КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ | 02 ДЕКАБРЯ 2021

КАК АТАКОВАЛИ ЛЮДЕЙ В 2021 ГОДУ И КАК ЗАЩИТИТЬ СВОИХ СОТРУДНИКОВ В 2022 ГОДУ?

СЕРГЕЙ ВОЛДОХИН, АНТИФИШИНГ

МОСКВА

АНТИФИШИНГ

Как атаковали людей в 2021 году

и как защитить своих сотрудников
в 2022 году

www.antiphish.ru

1. Как атаковали людей в 2021 году?

blog.antiphish.ru

t.me/antph

Киберкампании

Обнаружена киберкампания группировки ChamelGang против топливно-энергетического комплекса и авиационной промышленности РФ.

Психологические векторы атак

Усилители реакции

Страх Ваш компьютер заражен и заблокирован. Кликните здесь.	**Невинма-тельонсть** www.sbernbank.ru www.gmall.com	**Раздражение** Чтобы отписаться, перейдите по ссылке.
Любопытство Смотри как ты отжигаешь на видео!	**Жадность** Скидка 50% при оплате прямо сейчас!	**Желание помочь** Ваш коллега потерял свои вещи. Дайте его номер.

Срочность

Отчет прислать сегодня до 15:00

Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

Психологические векторы атак

93% атак

Страх Ваш компьютер заражен и заблокирован. Кликните здесь.	**Невинма-тельонсть** www.sbernbank.ru www.gmall.com	**Раздражение** Чтобы отписаться, перейдите по ссылке.
Любопытство Смотри как ты отжигаешь на видео!	**Жадность** Скидка 50% при оплате прямо сейчас!	**Желание помочь** Ваш коллега потерял свои вещи. Дайте его номер.

Усилители реакции

Срочность

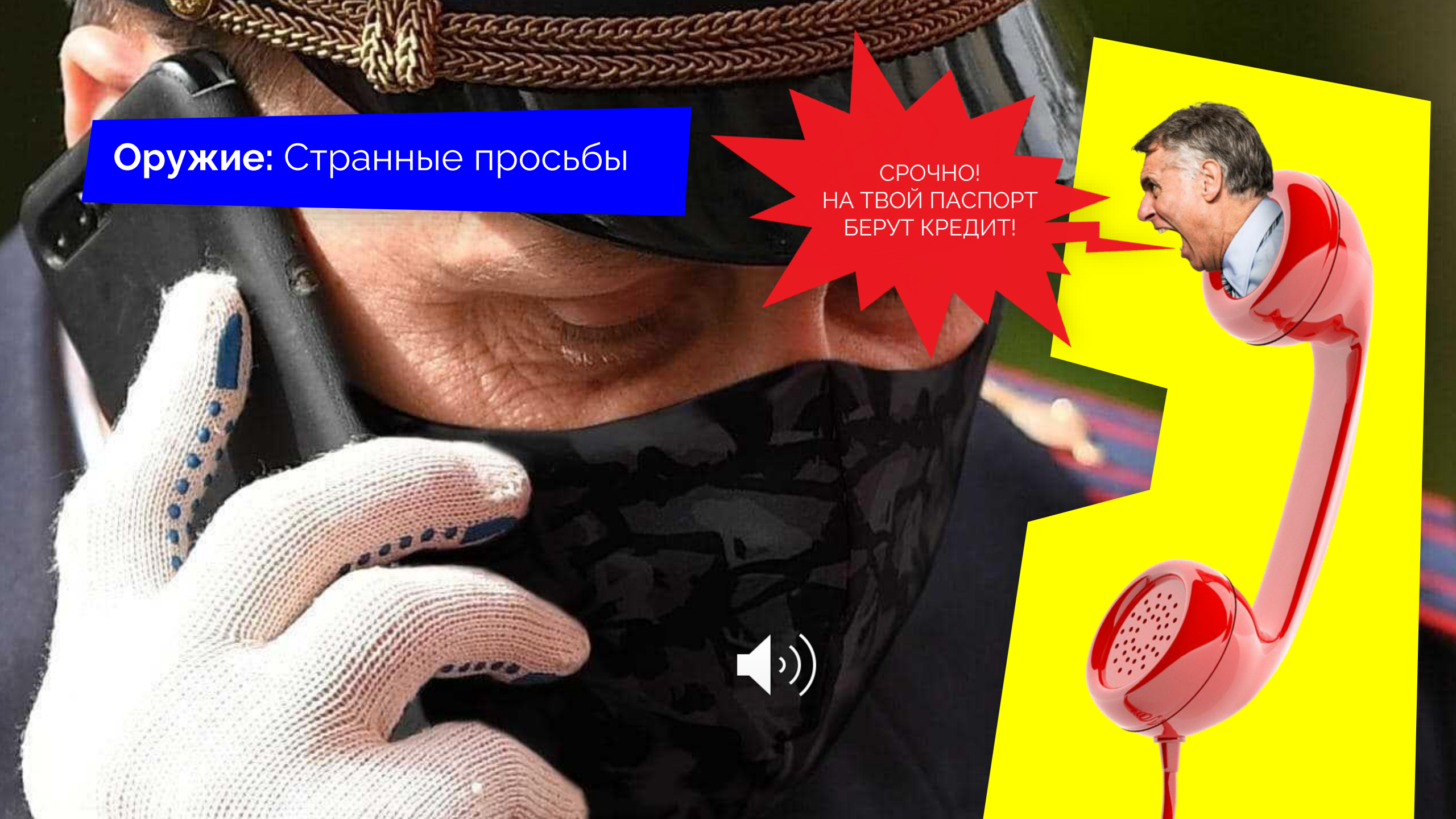
Отчет прислать сегодня до 15:00

Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

Оружие: Странные просьбы

СРОЧНО!
НА ТВОЙ ПАСПОРТ
БЕРУТ КРЕДИТ!



13:13 LTE

Предложение от банка

Основные условия

до 5 млн ₽
сумма

от 1 до 7 лет
срок кредита

от 5,5 %
ставка

за 2 минуты
решение

Шаг 1 из 5. Получите **+40%** к одобрению, заполнив первый шаг

Персональные данные

Игорь Владимирович, укажите адрес вашей электронной почты, чтобы мы могли направить ценную для вас информацию по заявке.

Электронная почта
test@mail.ru

Главный | История | Платежи | Витрина | Чат

13:16

Кредит онлайн

Сумма	Ставка	Срок
до 5 млн ₽	от 5,9 %	до 5 лет

Подайте заявку
Без визита в офис

Узнайте финальное решение
Займет не более 2 минут

Получите деньги
Зачислим на ваш счет

Подать заявку

Узнать о преимуществах

13:17

Кредит наличными

Ставка от 5.9%

Перечислим деньги на дебетовую карту

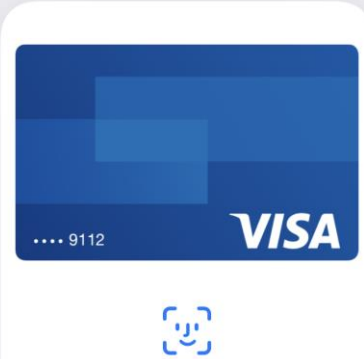
Досрочное погашение в любое удобное время

Нажимая «К оформлению», вы разрешаете ба просмотреть ваш кредитный отчет. Условия

К оформлению

13:18

Отменить

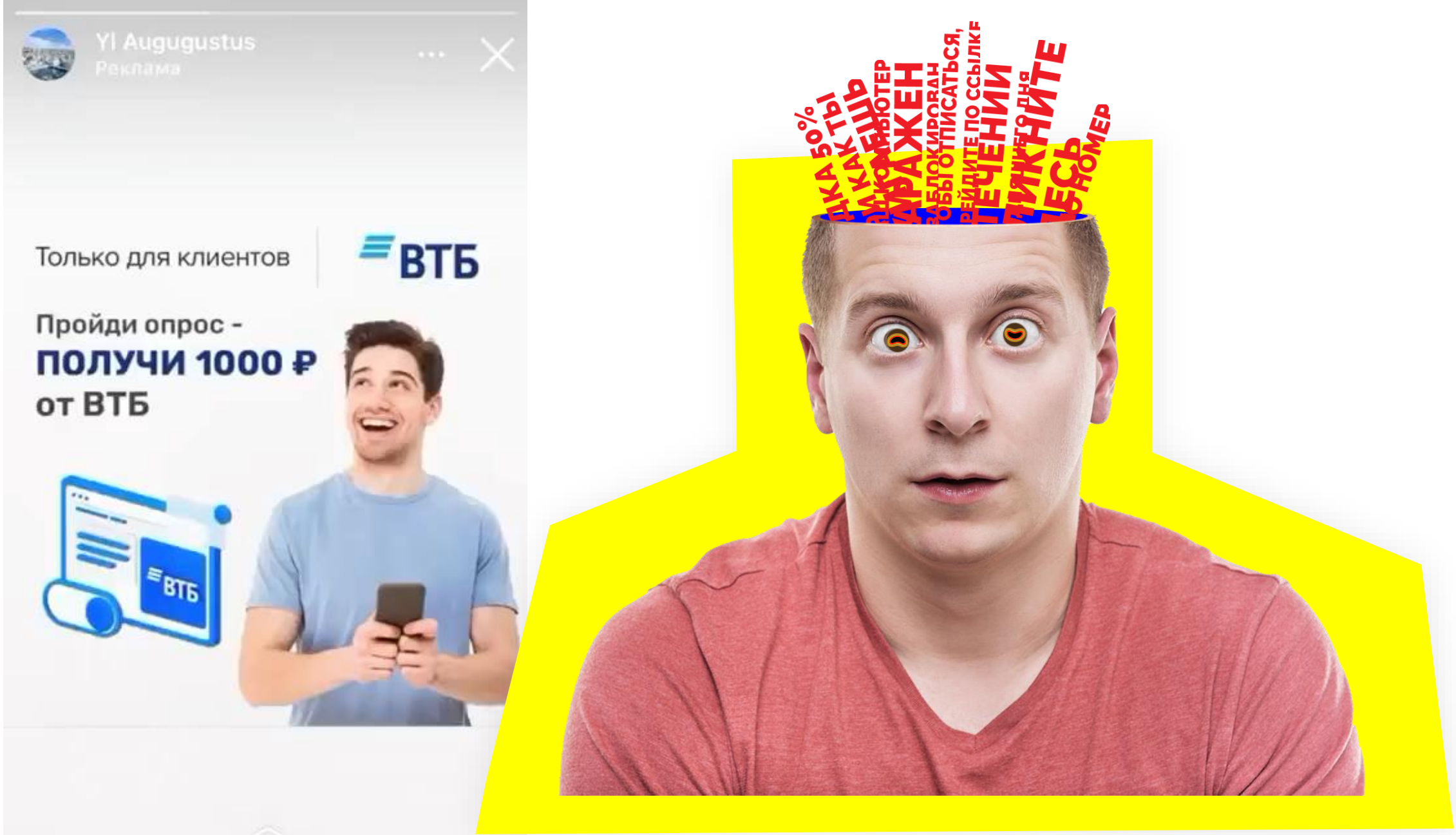


Pay

Добавьте кредитные, дебетовые или дисконтные карты в Apple Pay, чтобы безопасно платить в приложениях, на веб-сайтах и в магазинах, использующих технологию NFC.

Связанная с картой информация, геопозиция и сведения о настройках устройства и о том, как оно используется, будут отправлены в Apple. Apple может передавать эти данные вместе с учетной информацией эмитенту Вашей карты или банку для настройки Apple Pay.
Как осуществляется управление данными...

Дальше


Yl Augugustus
Реклама
Только для клиентов
ВТБ
Пройди опрос -
ПОЛУЧИ 1000 ₽
от ВТБ
ВТБ
Подробнее

ОТЧЕТ → GROUP-IB

ПРОГРАММЫ-ВЫМОГАТЕЛИ:

НОВЕЙШИЕ МЕТОДЫ АТАК Ш

Emotet чаще всего доставлялся жертве через фишинговые письма с вложенным документом Microsoft Word, ссылкой на такой документ или PDF-файлом со ссылкой:

Тактики вымогателя REvil

REvil — одно из современных вымогательских семейств, которые постоянно обнаруживаются в банках, госорганах, транспортных компаниях). Децентрализованный характер деятельности группы и её филиалов позволяют осуществлять одновременные проникновения и развёртывания с использованием множества техник и инструментов.

Операторы REvil обычно получают первоначальный доступ к ИТ-среде организаций через:

- фишинговые электронные письма,
- протокол удалённого рабочего стола (RDP) или похищенные учётные записи, скомпрометированные веб-сайты
- непропечённые уязвимости.

Группа REvil стояла за массовыми атаками с использованием вымогательского ПО в 2021 году. Поставщик мяса JBS и поставщик программного обеспечения для управления ИТ-системами Kaseya стали одними из самых громких жертв этой группы в текущем году. Производственные операции JBS были нарушены в США, Великобритании, Канаде и Австралии, и компания заплатила вымогателям 11 млн долларов США выкупа. Операторы REvil заразили почти

Психологические векторы атак

71% атак

Страх Ваш компьютер заражен и заблокирован. Кликните здесь.	**Невинма-тельонсть** www.sbernbank.ru www.gmall.com	**Раздражение** Чтобы отписаться, перейдите по ссылке.
Любопытство Смотри как ты отжигаешь на видео!	**Жадность** Скидка 50% при оплате прямо сейчас!	**Желание помочь** Ваш коллега потерял свои вещи. Дайте его номер.

Усилители реакции

Срочность

Отчет прислать сегодня до 15:00

Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

A

Zoom Meeting for [redacted] at January 28, 2021, 3:23:23 PM - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward Create New Move Mark Unread Categorize Follow Up Translate Read Aloud Zoom

Delete Respond Quick Steps Move Tags Editing Speech

Zoom Meeting for [redacted] at January 28, 2021, 3:23:23 PM

IM [redacted] MServer [redacted]

Reply Reply All F

Thu 1,

zoom

Dear [redacted]

You received a video cor

http://t.emails.[redacted].com/r/?id=hddbefa2,2c89d299,2c89d2c4&cid=dm413465&bid=232517538&p1=www.[redacted].com@c-hi.xyz?e=[redacted]#

Click or tap to follow link.

Re-view Invitation

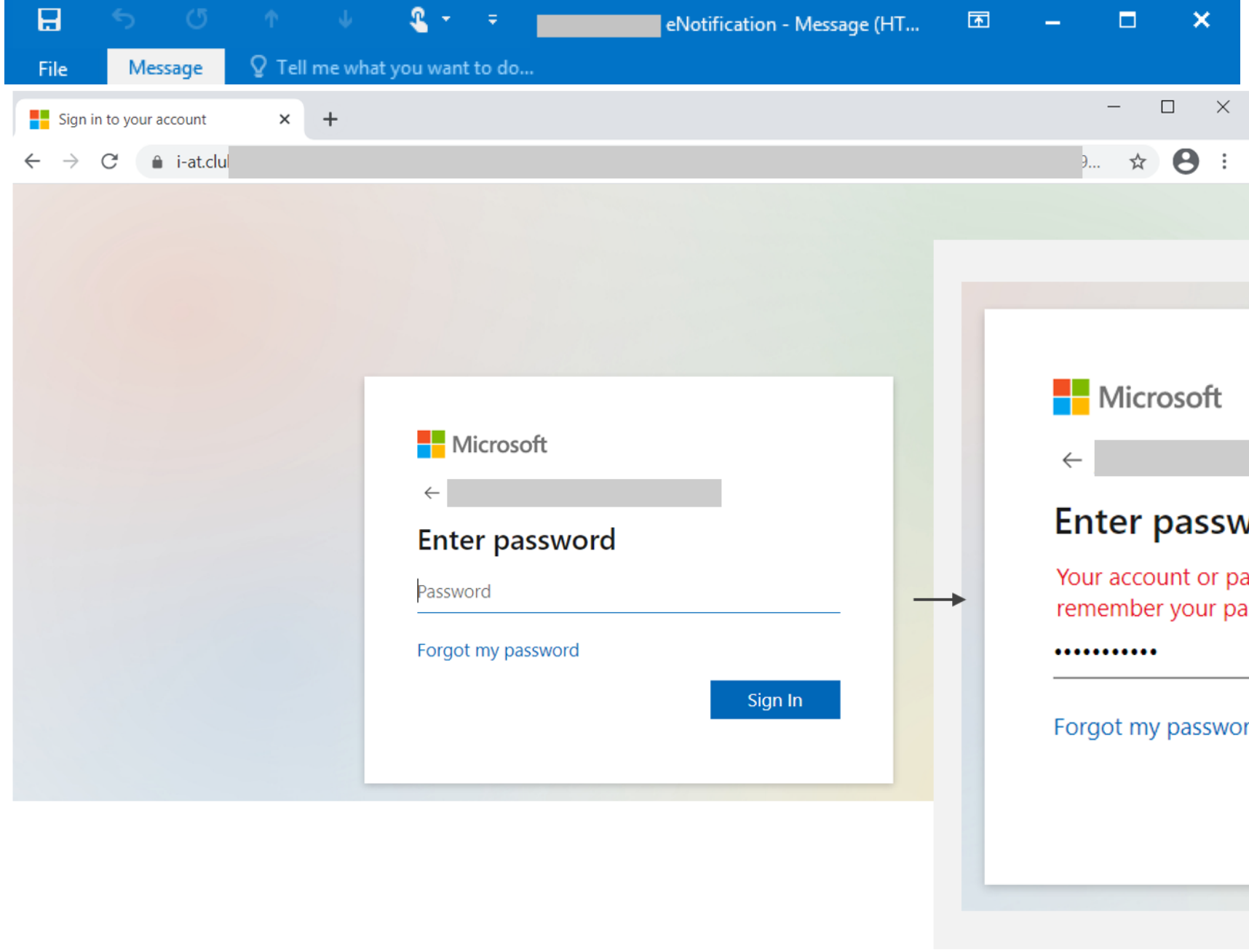
Team Zoom

Copyright ©2020 Zoom Video Communications, Inc. All rights

http://t.emails.[redacted].com/r/?id=hddbefa2,2c89d299,2c89d2c4&cid=dm413465&bid=232517538&p1=www.[redacted].com@c-hi.xyz?e=[redacted]#

Click or tap to follow link.

A


eNotification - Message (HT...
File
Message
Tell me what you want to do...
Sign in to your account
i-at.clu
Microsoft
Enter password
Password
Forgot my password
Sign In
Microsoft
Enter password
Your account or password is incorrect. If you don't remember your password, reset it now.
Forgot my password
Sign In
Thank you,

Психологические векторы атак

64% атак

Страх Ваш компьютер заражен и заблокирован. Кликните здесь.	**Невинма-тельонсть** www.sbernbank.ru www.gmall.com	**Раздражение** Чтобы отписаться, перейдите по ссылке.
Любопытство Смотри как ты отжигаешь на видео!	**Жадность** Скидка 50% при оплате прямо сейчас!	**Желание помочь** Ваш коллега потерял свои вещи. Дайте его номер.

Усилители реакции

Срочность

Отчет прислать сегодня до 15:00

Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

Внешняя

InnaS <info@zaometallniva.ru>

Блокировка карты!

Кому [redacted]

Анкетные данные.doc
397 KB

Добрый день!
В сязи с утерей телефона и ка
Копию паспорта, номера карт

Спасибо за понимание.

Авторитет

[redacted] Request (Protected View) - Word

File Home Insert Design Layout References Mailings Review View Tell me what you want to do... Sign in Share

Paste Calibri 11 Aa Find Replace Select

Clipboard Font Paragraph Styles Editing

AaBbCcDc ¶ Normal AaBbCcDc ¶ No Spac... AaBbC Heading 1

SECURITY WARNING Macros have been disabled. Enable Content

THIS DOCUMENT WAS MADE
ON WINDOWS 11 ALPHA

TO SAFELY OPEN THE DOCUMENT,
PLEASE PERFORM THE FOLLOWING STEPS

To view this content, please click "**Enable editing**" at the top in the yellow bar,
and then click "**Enable content**"

А

А как же «самые новые» технологии?

ВАЖНОЕ ЗАЯВЛЕНИЕ

от Олега Тинькова

Узнать Подробнее

15 октября 2021, 16:33 Технологии

Знакомый голос: мошенники с помощью дипфейка украли у банка $35 млн

Group-IB и Avast: количество мошенничеств с использованием дипфейка будет расти

Валерия Бунина

Желание помочь

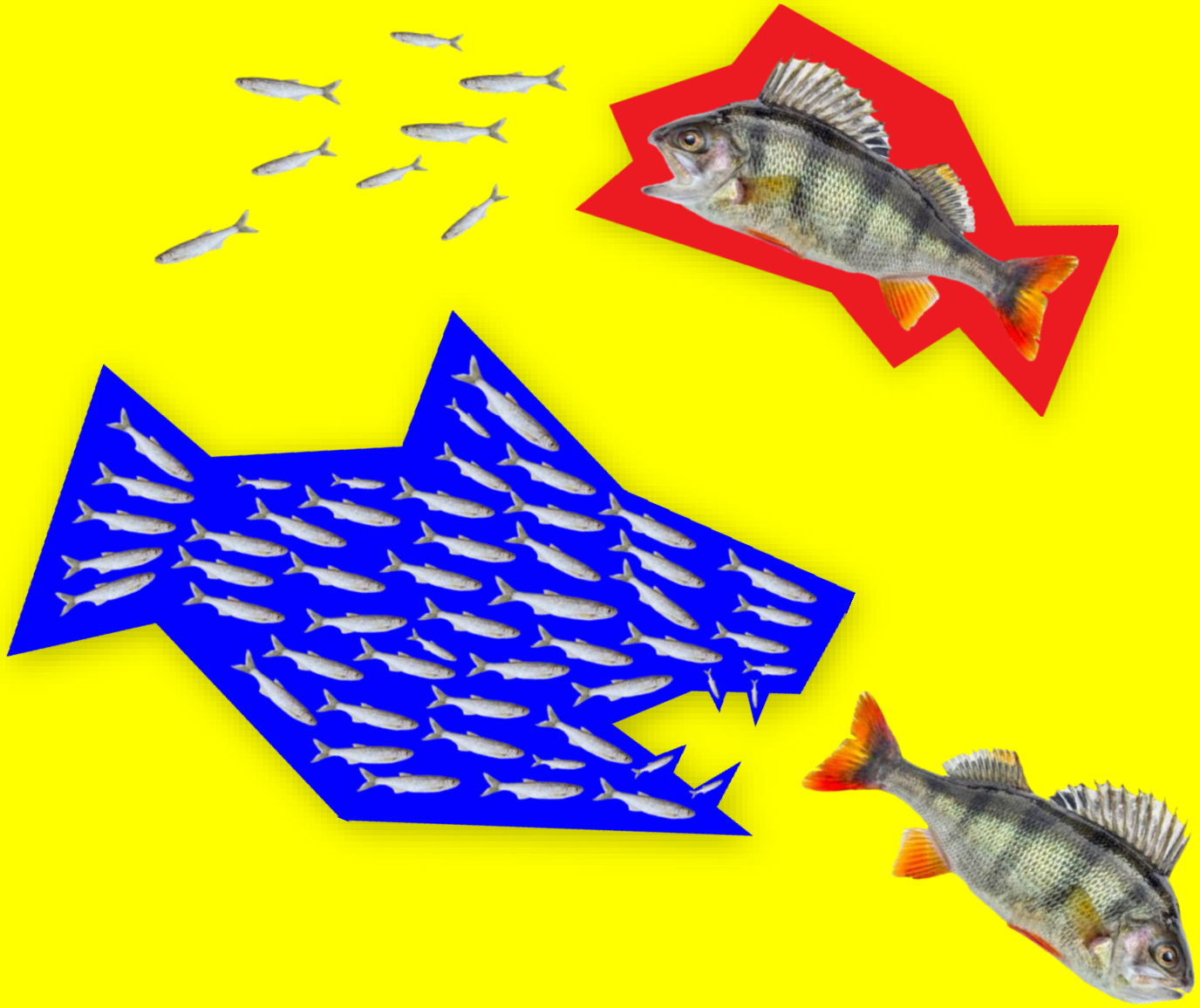
Срочность

Авторитет

В ОАЭ мошенники с помощью аудиодипфейка «клонировали» голос директора крупной компании и обманули менеджеров банка, которые перевели на их счет $35 млн. ИБ-эксперты утверждают, что в будущем такая схема может широко распространиться по всему миру. Можно ли распознать дипфейк и защитить себя от злоумышленников — в материале «Газеты.Ru».

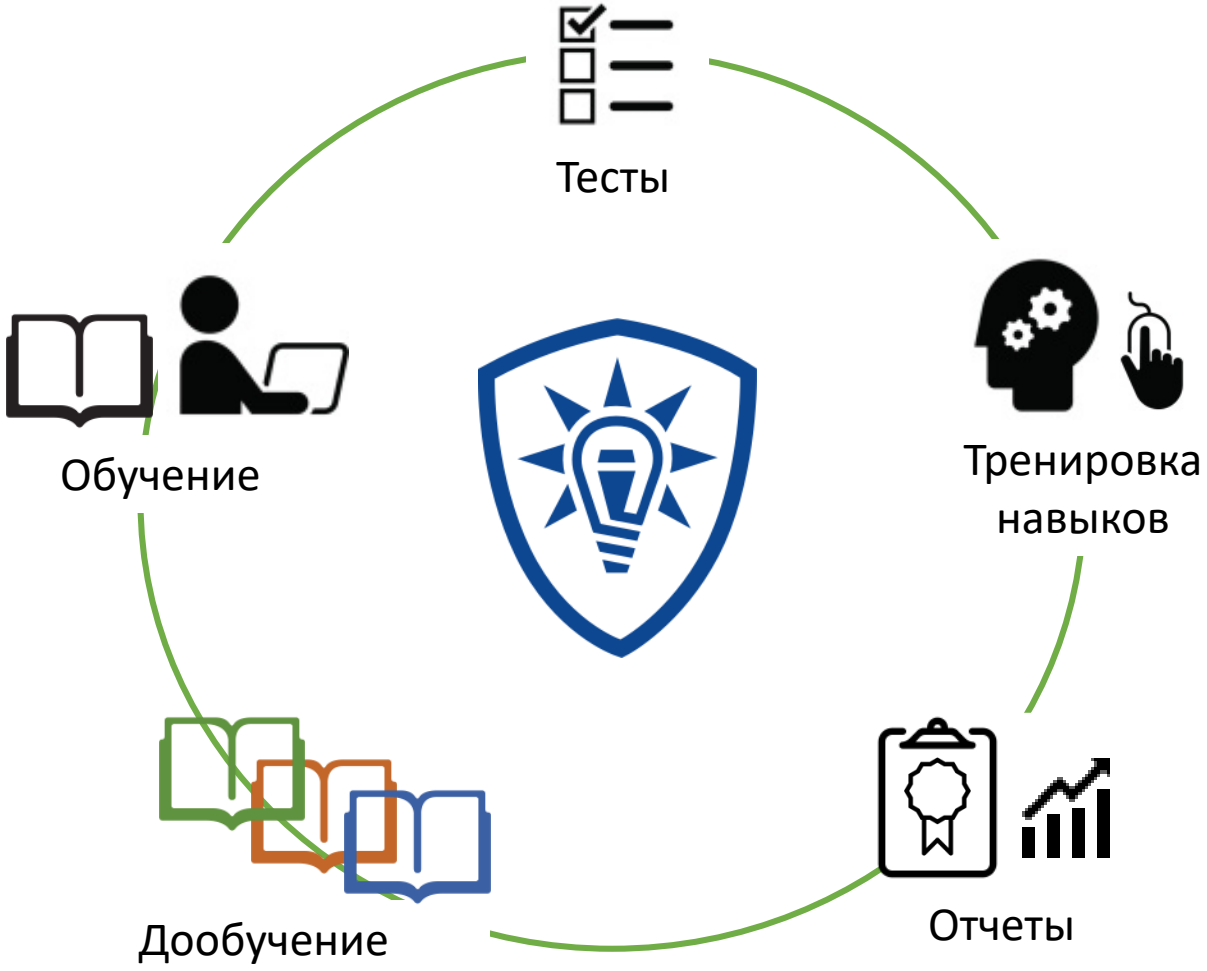
Мошенники смогли украсть у банка $35 млн в ОАЭ с помощью дипфейка, об этом сообщает Gizmodo.

2. Как защитить своих сотрудников в 2022 году




ДОБРО ПОЖАЛОВАТЬ НА КОРПОРАТИВНЫЙ ТРЕНИНГ ПО БЕЗОПАСНОСТИ.
DILBERT.COM @SCOTTADAMSSAYS
НИЧЕГО НЕ ТРОГАЙТЕ, НИКУДА НЕ ХОДИТЕ И НИ С КЕМ НЕ РАЗГОВАРИВАЙТЕ. НИКОГДА!
СПАСИБО, ЧТО ПРИШЛИ.
Scott Adams, Inc./Dist. by Andrews McMeel
НЕ МОЯ ВИНА, ЧТО Я УМЕЮ КРАТКО ИЗЛАГАТЬ.

Создайте непрерывный процесс



Обучение и тренировка навыков по безопасности

(Знания + Навыки) x Измерение

Ответить | Ответить всем | Переслать | Собрание | Больше — Ответить

Сообщение гр... | Ответить и уда... | Создать новое — Быстрые действия

Переместить | Правила — Переместить

Прочитано? | К исполнению — Теги

Адресная книга | Фильтр почты — Найти

Прочесть вслух — Речь

Отправить и получить почту — все папки — Отправка и получение

22:28

22:01

22:01

20:45

20:40

18:10

18:08

15:41

Счет на оплату

Ответить | Ответить всем

CA

Соколова Анна Дмитриевна <sokolova.vis@oat-group.ru> <sokolova.vis-oat-group.ru@templates.antph.ru>

Кому orlenko@antiphish.ru

Счет_8901_9 декабря 2019.docx
41 KB

Здравствуйте, Александр!

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

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

С уважением,

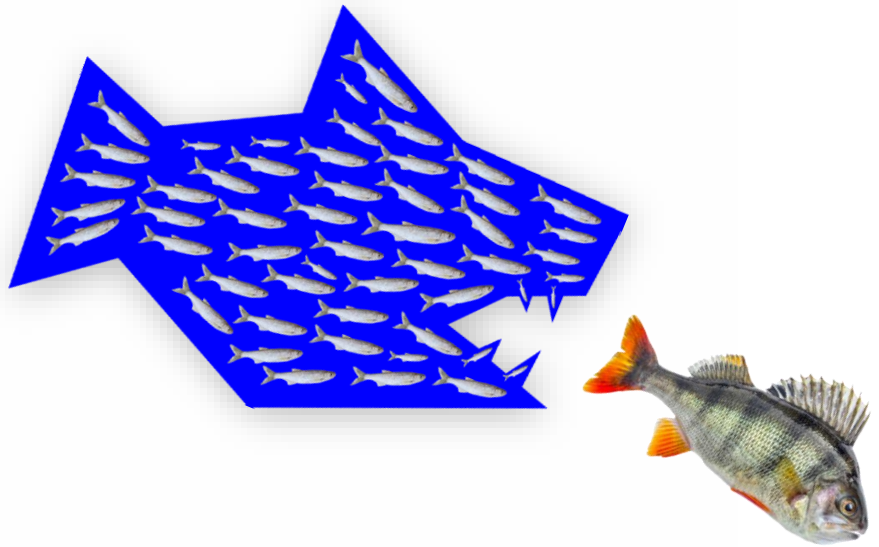
Менеджер по продажам

Соколова Анна Дмитриевна

Тел.: +7 (8482) 69-15-21

vazinter.ru

АКЦИОНЕРНОЕ ОБЩЕСТВО
ВАЗИНТЕРСЕРВИС



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

...ntph.ru запрашивает разрешение на:

Использование микрофона

Использование камеры

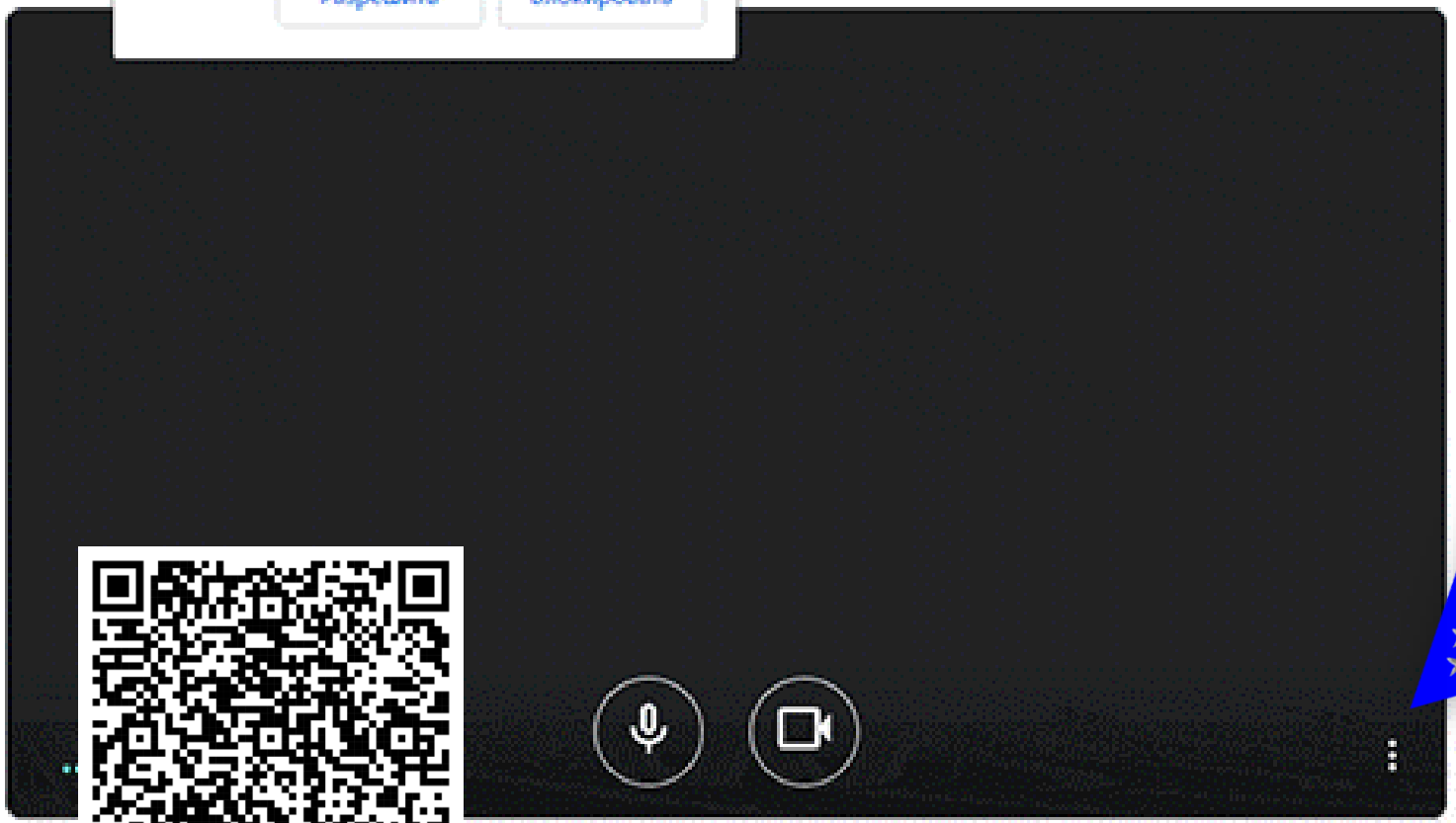
Разрешить | Блокировать

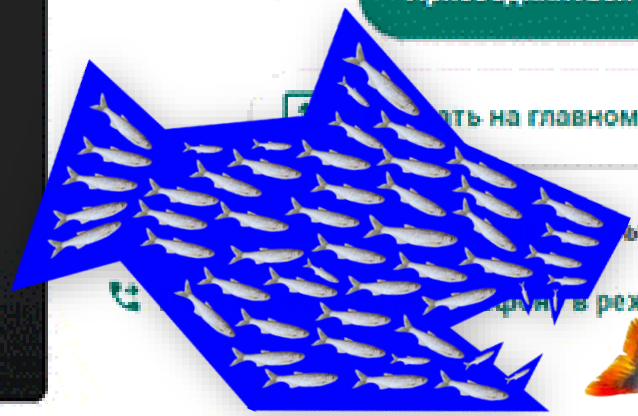
e.kravcova@antph.me
Алиса Кравцова

16.09.2020 Обсуждение про...

Подключено 2 человек

Присоединиться





Проверьте в новом году:

1. Как ваши сотрудники узнают об актуальных угрозах и правилах безопасности?

2. Как выглядят обучающие материалы для сотрудников?

3. Как автоматизирована тренировка навыков?

4. Как часто обновляются материалы и шаблоны целевых атак?

5. Как сотрудники могут помочь информационной безопасности?

АНТИФИШИНГ

www.antiphish.ru

ask@antiphish.ru