TRImedia

#physical security #psychological security #digital security

Где надо провести черту?

Мы готовимся к новому году, подстраиваем стратегии, строим планы и, возможно, намереваемся расширить команду или же запустить новые формы взаимодействия со своим сообществом. **Но как организовать процесс включения нового сотрудника в состав команды, проявив при этом бдительность, заботу о внутренней и внешней безопасности и о благополучии команды?** Все эти аспекты мы обсудили с сотрудницей по вопросам безопасности социальных сетей в Deutsche Welle Ясминой аль-Ганнаби.

Ясмина аль-Ганнаби

сотрудница по вопросам безопасности социальных сетей в Deutsche Welle

Как происходит процесс предоставления журналистам доступа к рабочему месту с учетом аспектов безопасности?

В таком случае речь идет о двух важных уровнях. Первый относится к доступу к корпоративным аккаунтам для тех лиц, которым поручено быть администраторами сообществ в сети или же производить контент, тогда как второй предполагает сохранение безопасности их личных аккаунтов.

Обычно мы рекомендуем департаментам обеспечить сотрудникам доступ только через предлагаемые на платформах системы управления, такие как Meta Business Suite или YouTube Creator. Только в частных случаях сотрудники, ведущие прямые эфиры или которые хотят использовать функцию сотрудничества в Instagram, могут заходить непосредственно в приложение. Права администратора получают только два или три человека, координирующие контент либо возглавляющие департаменты и которые могут следить за темпом работы сотрудником, графиком отпусков. Тем, кто находится в отпуске, мы временно закрываем доступ, чтобы избежать случаев подключения через открытые сети либо из гостиниц.

На предоставлении доступа процесс не заканчивается — далее потребуется много усилий для обслуживания. К примеру, каждые два месяца мы проверяем, все ли в порядке с доступом, не подключены ли определенные сторонние приложения, представляющие угрозу. Может случиться, что ты увидишь рекламу в своем аккаунте в Instagram, скачаешь приложение, войдешь в него, а затем забудешь о нем. Но доступ к приложению остается. Вот почему мы стараемся проверять и удалять приложения, на которые не давали свое согласие на уровне организации. Мы пользуемся только инструментами, проверенными нашей IT-командой. Это способ проявить ответственность, в том числе к нашим пользователям, в частности из стран, где обстановка в плане безопасности не совсем стабильная.

Насколько быстро следует предоставлять новым коллегам доступ к нашим рабочим платформам?

Необходимо доверять людям, чтобы предоставлять им доступ. В случае моей команды речь идет о по меньшей мере двух или трех месяцах, ведь объем получаемой информации лавиной обрушивается на нового работника, а из-за этого он, не исключено, может допустить ошибки и промахи. Вот почему мне необходимо для начала убедиться, что мои коллеги хорошо понимают все процессы.

Принимаемые на работу редакторы должны быть готовы трудиться с первого дня, но я рекомендую коллегам дать новым сотрудникам поработать хотя бы месяц и только после этого предоставить им доступ к платформам.

Какие критерии помогут определиться с уровнем доверия, чтобы предоставить доступ?

Важно, чтобы присоединившиеся к команде новички точно понимали нашу роль и наши задачи. Обычно новым сослуживцам я для начала поручаю проводить расследования/поиск, помогать мне с презентациями. Если вижу, что они хорошо справляются, провожу для них последний тренинг, на котором четко объясняю, что предоставление доступа несет с собой и огромную ответственность.

У всех участников нашей команды в *Audience Development* есть доступ ко всем аккаунтам Deutsche Welle. И если что-то случиться с одним из членов команды, может пострадать вся система организации. У нас есть доступ к системе управления паролями, а это сопряжено с огромным риском. Вот почему я добиваюсь, чтобы они поняли одну вещь: пользоваться можно только служебными устройствами и нельзя пользоваться бесплатным Wi-Fi для работы. Я объясняю им, как защищать свои устройства в поездках. У нас даже есть список, с которым им надлежит периодически сверяться и, тем самым, убедиться, что все в порядке. К счастью, до настоящего времени ни у кого из нашей команды не было неприятностей. Может показаться, что все это трудоемко, впрочем, так оно и есть в самом начале, но в долгосрочной перспективе эти усилия того стоят.

Какие угрозы вы пытаетесь предупредить?

Думаю, к наиболее серьезным угрозам, даже если тебе и не взломали аккаунт, относится доксинг (прим. ред. – доксинг определяется как умышленное обнародование личной информации о человеке без его согласия с целью запугать). Люди очень сильно недооценивают опасность доксинга. К сожалению, у нас было достаточно таких случаев. Причем это может произойти не только лично с тобой, но и с кем-то из близких тебе людей: с членом семьи, с другом или еще с кем-нибудь из твоего окружения. И даже если твои личные аккаунты не связаны со служебными и ты используешь другое имя, в любом случае угроза оказаться под ударом существует. Достаточно получить доступ к аккаунту близкого тебе человека, чтобы посредством его аккаунта получить личную информацию о тебе. Все мы знаем, что нужна двухфакторная аутентификация, что нужно работать на служебных устройствах, что существует Meta Business Suite или иные системы, но когда речь заходит о нашей личной жизни и нашей личной информации, мы становимся гораздо легкомысленнее.

Однажды у нас случился инцидент с нашей коллегой, которая вела прямой эфир в Facebook с нашего корпоративного аккаунта. Беседа с гостем в студии была непринужденная и наша коллега вдруг заявляет, что она живет в том же районе — буквально в двух минутах ходьбы от кафе, из которого и вела прямой эфир. В комментариях мы заметили двух пользователей, которые писали друг другу: «Я же говорил, что видел эту ведущую в нашем районе, а ты не поверил. Смотри, я узнаю кафе. Не пойти ли нам вечером туда, глядишь, ее встретим?». Разумеется, нам пришлось остановить тот прямой эфир, так как дело стало принимать опасный оборот.

Пару лет назад у меня тоже был неприятный инцидент: случилось так, что моей матери взломали аккаунт. Она даже не поняла сразу, так как хакер не стал сразу же выкладывать посты от ее имени. Однако получив доступ к ее аккаунту, злоумышленник начал собирать информацию обо мне, о моей семье и открыл новый аккаунт, с которого опубликовал определенные подробности. К счастью, ничего конфиденциального там не было, но для меня этого оказалось достаточно, чтобы понять: следовало «проинструктировать» мать насчет ее безопасности в сети, чтобы тем самым защитить и нас.

Хотя подобное и не ранит непосредственно физически, но все равно пугает. И тебе даже невдомек, каким образом полученные сведения смогут когда-нибудь использовать против тебя же.

Как журналистам оставаться бдительными при своей публичности в сети?

У нас в учреждении действуют разные типы правил. Существуют руководства насчет использования социальных сетей, которые наш департамент — Audience Development — разработал в сотрудничестве с различными экспертами, работающими в Deutsche Welle, к примеру, из юридического департамента и издательской команды. Также у нас есть и правила непредвзятости, установленные главным редактором и издательским советом. Необходимость в них обусловлена тем, что работа общественной телерадиовещательной организации предполагает и ответственность, когда речь идет о наших мнениях и убеждениях. В рамках организации мы управляем проектами Newsfluencer и Ambassadors.

Проект Ambassadors рассчитан для сослуживцев, которых отбирает наш департамент коллективной коммуникации и которые выступают в качестве амбассадоров нашего бренда. Они рассказывают о «кухне» Deutsche Welle, о наших ценностях, о специфике нашей работы, о предлагаемых возможностях и т. д. Что касается их аккаунтов, то они активны главным образом в LinkedIn и, в меньшей степени в Instagram. Участники проекта Ambassadors установили собственные правила о том, насколько подробно можно делиться фактами о своей личной жизни.

Ньюсфлюенсеры или, как их еще называют журно-инфлюенсеры, отобраны из числа сотрудников разных департаментов. Данный концепт мы еще только развиваем, вот почему это предполагает также, что мы заключаем с ними специфические контракты. У них уже есть контракт с Deutsche Welle, а наряду с ним подписывается еще и дополнительный контракт, в котором мы проясняем множество аспектов: доступные пределы анализа контента с нашей стороны, границы нашего вмешательства в управление сообществом, проверку личных сообщений, данных и т. д., ведь это уже отдельная сфера работы.

Устанавливаем мы пределы и насчет скрытой рекламы или так называемого продакт-плейсмента. Часто коллеги приходят и спрашивают, могут ли они рекламировать тот или иной продукт, а нам следует проанализировать, соответствует ли он ценностям Deutsche Welle. К примеру, насчет алкоголя. Мы не рекомендуем нашему коллеге-ньюсфлюенсеру рекламировать алкоголь со своих аккаунтов. Но если речь зайдет, скажем, об эко-моде в Гватемале, а у нашего коллеги окажется там кто-то знакомый и он захочет поддержать такую инициативу, тогда для нас это, разумеется, не будет проблемой.

Как быть с остальными сотрудниками? Они какие правила должны соблюдать?

В основном, речь идет о правилах непредвзятости и правозащитном контенте, а если кто-то выкладывает посты против таких ценностей, тогда это уже становится проблемой.

Это не значит, что мы проверяем личные аккаунты наших сотрудников — мы даже не располагаем кадровым потенциалом для этого, да и не хотим. Но если руководитель департамента случайно увидит в сети нежелательный пост, то он вначале пообщается лично с соответствующим сотрудником, а затем может привлечь и нашу команду, которая занимается медиацией.

В Deutsche Welle есть команда по медиации, она действует в таких случаях и оказывает помощь. Команда по медиации и команда по оказанию поддержки в вопросах психического здоровья — относительно новые, они появились в период пандемии, когда мы поняли важность этой проблемы.

Соответствующие правила постоянно обновляются и каждый должен их прочесть и указать во внутреннем профиле свое согласие с ними. То же самое применимо и к фрилансерам, стажерам и даже в случае партнерств.

Как можно управлять взаимодействием репортеров с общественностью?

Среди наших задач на текущий год было наращивание взаимодействия репортеров с общественностью, а для нас важно как можно чаще применять это.

Когда речь идет о корпоративных аккаунтах, коллеги, занимающиеся модерацией комментариев и общающиеся с аудиторией, всегда действуют с официальных аккаунтов, а не со своих личных, за исключением участников команды амбассадоров или же проекта Newsfluencer.

Обычный редактор не комментирует со своего личного аккаунта. Такое не поощряется. К сожалению, много лет назад у нас был случай, когда наша коллега подверглась расовым нападкам. Это ее так сильно расстроило, что она вступила в спор со своего личного аккаунта. Таким образом, люди, которым до этого было невдомек, что у нее есть аккаунты в Instagram или Facebook, обнаружили ее и там. По сути, она сама себя задоксила. Все мы люди. Достаточно одного комментария, который станет тем самым триггером, и ты «сломаешься», ввяжешься в прямой конфликт с пользователями. Я же лично – яростный сторонник идеи, которая гласит: «не кормите троллей».

Какая роль отводится психическому здоровью в дискуссиях насчет бдительности?

И в этом случае тоже существует несколько уровней. Первый касается администраторов сообщества. Наши коллеги ежедневно сталкиваются с полными ненависти сообщениями. И может так случиться, что в определенный момент ты просто утратишь веру в гуманность. Я говорю это из своего личного опыта. Когда начинала работать в Deutsche Welle, то была в числе менеджеров сообщества для кувейтской аудитории. Это был очень сложный период, нам каждый день приходилось сталкиваться с непростыми изображениями. Наряду с этим мы занимались и фактчекингом. Мы не только модерировали комментарии, но и проверяли контент, отправляемый пользователями. Люди присылали нам изображения, ролики, а мы должны были проверять, можно ли использовать такой контент. Представь себе, что такое каждый день видеть изображения крови и насилия. Думаю, то же самое применимо и к коллегам, которые в настоящее время занимаются украинской тематикой. В какой-то момент это сказывается на твоей личной жизни.

Следующий уровень — хейт, направленный против тебя лично. Ты публикуешь под своим именем, люди видят твое имя и начинают прибегать в своих комментариях к нападкам против тебя, хотя они с тобой и не знакомы. Это происходило и еще происходит очень часто. Как показывает статистика, женщины в большей степени страдают от такого хейта. Но дело в том, что нам, женщинам, хейт настолько привычен, что мы перестаем принимать его всерьез, пока он не превращается в явную угрозу для нас и нашей семьи.

Другой аспект, связанный с психическим здоровьем, обусловлен непрерывным давлением — тебе приходиться постоянно быть в курсе новых тенденций и требований в области массмедиа. Когда работаешь в редакции, тебе надо выполнять одновременно несколько ролей: быть создателем видеоконтента, ведущим передачи, редактором или модератором сообщества в сети. Все это вместе повышает уровень стресса.

В период пандемии многие люди развили собственные механизмы эмоционального регулирования, однако этого тоже недостаточно, особенно когда появляются новые вызовы, как случае украинских коллег. Я помню рабочую мастерскую, которую проводила для украинского департамента всего через пару недель после российского вторжения. Я уже не помню точно, что именно сказала, но что-то вызывало реакцию у одной из коллег, которая разрыдалась. Нам пришлось отказаться от первоначального плана насчет способов реагирования на риторику ненависти и приступить сообща к поиску механизмов эмоционального регулирования для тех, кого война затрагивает лично, у кого семья осталась в Украине. В подобных случаях, когда наваливаются неопределенность, страх и бессилие, ясно, что пренебрегать психическим здоровьем не стоит.

Каким образом влияет ИИ на эти изменения?

Одна из самых больших проблем — генерирование дипфейков. Лица телеведущих или авторов телепередач используются в сомнительных видео, причем я имею в виду не только контент сексуального характера, но и клипы, из содержания которых вытекает, что эти люди якобы совершают преступления, делают компрометирующие их вещи.

Полагаю, мы, в качестве индивидуальных организаций, мало что можем сделать, но если мы сплотим силы с другими организациями и проявим настойчивость, тогда, надеюсь, что начнут лучше осознавать опасность не только простые люди, но и политики, которые могут создать более ясные правовые рамки насчет использования ИИ, фейков и дипфейков.

Какие навыки следует развивать начинающим журналистам в этих условиях?

Думаю, что для молодых журналистов и, говоря это я отнюдь не пытаюсь недооценивать их навыки и знания, очень актуальной остается проблема источников. Мы работаем со студентами, которые приходят на наши тренинги или подают документы для стажировок в составе наших команд. Меня поразил их недостаточный уровень в плане ответственного потребления новостей: они не уделяют внимание источнику, к примеру, увидев видео в TikTok, говорят, «ок, я увидел(а) в TikTok», но не проверяют аккаунт, с которого выложили тот ролик, не выясняют, достоверна ли соответствующая информация.

Какой практический совет может легко применить маленькая организация?

Выбирай свои битвы и не пытайся быть везде — будь только там, где ты чувствуешь, что приносишь самую большую пользу себе и своей аудитории. Если замечаешь, что присутствие в комментариях, диалоге с сообществом, приносит дискуссии больше пользы и улучшает заметность сюжетов, в которые ты веришь, хотя это и предполагает производить меньше контента, то это нормально. Но когда речь идет об инструментах, не стоит слишком сильно фокусироваться на них. Лучше начать с бесплатных и доступных сейчас, а когда появятся финансовые ресурсы, вы сможете инвестировать в более продвинутые инструменты.

Возможность!

Организация Reporters Without Borders (RSF) запустила платформу **RSF Resources for Journalists**. На ней собраны практические простые в использовании ресурсы, призванные помочь журналистам защищаться, самосовершенствоваться и работать в безопасных условиях даже в самой враждебной обстановке. На платформе выложено более 150 статей и материалов, сгруппированных по тематике, например, цифровая безопасность, физическая безопасность, психическое здоровье, юридические рекомендации.

Проси о помощи!

Если сталкиваешься с постоянным стрессом и тревожностью, можешь обратиться за бесплатной и конфиденциальной консультацией психолога через **этот чат-бот** или заполнив **этот бланк**. В течение 48 часов с тобой свяжется специалист.

Если эти материалы тебе понравились, тогда рекомендуй нашу электронную рассылку и своим коллегам по журналистскому цеху. Отзывы и обратная связь помогут нам стать лучше. Напиши свое мнение об электронной рассылке и отправь его нам на следующий адрес api@api.md.

Funded by the European Union

Эта электронная рассылка подготовлена при финансовой поддержке Европейского Союза. Ее содержание является исключительной ответственностью проекта **«TRIMEDIA – достоверная информация, успешные медиа и активные местные сообщества»**, финансируемого Европейским Союзом и софинансируемого Федеральным министерством экономического сотрудничества и развития Германии (BMZ). Содержание рассылки принадлежит авторам и не обязательно отражает видение Европейского Союза.

Follow us: Facebook, Instagram

Unsubscribe