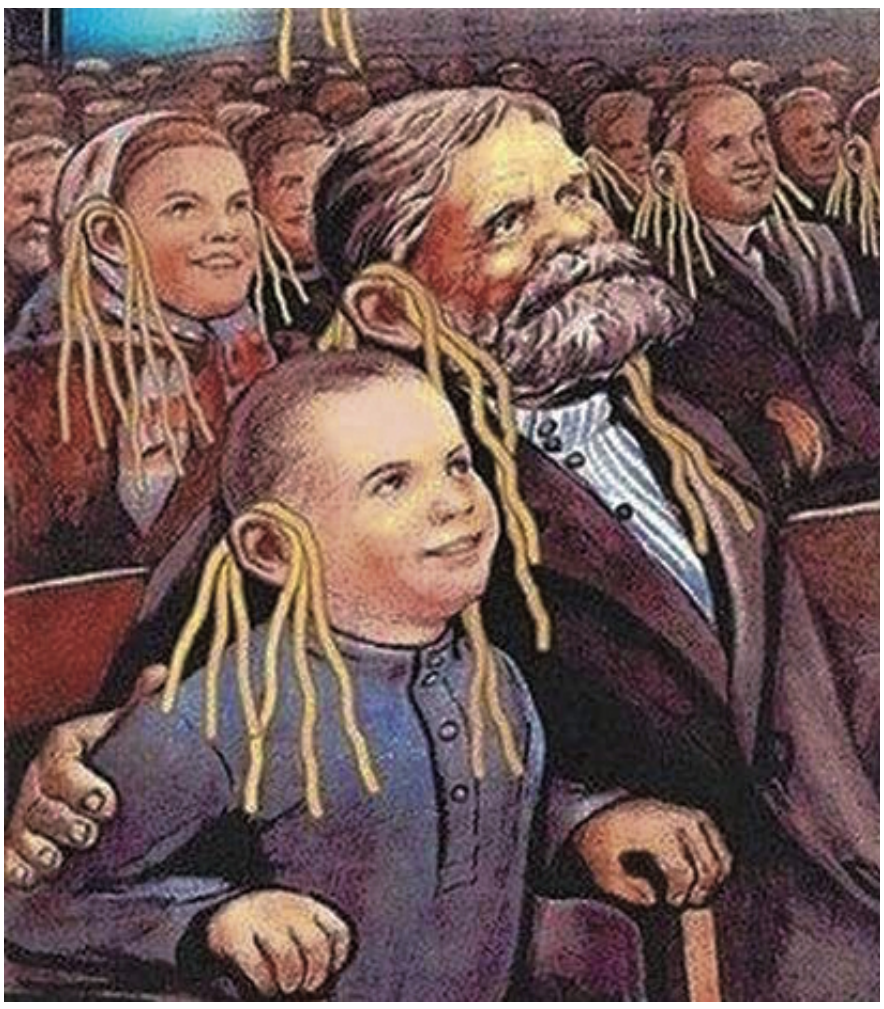
Практика

Обмани меня!

Человек склонен доверять лишь той информации, которая не противоречит его личной картине мира



«ММ» принял участие в федеральном интенсиве «Инфорум», который провёл Союз журналистов России. Интенсив посвятили фактчекингу – проверке достоверности фактов. С началом пандемии тема стала актуальной как никогда. В Рунете постоянно всплывают «удивительные» публикации об инфекции, и верят им даже профессиональные журналисты. Они помогают фейкам плодиться в Сети – ссылаясь на «источники» в собственных новостных заметках и статьях. Союз журналистов России намерен если не устранить, то хотя бы сбавить обороты этой практики.

Одним из спикеров «Инфорума» стал доцент института массмедиа и рекламы Российского государственного гуманитарного университета, партнёр аналитической компании Media Toolbox Максим Корнев. Он объяснил, почему ковид всколыхнул распространение фейков и как отделить правду от вымысла.

В современном медиаполе существуют четыре главные проблемы: фейки, постправда, когнитивные искажения, алгоритмы Интернета

Так, постправда – это обстоятельства, при которых объективные факты имеют меньше влияния на общественное мнение, чем апелляция к эмоциям и личным убеждениям:

– Человек выбирает те факты, которые ему удобны и выгодны. В этой ситуации интересен микротаргетинг – «новая пропаганда». Старую пропаганду можно сравнить с катком, потому что она работала сразу по всему обществу и была эффективна в условиях территориальной изоляции, когда один источник информации доминирует над остальными, – размышляет Максим Корнев. – В Интернете же огромное количество мнений, и пользователь легко может потерять фокус. Новая пропаганда – это точечная пропаганда. От того, каков человек по натуре, зависит, какую реальность ему показывают в Сети. Если человек верит в заговоры, то, скорее всего, он охотно поверит, что ковид – изобретение китайцев или даже что Земля – плоская.

Максим Корнев

Такая впечатлительность связана с тем, что мозг – орган затратный, ему для обработки информации необходимо очень много энергии. Поэтому человек вырабатывает привычки и старается идти по накатанной: когда узнаёт что-то новое, сопоставляет с имеющимся багажом и добавляет в «копилку», если есть схожесть. В большом потоке информации неосознанно выбирает только ту, что хоть чем-то ему знакома. А критическое мышление – это напряжение эмоций и сил. Именно так возникают когнитивные искажения:

– Если сложить вместе постправду и когнитивные искажения, добавить алгоритмы Интернета, то получим эффект «фильтр-пузыря», внутри которого возникает «эхокамера», – продолжает спикер «Инфорума». – Когда человек пользуется Интернетом, все ресурсы начинают подстраиваться под его запросы. Те самые cookie-файлы, согласие на использование которых даётся ресурсу, помогают другим сайтам видеть историю просмотров.

Каждая система хочет, чтобы люди как можно чаще пользовались именно её ресурсами – больше проводили времени, например, в Facebook или в «ВКонтакте». Для этого и создают алгоритмы, подбирающие конкретную информацию, которая непременно понравится. Когда человек лайкает или дизлайкает, подписывается или отписывается от интернет-сообществ, он формирует замкнутый круг. И, попав в этот кокон, начинает думать, что созданная картина мира и есть реальный мир:

Казалось, что Интернет всех объединяет, но на самом деле эффект обратный. Общество распадается на микросообщества. Вот такой парадокс. Всё это и поспособствовало всплеску так называемой инфодемии – наплыву различных фейков о коронавирусе:

– Инфодемия – это наши пороки, готовность общества воспринимать удобную и желанную правду, – убеждён Максим Корнев. – А люди с готовностью лайкают и перепощивают. Но гораздо хуже, когда фейк проникает в серьёзное медиа, и тогда переубедить людей становится сложнее. Ведь человек с конспирологическим сознанием всегда найдёт причину опровержениям – подумает, что это, конечно же, заговор.

Корнев считает, что в основе фактчекинга должно стоять критическое мышление, реагирующее на сомнительные источники и шок-картинки. Этой предпроверкой информации могут заниматься все пользователи.

Постпроверка же затрагивает ситуацию, когда фейк уже гуляет по Сети, и здесь необходимо включаться редакциям СМИ, чтобы не допустить дальнейшей манипуляции обществом

«Хороший» фейк – это не грубая провокация, а тонкая манипуляторная работа.

Отвечая на вопрос «ММ» о том, почему Роскомнадзор не отбирает лицензии у СМИ, которые публикуют фейки, и не блокирует ресурсы, где была замечена дезинформация о ковиде, Максим возразил, что прецеденты всё-таки есть. Но и добавил, что бороться с Интернетом невозможно – чем больше будешь удалять, тем чаще станут распространять:

– Главная проблема не в том, кто опубликовал фейк – легальное СМИ или блогер, а в том, что распространяют информацию сами люди через мессенджеры и социальные сети. Хотя наказание за фейки повышает уровень ответственности, и всё-таки должен работать принцип саморегулирования, чтобы профессиональные медиа хотя бы не эксплуатировали «хайповые» темы и «рубили» трафик.

Спикер порекомендовал в качестве фактической базы использовать Энциклопедию коронавирусных слухов и фейков, созданную школой актуальных гуманитарных исследований РАНХиГС. В Энциклопедии содержатся псевдомедицинские советы, народные и религиозные рецепты, алармистские предубеждения, «свидетельства» о происходящем от первого лица, подделки официальных документов, рассказы об этиологии вируса. Всё «выловили» в Сети и проверили – факты не подтвердились. Но эти фейки продолжают блуждать в Интернете, кроме того, создают и новую дезинформацию.

Ссылка на Энциклопедию – nplus1.ru/material/2020/04/08/coronarumors

Максим Юлин

Прокуратура разъясняет

Фишинг - новый вид «рыбалки»

К сожалению, фантазия мошенников по ограблению честных граждан не знает предела и совершенствуется синхронно с техническим прогрессом, не отставая ни на шаг, а иногда его опережая.

Фишинг (от англ. слова phishing – рыбная ловля, выуживание) – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям – и является одной из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности.

По данным МВД России, так называемый фишинг – это наиболее распространённый способ совершения преступлений, направленный на получение платёжной информации и хищение денежных средств в Интернете. Основная цель злоумышленников – получить данные кредитной карты, пароль в мобильный банк для последующего незаконного списания средств с банковских счетов. При этом фишинговые сайты внешне сделаны так, чтобы пользователи принимали их за существующие популярные ресурсы. Обманным путём такие порталы могут выудить у неопытного пользователя персональные данные или платёжную информацию.

Также всё большую популярность обмана доверчивых граждан набирает голосовой фишинг, когда клиенту банка звонят от имени финансовой организации и под разными предлогами стараются узнать платёжную информацию. Мошенники находят способы для блокировки облачных хранилищ с личными данными, устройств Apple в целях последующего шантажа.

Сложность раскрываемости таких преступлений обусловлена тем, что жертва электронной кражи узнаёт о потере денег не сразу. Чем больше проходит времени с момента незаконного списания средств до обращения в правоохранительные органы, тем меньше шансов поймать нарушителей закона. Подобные преступления – дело рук организованных преступных сообществ, в которых действия строго поделены между членами банды. Ещё одна сложность в раскрываемости такого вида преступлений состоит в том, что сайт-двойник существует максимум сутки.

Для защиты от мошенников следует придерживаться некоторых правил

Никогда и никому, ни при каких обстоятельствах, нельзя передавать такие конфиденциальные данные, как логин, пароль или реквизиты вашей банковской карты (секретный код безопасности CVV2, подтверждающий подлинность карты, имя ее владельца, срок действия) и, разумеется, пин-код.

Если вы потеряли карту или у вас есть основания полагать, что третьи лица узнали ее реквизиты, обратитесь в банк и заблокируйте её.

Не забывайте, что банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

Делая покупки в интернет-магазинах, предварительно узнайте, с кем имеете дело. Попробуйте найти физический адрес продавца (не абонентский ящик) и его телефон. Поищите отзывы в Интернете. Если люди пишут о неприятном опыте с такими магазинами, вам придется решить, стоит ли рисковать.

Следите за своими банковскими отчётами и отчётами по кредиткам на предмет списаний с вашей карты, которых вы не узнаете или которые подозрительно выглядят. Позвоните своему банку, эмитенту карты или кредитору, если найдете транзакции, которых вы не совершали.

Не отвечайте на сообщения с просьбами предоставить личную или финансовую информацию.

Имейте в виду: фальшивые письма и фальшивые сайты могут во всём повторять дизайн настоящих (качество подделки зависит от того, насколько хорошо мошенники знают свою работу), но гиперссылки, скорее всего, будут неправильные – или с ошибками, или вообще будут отсылать не туда. По этим признакам можно отличить фишинговое письмо от настоящего.

Альбина Бурьян,
помощник прокурора Орджоникидзевского района
г. Магнитогорска, юрист 1-го класса