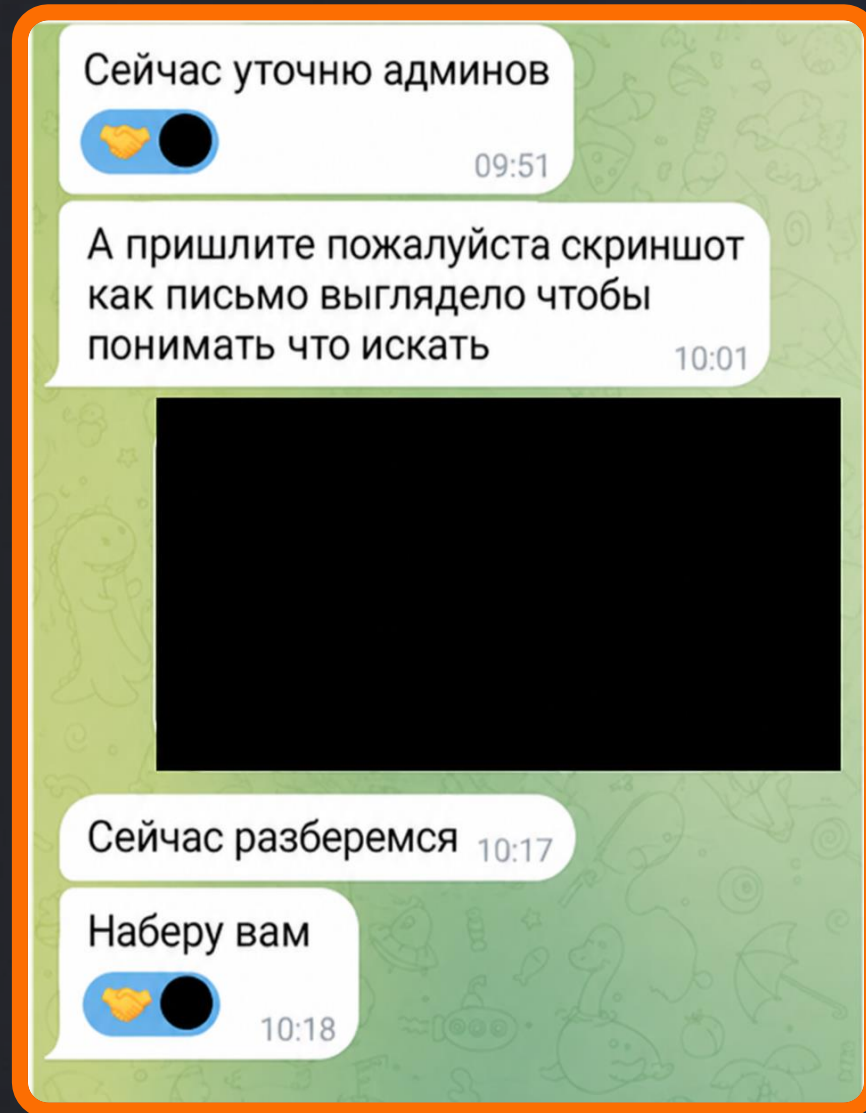
 Windows (OS Version: 10)

 Firefox (Version: 155.0)

 [Replay Credentials](#)

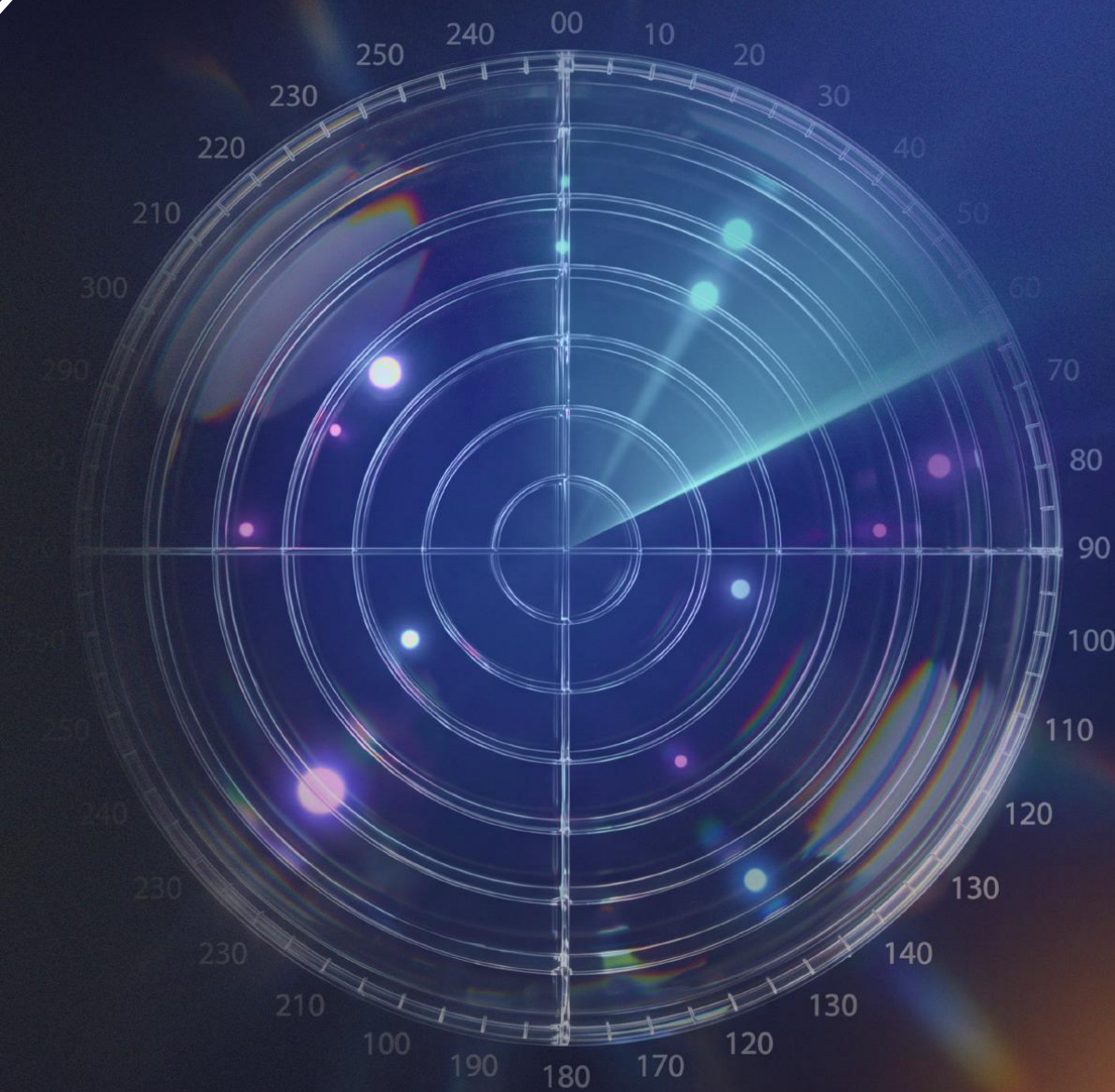
[View Details](#)

Поиск пропавшего письма



Шоу «Интуиция»

Ampire 360°



История №4

Пример фишингового письма

Актуализация данных клиента



info@[REDACTED] Сегодня в 11:36

Я >

Папка: Входящие

Уважаемый клиент!

Ваши персональные данные не прошли проверку. По закону "О связи" номер может быть заблокирован, если данные не будут подтверждены.

Проверьте ваши данные (фамилия, имя, отчество, дата рождения, место жительства, реквизиты основного документа, удостоверяющего личность) в личном кабинете [https://lk.\[REDACTED\]](https://lk.[REDACTED]). Служба поддержки - [https://support.\[REDACTED\]](https://support.[REDACTED])

Список нормативных документов

- Ст. 44, 46 и 64 Федерального закона от 07.07.2003 г. № 126-ФЗ «О связи».
- П. 25 Правил оказания услуг телефонной связи (утв. Постановлением Правительства РФ от 09.12.2014 N 1342) Федеральный закон от 07.08.2001 г. N 115-ФЗ «О противодействии легализации («отмыванию») доходов, полученных преступным путём, и финансированию терроризма».
- П. 14 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность (утв. Постановлением Правительства РФ № 538 от 27.08.2005 г.).

Пример фишинговой страницы

Вход



Личный кабинет для корпоративных клиентов

Номер телефона в формате 9XXXXXXX...

Введите пароль* 

[Забыли пароль?](#)

Продолжить

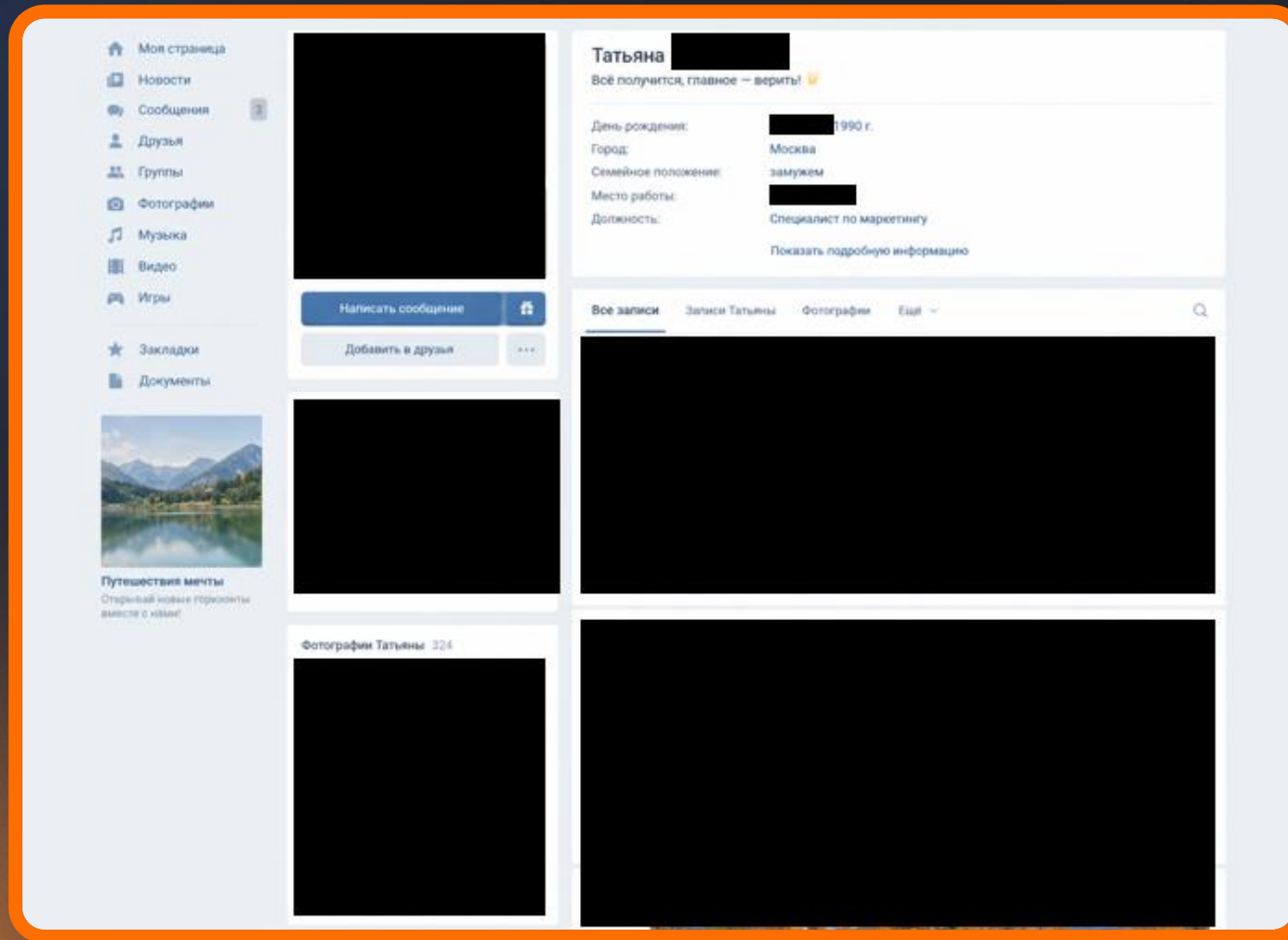
Доступ в Личный кабинет 

Код доступа: Арабика

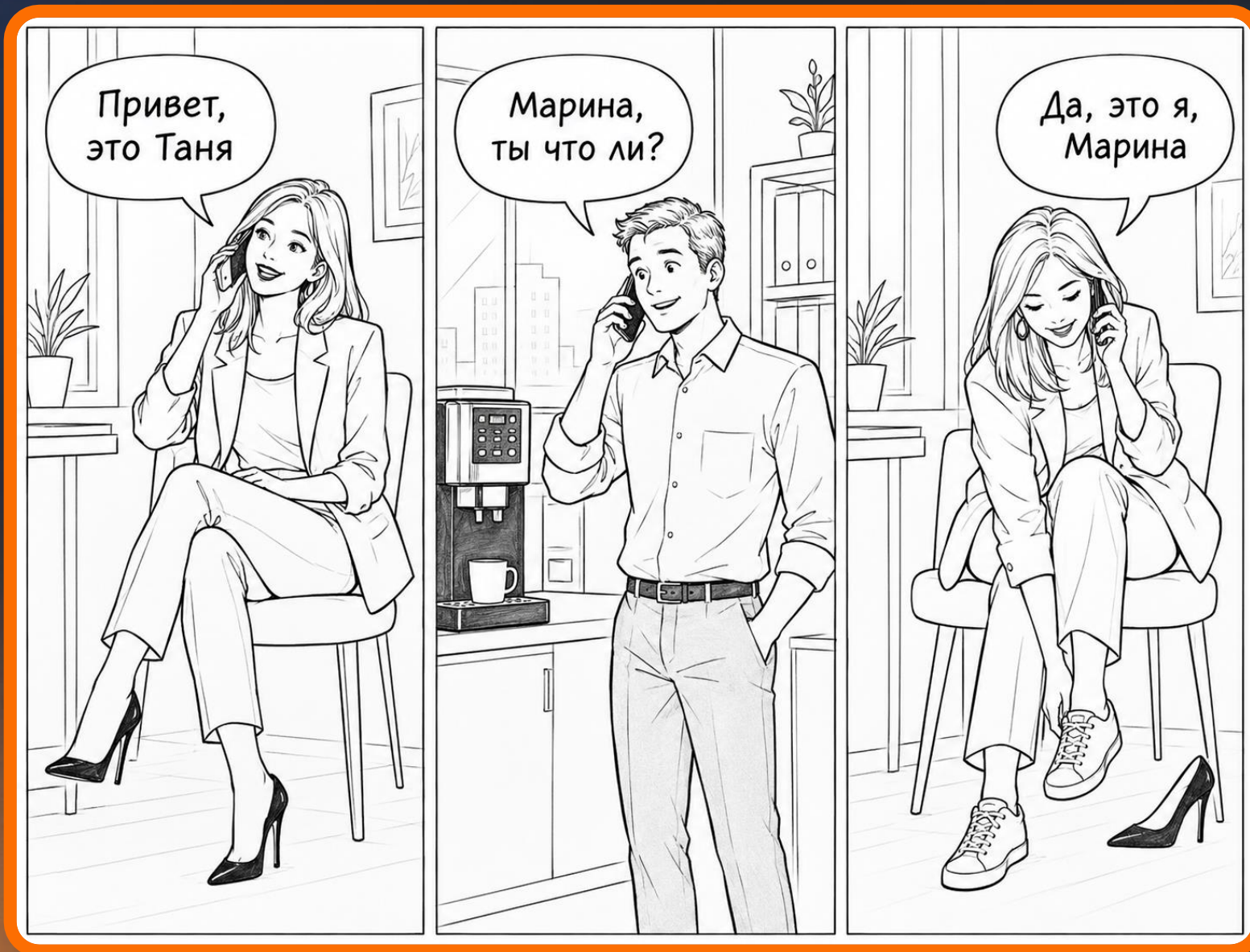
История №5



Пример страницы из разведки



Первая часть вишинга

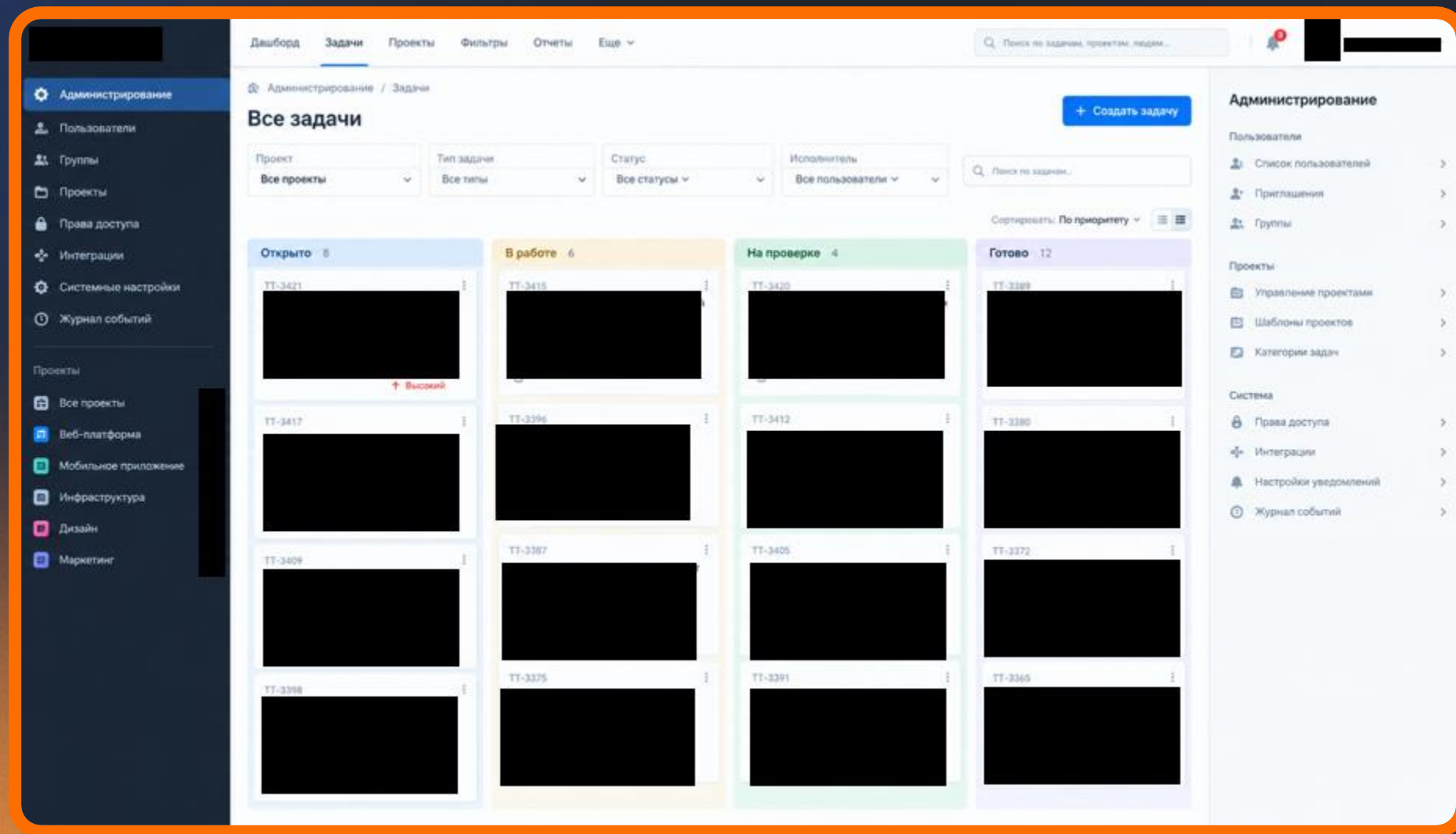


Вторая часть вишинга

Звонок полученному контакту



Пример доступа к системе



Подозрительные мужчины

Ampire 360°

История №6

Незаблокированные АРМ

Ampire 360°



Рассылка от бдительного сотрудника

Subject: ВАЖНО !!!! БЕЗОПАСНОСТЬ !!!!ЧУЖИЕ ЛЮДИ В НАШЕМ ОФИСЕ!!!

Здравствуйте! Коллеги!!!

*Убедительная просьба к вам **смотреть, когда заходите из лифтового холла в офис, кто стоит там и кто заходит с вами.***

При входе в офис дождитесь , пока за вами закроется дверь. Дверь с доводчиком и надо время, чтобы она закрылась,

*но это стоит того. Это, в конце концов, **НАША БЕЗОПАСНОСТЬ !!!***

Сейчас кто-то входил либо с улицы, либо ходил через холл в туалет или столовую и запустил двух мужчин подозрительных , которые ничего внятно не могли сказать о цели своего визита к нам.

*По распоряжению директора **ПРОХОД ЧЕРЕЗ ХОЛЛ С ДРУГОГО КРЫЛА В ТУАЛЕТ, ЛИБО В СТОЛОВУЮ ЗАПРЕЩАЕТСЯ***

И ДВЕРИ БУДУТ ЗАБЛОКИРОВАНЫ В БЛИЖАЙШЕЕ ВРЕМЯ !!!

Это уже не первый раз , когда с нашими сотрудниками в офис проникают совершенно посторонние люди!!!

Будьте бдительны!!!

Рассылка от ИБ

Уважаемые руководители! Уважаемые коллеги!

В рамках мероприятия по повышению уровня информированности сотрудников в области информационной безопасности напоминаем Вам основные требования по обеспечению информационной безопасности при использовании персональных компьютеров.

1. Доступ к ПК предоставляется сотрудникам после ознакомления с организационно-распорядительными и нормативно-методическими документами по информационной безопасности.

2. Сотрудник, которому предоставлен доступ к ПК, обязан:

- **на время отсутствия на рабочем месте блокировать экран ПК** (путем одновременного нажатия на клавиатуре ПК комбинации клавиш «CTRL+ALT+DEL» и выбором пункта «Блокировать компьютер»);
- по завершении рабочего дня выключать ПК и источники бесперебойного питания;
- сообщать в отдел информационной безопасности обо всех случаях появления сообщений антивирусной системы, о наличии вредоносного программного обеспечения, несанкционированного доступа к информации на ПК, а также о фактах нарушения настоящих Требований.

3. Пользователям ПК **запрещается**:

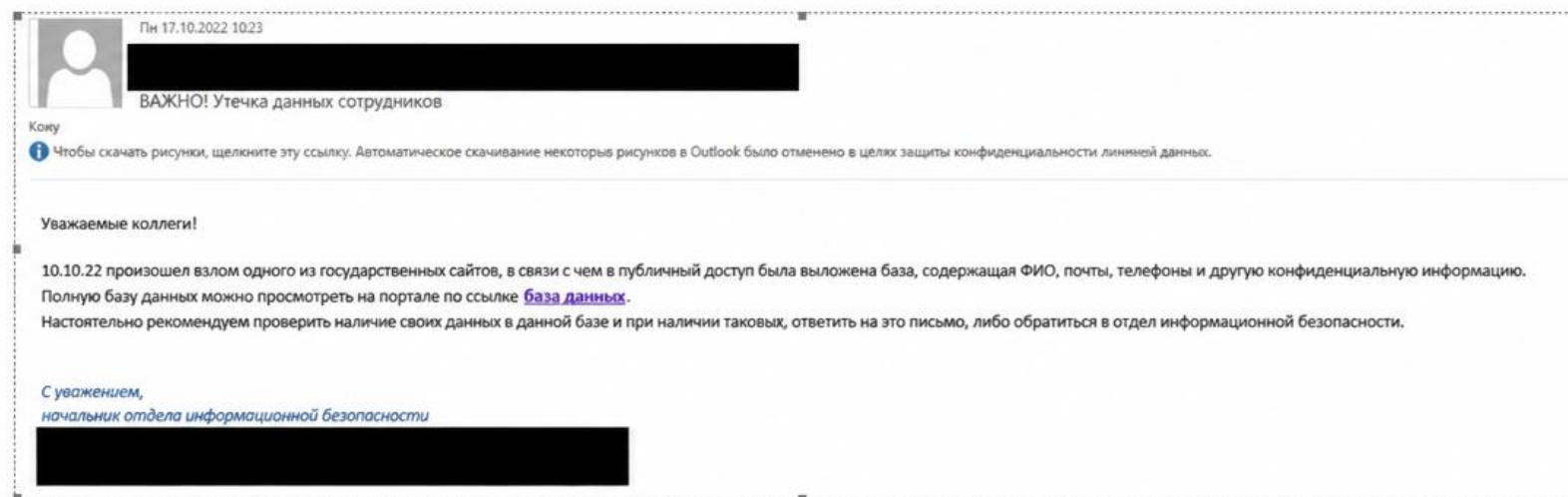
- предоставлять доступ к ПК иным лицам, за исключением сотрудников отдела информационной безопасности и сотрудников обслуживающей организации. Если вы сомневаетесь, действительно ли это представившийся сотрудник, необходимо уточнить это в отделе информационной безопасности или в технической поддержке [REDACTED];
- работать под учетными записями, зарегистрированными на других пользователей ПК;
- осуществлять действия, направленные на получение несанкционированного доступа к ресурсам локальных вычислительных сетей.

4. При возникновении неисправностей в ПК, для их устранения пользователю ПК следует обратиться в обслуживающую организацию в установленном порядке.

Уважаемые руководители! Уважаемые коллеги!

В ближайшее время была зафиксирована рассылка спам-сообщений. Напоминаем Вам о необходимости соблюдения простых правил при работе с электронной почтой:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);
- не нажимать на ссылки из письма, если они заменены на слова;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывать вложения от неизвестных отправителей, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
- внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.



Инструкция для проверки безопасности корпоративных учетных записей - во вложении.

Вторая рассылка от ИБ

Уважаемые руководители! Уважаемые коллеги!

В связи с продолжающейся спам-рассылкой просим внимательно проверять адрес электронной почты при получении писем, **особенно** писем, содержащих вложения или предлагающих перейти по ссылке.

Не отвечайте на сообщение, не переходите по ссылкам и не загружайте подозрительные вложения.

При наличии каких-либо подозрений, обращайтесь в отдел информационной безопасности.

Все письма от сотрудников [REDACTED] автоматически подписываются цифровой подписью. У большинства сотрудников привязана фотография к учетной записи, что также является отличительной чертой.

Астрологи объявили неделю взломанных аккаунтов

Ampire 360°



История №7

Разные способы получения пароля



Результат работы

email:pass

[REDACTED]:17012002

[REDACTED]:18041978

[REDACTED]:19011988

[REDACTED]:21021963

[REDACTED]:19071993

[REDACTED]:18081955

[REDACTED]:13051968

[REDACTED]:02031994

[REDACTED]:26062007

[REDACTED]:28051979

[REDACTED]:25111975

[REDACTED]:18041985

[REDACTED]:16122005

[REDACTED]:27011963

[REDACTED]:03011966

[REDACTED]:27091972

Заключение



Методы воздействия

Искусственный дефицит ресурса

Намеренное ограничение времени или объема доступного предложения для цели

Давление авторитетом

Имитация запросов от лица высшего руководства, контролирующих органов или регуляторов

Новостной джекинг

Использование актуальных внешних новостей или плановых внутренних процессов компании

Социальное доказательство

Использование ориентации на поведение большинства при принятии решений

Эмоциональные триггеры

Целевое воздействие на чувства человека: страх, вину, жадность, эмпатию, чувство противоречия и др.

Автоматизм поведения

Использование привычных повседневных привычек и отработанных поведенческих паттернов

Спасибо за внимание!

Сайма Челейкина

тимлид

Микаэл Хачатрян

Ведущий эксперт

Перспективный мониторинг



Ampire 360°