prpartner

Как пиар в ИБ помогает сейлз и маркетинг-менеджерам

Инна Анисимова

prpartner

- Более 20 лет в PR, маркетинге, рекламе,
- 600 тренингов по PR, медиатренингов,
- В 2018 году окончила Global Executive MBA в бизнес-школе IESE,
- **PR Partner:** топ-40 PR-агентств (HP2K, 2022).
- Оборот 184 млн руб., 30 сотрудников, работа с международными сетями.

@inna_prpartner
@marketingna5

Подход: говорим не о продуктах, а о проблемах в ИБ

- Говорить про свой продукт — часто скучно, рекламно и отталкивает. Или интересно совсем узкой ИТ-аудитории. Не говорите про продукт, рассказывайте про ситуацию в мире, повестку дня. Аргументируйте свои слова!
- *«Наше уникальное, первое в мире решение защитит вас от всех типов угроз. В нем есть много фильтров и уровней защиты, и сейчас мы вам расскажем, почему они обязательно нужны всем пользователям мобильных устройств»* — плохой посыл для широкой аудитории.
- *«В России за два месяца увеличились кражи с помощью мобильного вредосного ПО, а в Москве в три раза»* — уже лучше.

ТАСС

Эксперты предупредили о приложениях, списывающих несоразмерно большие деньги за подписку

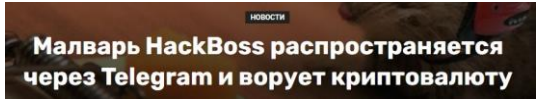
По оценкам SensorTower, такие приложения были загружены в совокупности более 1 млрд раз

МОСКВА, 24 марта. /ТАСС/. Компания Avast, специализирующаяся на цифровой безопасности, обнаружила более 200 новых условно бесплатных приложений в App Store и Google Play, которые списывают несоразмерно крупные суммы с пользователей за продление подписки. Об этом ТАСС рассказали в компании.

Речь идет о так называемых fleeceware-приложениях. Так, пользователю предлагают скачать приложение на бесплатный пробный период, чаще всего - на три дня. Затем приложение автоматически списывает несоразмерно высокую плату за подписку.

Какие данные нужны для крутого PR

- Исследования. И очень здорово, если они будут масштабные.
- Локальные данные. Чем локальнее, тем лучше: для региона, для стран, областей, городов. Хотите хороший (и бесплатный!) региональный PR? Будьте готовы рассказать, от какой малвари пострадали жители конкретного региона.
- Цифры, кейсы. Все любят истории с цифрами.
- Деньги. То, что всегда будет волновать людей. Сколько в среднем теряет человек после атаки?
- Популярные программы и вещи. Ищите и изучайте то, чем пользуется много людей. Кофемашины, мессенджеры, смартфоны. Есть уязвимость в популярном мессенджере или умном гаджете? Отлично.
- Результаты. И конкретный сравнительный анализ: а что изменилось за месяц? За полгода? Как изменились атаки? Тактика киберпреступников?



Эксперты Avast обнаружили инструмент для кражи криптовалюты HackBoss, который распространяется в Telegram под видом бесплатной малвари для начинающих. Создатели HackBoss уже похитили более 500 000 долларов у «начинающих хакеров», которые попались на эту уловку.

Какие исследования нужны?

- Берите то, что интересует широкий круг людей. Не берите одну узкую категорию респондентов.
- Ищите драму. Когда все хорошо — это скучно. Не беремся оценивать этичность этого утверждения, но даже вы скорее прочитаете «угрожающую» новость, чем мирную и позитивную.
- Идеально, если у вас исследование от 1500 респондентов. Это требование информационных агентств. Если меньше, будьте готовы объяснить, как отбирали респондентов и почему это релевантная подборка.
- Главный упор — на Россию. Многие ведущие СМИ не берут исследования, где нет респондентов из РФ (или где их слишком мало).
- Нет идей? Идите к лояльному редактору в топовые СМИ и спрашивайте, что он хотел бы получить. Но будьте готовы сразу обсуждать условия — скорее всего, он захочет материал под эмбарго или на эксклюзиве.

Коммерсантъ

$ 61,09 ▲ € 61,25 ▲ ¥ 8,40 ▲ IMOEX 2185,70 ▼ Валютный прогноз Военная операция на Украине Мобили

Скандалы с персональными данными

12.03.2021, 00:20

Видео без ограничений

В России обнаружились камеры наблюдения с общедоступными данными

Более 6,3 тыс. камер видеонаблюдения, размещенных в том числе на объектах критической инфраструктуры и промышленных предприятиях России, имеют откры IP-адреса, а доступ к ним может получить любой желающий. На базе камер с открыт злоумышленники могут организовать нелегальную систему видеонаблюдения или использовать их как вычислительный ресурс, предупреждают эксперты.

71K

5

2 мин.

Порядка 6,3 тыс. камер видеонаблюдения, расположенных на электростанциях, промышленных предприятиях, заправках и в системах «умных» домов в России, оказались уязвимы, рассказали "Ъ" в компании Avast со ссылкой на данные поисковой системы по интернету вещей Shodan.io. IP-адреса этих камер открыты, и к ним могут получить доступ киберпреступники, говорят эксперты.

> **«К системе большинства таких камер можно получить доступ бе имени пользователя и пароля, либо пароль к ним установлен по умолчанию»,— пояснили в Avast.**

Россия, по данным Shodan.io, находится на пятом месте по числу камер видеонаблюдения с открытым IP. На первых строчках располагаются Вьетнам, Тайвань Южная Корея и США. Во всем мире около 124 тыс. камер имеют такую уязвимость.

Нет ресурсов для самостоятельной аналитики?

- Используйте сервисы проведения исследований (Яндекс.Взгляд, сервисы Tiburon Research). Вы не получите данные угроз, но сможете понять риски и опасения бизнеса и обычных людей;
- Просматривайте отчеты авторитетных международных компаний и исследования крупных компаний по информационной безопасности. Не стесняйтесь использовать эти данные и предлагать их спикерам.

РИА НОВОСТИ

Эксперты предупредили об утечке данных миллионов Android-смартфонов

МОСКВА, 25 мая — РИА Новости. Данные примерно 100 миллионов пользователей Android -устройств были раскрыты из-за ошибки в нескольких популярных приложениях в магазине приложений Google Play. К такому выводу пришли исследователи компании Check Point Software Technologies, которая занимается изучением кибербезопасности.

Как выяснили эксперты, 23 популярных приложения неправильно обрабатывали пользовательские данные из-за недоработанной синхронизации с облачными базами данных. Среди такого софта называются Astro Guru, iFax и Screen Recorder.

А как писать?

- Просто. Будьте готовы вникнуть в механизм работы уязвимости или вредоносной программы. И объяснить это на пальцах. Если это не интересно вам, почему это должно быть интересно вашим читателям и СМИ?
- Коротко. Будем честны — длинные лонгриды любят только избранные СМИ. Не тратьте ресурсы спикеров, готовьте длинные рассказы только для самых ярких историй.
- Интересно. Рассказывайте истории: например, как работают хакерские группировки, как взламывают системы. Иногда это круче детектива! Заодно покажете, насколько хорошо вы разбираетесь в теме.
- Оперативно. Инфоповоды в ИБ очень быстро тухнут, поэтому и пиарщики должны отлично разбираться в теме (знать уязвимости, особенности работы вредоносных программ) и спикеры должны уметь общаться с медиа.

газета.ru

Вирусный рост. Поддельные справки о вакцинации подорожали в несколько раз

ИБ-эксперты Check Point связали с «омикроном» рост цен на фейковые сертификаты

Цены на поддельные сертификаты о вакцинации и результаты ПЦР-тестов во всем мире за последние несколько недель выросли до 6 раз, выяснили специалисты ИБ-компании Check Point. Россию новая тенденция тоже не обошла стороной. Эксперты связывают резкий скачок цен с быстрым распространением штамма «омикрон» — из-за него во многих странах снова ужесточился эпидемиологический контроль, а следовательно, возрос спрос и на медицинские справки.

Совет 1. Говорите на актуальные темы

МОСКВА, 1 ноя — ПРАЙМ. Чем популярнее мессенджеры, тем больше хакерских атак приходится преодолевать его разработчикам. Поэтому мы чаще всего видим новости о том, что в WhatsApp выявлена очередная критическая уязвимость, благодаря этому его можно называть самым опасным из-за количества зафиксированных взломов или угроз, рассказал агентству "Прайм" эксперт по информационной безопасности Лиги Цифровой Экономики Андрей Слободчиков.

Эксперт рассказал, как защитить переписки в мессенджерах от посторонних

"Например, обнаруженные недавно две уязвимости в WhatsApp CVE-2022-36934 и CVE-2022-27492, которым присвоили уровни критичности 9,8 и 7,8 из 10 соответственно. Они позволяли запустить произвольный код на устройстве и получить к нему неограниченный доступ", — рассказал эксперт.

- Масштаб: мессенджером пользуются миллионы россиян;
- Есть драма;
- Примеры;
- Все коротко и по делу;
- Получили 169 перепечаток.

Статьи в ИА очень часто имеют большой охват и много перепечаток.

Говорите на актуальные темы

газета.ru

Фальшивые сайты, фиктивные продавцы: как обманывают пользователей «Юлы» и «Авито»

Эксперты объяснили, как распознать фишинговый сайт на досках объявлений

Технический директор Check Point Software Technologies в России и СНГ Никита Дуров отметил, что кибермошенники часто используют в фишинговых атаках известные бренды, например, имитируют официальный сайт с помощью похожих доменов и URL-адресов, а также копируют дизайн.

«Совершайте покупки только на тех сайтах, которые используют протокол SSL (Secure Sockets Layer). В URL-адресе таких сайтов вместо «http» указано «https», а слева от адресной строки или снизу в строке состояния, как правило, появляется значок в виде закрытого замка. Если замка нет, вводить данные своей карты однозначно не стоит. Остерегайтесь сайтов с ошибками в названии или с непривычным доменом верхнего уровня, например «.co» вместо «.com», скорее всего это «копия» сайта для фишинговых рассылок. Предложения на поддельных сайтах могут быть даже выгоднее, чем на официальных — так хакеры заманивают покупателей, чтобы украсть их данные», — отмечает Дуров.

- Масштаб: досками объявлений пользуются миллионы россиян;
- Есть драма;
- Примеры;
- Все коротко и по делу.

Дедлайны запросов Газеты.ру очень короткие! Нужно реагировать быстро, давать конкретику без воды.

Совет 2. Ищите локальные данные

prpartner

LENTA.RU

15:12, 25 мая 2021 Интернет и СМИ

Россия вошла в лидеры антирейтинга по цифровой безопасности

Эксперты компании Avast, специализирующейся на цифровой безопасности, составили рейтинг стран, в которых больше всего распространены шпионские приложения. Как сообщается в пресс-релизе, поступившем в «Ленту.ру», Россия заняла в нем предпоследнее место.

Фото: Ирина Бужор / «Коммерсантъ»

В общей сложности Avast изучила данные из 15 стран мира. Оказалось, что чаще всего со шпионским программным обеспечением сталкивались пользователи из Индии. Россия и США заняли второе и третье места соответственно. В пятерку лидеров вошли также Нидерланды и Австралия. При этом в России, по данным исследователей, количество установок подобных приложений, в том числе незаметно от жертвы, только за первый квартал 2021 года выросло на 390 процентов по сравнению с аналогичным периодом прошлого года.

- Локальные данные;
- Есть драма;
- Примеры;
- Все коротко и по делу.

Исследование упаковали в формат пресс-релиза, сделали упор на локальных данных. Задача PR-команды — не просто достать данные, а правильно их подать.

Совет 3. Делитесь исследованиями!

prpartner

ТАСС

1 февраля, 03:01

Число криптомайнеров в мире в конце 2021 года выросло на 40%

© Александр Рюмин/ТАСС

Одним из самых активных криптомайнеров в последнем квартале был CoinHelper

МОСКВА, 1 февраля. /ТАСС/. Количество криптомайнеров в мире в конце 2021 года выросло на 40% на фоне роста стоимости биткойна, сообщили ТАСС в пресс-службе компании-разработчике антивирусного ПО Avast.

- Локальные данные;
- Актуальная тема: тогда о крипте говорили все;
- Есть драма;
- Примеры;
- Все коротко и по делу.

Рассылка пресс-релиза с предварительным питчигом с акцентом на повестке — рост стоимости биткойна. Челлендж: оперативно вычленить из массивов данных самое главное, убрать лишнее и перевести на рус.

Совет 4. Используйте повестку

prpartner

DIGITAL Интернет Технологии Гаджеты Игры Видео

14.06.2021 01:00 Рубрика: Товары и цены Интернет

Как отличить фейковый интернет-магазин от настоящего

Иван Черноусов

Самые большие скидки на товары магазины устраивают летом и зимой. Мимо них не могут пройти и злоумышленники, которые активизируются в это время. Чаще всего для "наживы" используются сайты известных магазинов. Например, в феврале этого года россиянам предлагали купить iPhone и PlayStation по рекордно низкой цене, однако потом этот магазин был закрыт.

ЧИТАЙТЕ НАС НА DZEN.RU
Сделайте RG.RU вашим источником новостей
Добавить

Ссылки на такие фейковые магазины могут распространяться через фишинговые письма. Во время распродаж бренды обычно отправляют своим покупателям гораздо больше писем с информацией об акциях и спецпредложениями. Но вместе с письмами из реальных магазинов пользователи могут получить письма от киберпреступников. И они будут содержать ссылки на вредоносные сайты, имитирующие оригинальные сайты магазинов.

"Обратите внимание на адрес электронной почты, с которого отправлено письмо, а не только на имя отправителя. Посмотрите, кому оно адресовано: многие фишинговые кампании - массовые. Такое вредоносное письмо не будет обращено персонально к вам, вместо этого будет общее приветствие, например, "Дорогой клиент". При этом уважающий себя магазин, если вы подписывались на его рассылку, скорее всего обратится к вам по имени. Проверяйте грамматику, язык - нормальный магазин не будет рассылать плохо

ВЛАСТЬ
В полиции рассказали, как не стать жертвой мошенников в Сети

"Обратите внимание на адрес электронной почты, с которого отправлено письмо, а не только на имя отправителя. Посмотрите, кому оно адресовано: многие фишинговые кампании - массовые. Такое вредоносное письмо не будет обращено персонально к вам, вместо этого будет общее приветствие, например, "Дорогой клиент". При этом уважающий себя магазин, если вы подписывались на его рассылку, скорее всего обратится к вам по имени. Проверяйте грамматику, язык - нормальный магазин не будет рассылать плохо подготовленные электронные письма", - говорит Алексей Федоров, глава представительства Avast в России и СНГ.

ВЛАСТЬ
В полиции рассказали, как не стать жертвой мошенников в Сети

Большинство людей не сразу могут понять, что перед ними фальшивый сайт: современные фишинговые сайты мастерски маскируются под настоящие. Обратите внимание на то, как оформлен сайт, нет ли опечаток на страницах или в адресе сайта.

- Привязка к актуальному поводу: летним распродажам;
- Драма: в период распродаж риск нарваться на мошенников ощутимо возрастает;
- Есть примеры;
- Статья от топ-менеджера;
- Все коротко и по делу.

Совет 5. Говорите просто

prpartner

газета.ru

05 июня 2021, 03:51 Новости

Эксперт рассказал, чем опасен взлом домашнего Wi-Fi

Если злоумышленники взломают вашу домашнюю сеть Wi-Fi, они без труда могут получить доступ ко всем личным и критически важным данным, а также ко всем вашим устройствам, подключенным к сети, рассказал «Газете.Ru» ИБ-евангелист компании Avast Луис Корронс.

«Как правило, подключенные к сети устройства защищены от базовых киберугроз из интернета благодаря наличию роутера. Но если киберпреступник получит доступ к сети, скомпрометированы будут все без исключения подключенные к ней устройства», — пояснил эксперт.

По мере того, как наши дома становятся все более «умными», сталкеры все чаще используют домашние IoT-устройства, чтобы шпионить за своими жертвами и атаковать их, сообщил Корронс. Если в вашем умном девайсе или Wi-Fi-роутере есть уязвимости (слабый пароль, устаревшее программное обеспечение) сталкер может легко получить доступ, например, к камерам и динамикам умного дома, что даст ему возможность наблюдать и даже разговаривать с вами.

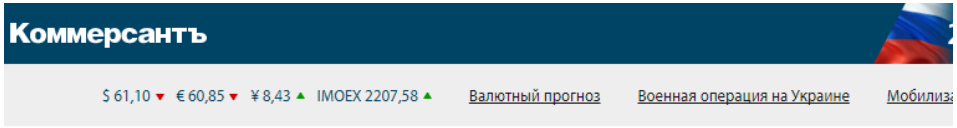
«При этом далеко не всегда возможно сразу узнать о взломе — хакеры могут месяцами наблюдать за жизнью жертвы, собирать данные о ней, не раскрывая своего присутствия», — заявил представитель Avast.

- Драма: взлом Wi-Fi приведет к катастрофе, и человек может долгое время не знать, что его взломали;
- Есть примеры;
- Статья от топ-менеджера;
- Все коротко и по делу.

Челлендж: Нужно хорошо ориентироваться в теме, быстро читать и знать, где в материалах компании находится информация. Без этого нереально уложиться в очень короткий дедлайн медиа.

Совет 6. Показывайте масштаб проблемы

prpartner



Информационная безопасность

15.12.2021, 21:32

Хакеры освоили новый язык

Уязвимость Log4j затронула почти половину российских компаний, работающих с Java

Более 48% российских корпоративных сетей затронула критическая уязвимость библиотеки Log4j, и «множество попыток» ее эксплуатации было зафиксировано компаниями по кибербезопасности. Уязвимость касается любых приложений на языке Java, поэтому масштаб угрозы велик, тем более что использовать ее очень просто, говорят эксперты. Разработчик уязвимой библиотеки Apache Software Foundation уже заявил, что выпустил два обновления безопасности.

- Драма: может нарушиться работа огромного числа компаний;
- Есть локальные данные: данные именно для российских компаний;
- Есть примеры;
- Все коротко и по делу.

Более 48% корпоративных сетей в России затронула опасная уязвимость Log4j (Log4Shell), рассказали «Ъ» в Check Point.

- В частности, в России она коснулась 72% телеком-компаний, 58% производств и 57% предприятий розничной и оптовой торговли, сообщил руководитель отдела анализа угроз Check Point Software Technologies Лотем Финкельстин.

Совет 7. Комментируйте актуальные темы

prpartner

Коммерсантъ

$ 61,07 ▲ € 61,27 ▲ ¥ 8,40 ▲ IMOEX 2188,40 ▼ Валютный прогноз Военная операция на Украине Мобил

Радио «Ъ FM»
06.01.2022, 17:08

Биометрия переходит в приложение

Какие услуги станут доступны сдавшим отпечатки пальцев

Сдать биометрию для Госуслуг можно будет через специальное приложение без визита в банк или МФЦ. О планах создать такое ПО заявили в Минцифры. По словам главы ведомства Максута Шадаева, пользователей нужно мотивировать делиться такими данными и упростить для них этот процесс. Господин Шадаев уточнил, что набор услуг, который станет доступен после фиксации биометрии в приложении, будет ограничен. Например, они смогут заменить паспорт при предъявлении QR-кода. Будет ли это эффективно? И насколько это безопасно? Расскажет Александр Мезенцев.

Какие услуги станут доступны после сдачи биометрии? По данным "Ъ", это некоторые банковские операции, проезд в метро и МЦК и заключение абонентских договоров. Сейчас данными можно поделиться в МФЦ или в отделениях банков. И судя по всему, процесс идет слишком медленно. Власти больше двух лет добиваются того, чтобы граждане могли сдавать биометрию самостоятельно. И приложение выглядит перспективно, говорит глава представительства компании Check Point Software Technologies в России и СНГ Василий Дягилев: «Сейчас многие люди испытывают какой-то животный страх перед тем, чтобы прийти в какое-то специализированное место, подписать кучу бумаг, сесть перед сканером, куда-то поставить свои отпечатки пальцев. Когда им дадут достаточно легкий и удобный способ, как они в обычной жизни привыкли разблокировать свой телефон, пользоваться биометрическими данными, то желающих использовать такую услугу, действительно, станет намного больше».

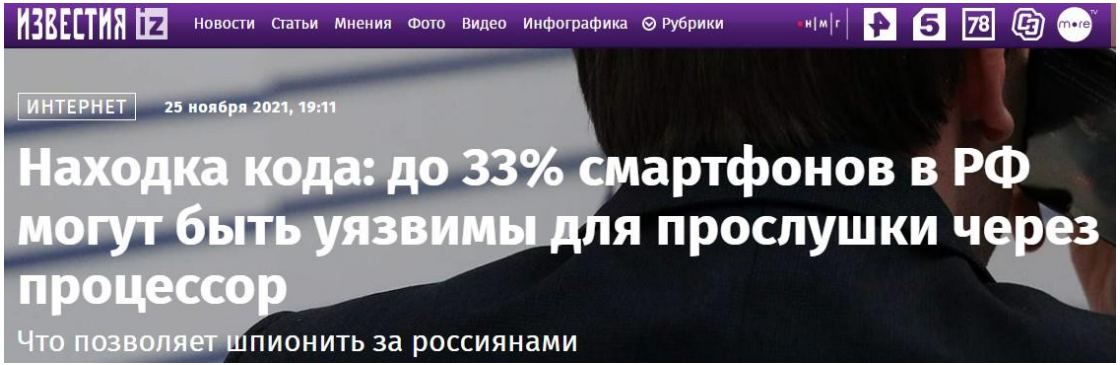
Как государство внедряет новые IT-решения

- Актуальная тема для россиян,
- Быстрый ответ спикера для радио Коммерсантъ FM.

Коммерсантъ FM, Бизнес FM, Вести FM хотят комментарий напрямую от спикера голосом и в течение часа. А еще лучше — в течение 10-15 минут. Важно готовить спикеров!

Совет 8. Говорите простым языком

prpartner



Россиянам может угрожать прослушка их телефонных разговоров через процессоры MediaTek, сообщили «Известиям» в Check Point Research. Специалисты этой компании обнаружили в процессорах тайваньского производства уязвимости, которые при определенных сценариях позволяют злоумышленникам прослушивать их звонки через приложения. Использовать эти дефекты чрезвычайно сложно, считают эксперты, но такая возможность есть. По данным аналитиков, доля смартфонов на уязвимых процессорах MediaTek может достигать 33%. Они используются преимущественно в устройствах низкой и средней ценовых категорий — от 8 до 30 тыс. рублей.

- Локальные данные: Россия;
- Цифры: 33%;
- Драма: треть смартфонов могут прослушиваться.

Исследование в формате пресс-релиза.
Челлендж: сложное исследование для перевода, много технических деталей. Важно разобраться в теме, чтобы быстро и доступно отвечать на вопросы журналистов.

Совет 9. Проверяйте, минимум дважды

!Перепроверяйте информацию:

- Написание банков и любых других организаций. Особенно, если работаете с переводом исследований. Многие банки по всему миру имеют похожие названия.
- Число затронутых и пострадавших. Это часто путают и исследователи, и пиарщики. В первом случае речь идет о тех, кто столкнулся с атакой. Во втором — кто от нее пострадал.
- Нет ли пострадавшей организации в числе ваших клиентов? Или партнеров. Есть сомнения? Советуйтесь с юристами.

Как маркетологи и сейлзы могут использовать PR-контент?

prpartner

- Аргументация для заказчиков — почему предлагаем именно это? Еще раз подчеркнуть необходимость использования решений, возможность легко делать дополнительные продажи.
- Демонстрация экспертизы и ресурсов: мы в курсе всех угроз, мы регулярно проводим исследования, мы знаем, как с этим бороться.
- Повышение репутации: компания готова вкладываться в такие исследования, развиваться, совершенствоваться.
- Примеры для выступлений на круглых столах и конференциях. Например, в ИБ-кругах любят и уважают круглые столы-эфиры Anti-Malware. Круто, когда спикер делится данными компании.

Как пиарщик может помочь сейлзам и маркетингу?

prpartner

- Делайте еженедельные рассылки: делитесь дайджестом ваших новостей.
- Если вы работаете в международной команде, делитесь локализованными материалами.
- Готовьте контент для медиа и презентаций спикеров, основанный на вопросах клиентов.

Как работать со спикерами?

prpartner

Медиатренинг — подготовка спикеров к эффективному общению с журналистами.

7 базовых упражнений:

- Самопрезентация
- Storytelling
- Работа с негативом («И это хорошо, потому что…»)
- «Бомба»
- Стрессовое интервью
- Обмен ролями
- «Кто ты?»

Подготовка спикеров

Самопрезентация — короткий рассказ о себе с деталями, которые могут быть интересны аудитории (журналист, партнер, инвестор, клиент и пр.).

СХЕМА: прошлое/настоящее/будущее

Подготовка спикеров

«Кубики историй», «Моя большая выставка» — детские игры, которые можно использовать для тренировки сторителлинга.

Правила: рассказ на ассоциациях, дополненный деталями, с позитивным концом.

Подготовка спикеров

prpartner

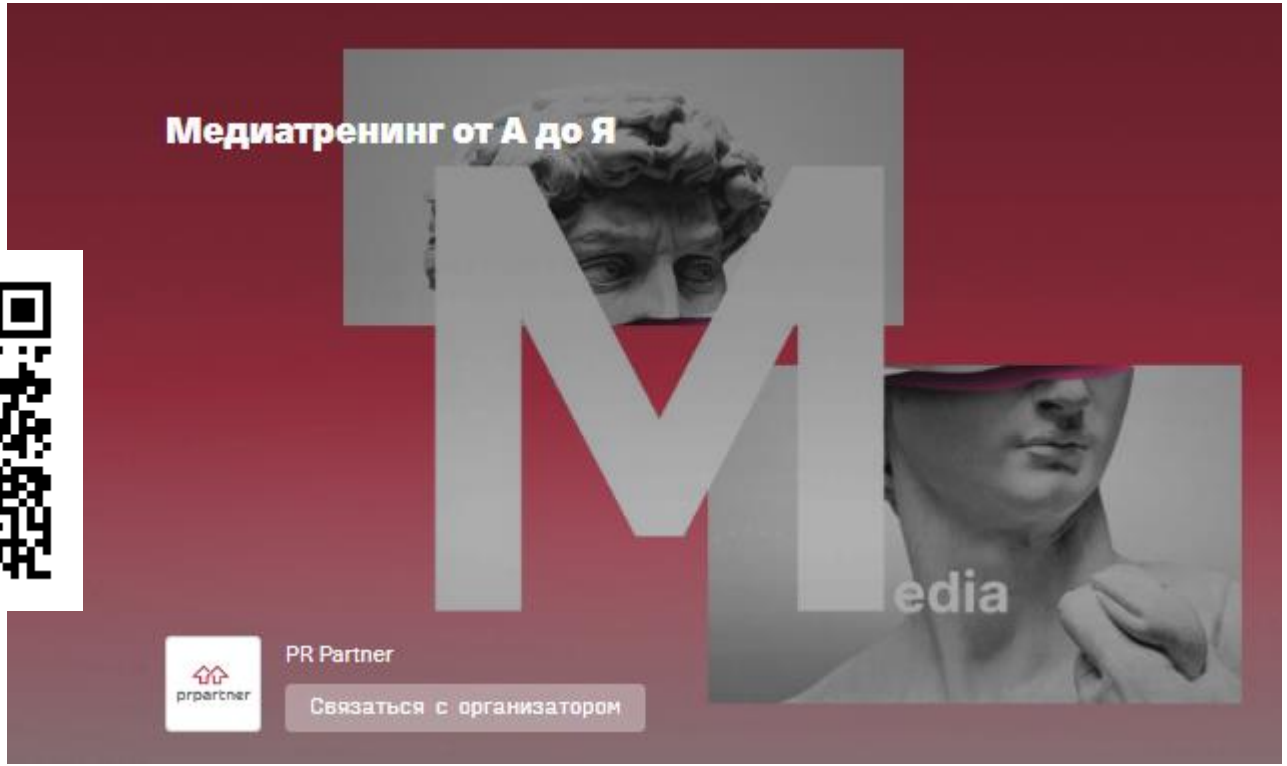
«Бомба» — упражнение для подготовки ответов на неудобные вопросы или тренировки прямого эфира.

1. Чем занимается ваша компания?
2. Почему выбрана эта ниша?
3. На чем зарабатываете деньги?
4. Структура прибыли компании?
5. Какова прибыль? Что на нее влияет?
6. Кто ваши конкуренты? Назовите их?
7. Чем конкуренты лучше вас?
8. Почему вы еще не первые?
9. Кто целевая аудитория?
10. Как вы ее определили?
11. Вы делали исследования рынка? Какие?
12. Кто основные акционеры? Они довольны прибылью?
13. Как вы переживаете кризис?
14. Насколько упала прибыль в этом году?
15. Сколько сотрудников работает внутри компании?
16. Вы работаете с временным персоналом?
17. Сколько офисов у компании и где они? Почему именно там?
18. Портрет сотрудника, опишите его?
19. Кто ваши партнеры?
20. Как вы нанимаете людей?
21. Какая атмосфера внутри?
22. Какая у вас текучка?
23. С кем из чиновников у вас налажены отношения?
24. С кем не сложилось? Почему?
25. В каких ассоциациях состоите? Почему именно в них?
26. Как компания будет развиваться в ближайший год? 5 лет?
27. Где можно посмотреть стратегию развития?

Спикер-мечта? Легко!

prpartner

18 ноября



Готовы к общению с медиа напрямую?

prpartner

Спасибо!

Мои контакты:

Инна Анисимова
inna@prpartner.ru
+7 926 118 94 22
@inna_prpartner
@marketingna5