

## **Что такое информационная гигиена и почему её надо соблюдать**

Соблюдать правила личной гигиены нас учат с раннего детства. Однако с развитием цифровых технологий и началом информационной эры не менее важным стало соблюдение правил информационной гигиены. В противном случае можно не только испортить себе настроение, но и стать жертвой кибермошенников.

Время, в которое мы живём, называют информационной эрой (Information Age, эра информации, автоматизации и компьютеров). Принято считать, что информационная эра началась после цифровой революции (примерно в 1980-х годах). Тогда во всём мире росла популярность компьютеров, интернета, игровых приставок, а позднее и персональных мобильных устройств — планшетов и смартфонов. Благодаря всеобщей цифровизации информация из бумажного формата перешла в электронный и стала мгновенно доступной пользователям. Где бы человек ни находился, он через интернет с помощью своего компьютера или мобильного устройства может прочитать любую книгу, послушать лекцию, пройти обучение, посмотреть интересный фильм, посетить театр или выставку, узнать новости. С каждым годом растёт и скорость передачи информации.

Но обилие и доступность информации (её может получать и размещать любой желающий) привели к тому, что в публичном поле можно столкнуться как с объективными сведениями, так и с ложью или манипулированием. Самое неприятное — такой обман могут использовать злоумышленники для управления не только конкретным человеком, но и общественным сознанием. То есть, они могут оказывать влияние на социальные процессы.

Так, именно из-за спланированной информационной кампании в Египте в 2011 г. произошла отставка правительства и президента Хосни Мубарака. Другой пример — «письмо счастья», автор которого просит переслать его 10 знакомым, иначе вас ждёт неудача и несчастье.

Если человек хочет пользоваться благами цифровой эпохи без негативных последствий, необходимо соблюдать правила цифровой гигиены. Разобраться в инфопотоке помогут простые правила.

### **Правило №1.**

**В интернете нельзя никому доверять, надо всё проверять**

Помните, что разместить информацию в интернете может любой желающий из любой точки мира. Поэтому никогда не верьте на слово. Проверяйте информацию, постарайтесь составить полную картину произошедшего события, понять, какие есть подтверждения и доказательства.

#### **Ситуация**

Вы прочитали, что в лесах Подмосковья обнаружен новый вид гадюки, чей укус смертельно опасен для человека. Авторы публикации ссылаются на сообщения МЧС и Минздрава и утверждают, что жертвами гадюки стали уже 10 человек, настоятельно рекомендуют не ходить в лес.

#### **Ваши действия**

Оцените достоверность информации по автору и источнику. Признаками достоверности могут быть:

- репутация автора: известный журналист, общественный или научный деятель;
- источник информации: информационное агентство или газета федерального уровня; пресс-служба государственного учреждения;
- наличие нескольких публикаций в различных доверенных источниках.

Новости имеют сетевую структуру: появляются на новостных лентах крупных интернет-изданий, далее попадают в новостные агрегаторы, потом распространяются блогерами. То есть значительная часть новостей — это перепечатки.

Если инфоповод появился в крупных изданиях, распространился в блогосфере и на аналитических ресурсах, то вы легко найдёте и первоисточник, и дополнительные детали. Если же вы увидели видеоролик блогера, а в достоверных источниках информации о событии нет, то с большой вероятностью это фейк или постановка. Таким образом автор хочет привлечь внимание и «накрутить» просмотры.

Поэтому если информация вас заинтересовала, проверьте, опубликована ли она хотя бы в двух-трёх крупных и известных источниках. Если в публикации упоминаются сообщения государственных ведомств или результаты исследований, то серьёзные издания обязательно поставят ссылку на источник информации. В противном случае вам придётся самостоятельно поискать его и внимательно изучить исходное сообщение.

Если в новости включены цитаты экспертов, то можно проверить, кто они и насколько компетентны в данной области. Просто скопируйте ФИО, должность и вставьте в поисковую строку.

Что будет, если не проверить информацию

Принимая на веру всё написанное в интернете, вы формируете в своём сознании искажённую картину мира. Кроме того, фейковые новости зачастую носят негативный характер, а значит вы совершенно зря испортите себе настроение.

Правило №2

Если реклама заинтересовала — не спешите с решением о покупке

Создать страничку в интернете несложно и недорого. А потом можно разместить на ней рекламу и постараться привлечь как можно больше посетителей. Ещё проще купить рекламу на агрегаторе новостей или у блогера. На крупных интернет-ресурсах рекламные объявления проходят модерацию, но не проверку качества. Сложно привлечь к ответственности авторов недостоверной информации, размещённой на малоизвестных сайтах. Поэтому нужно самостоятельно проверять содержащиеся в рекламе факты.

Ситуация

Вы увидели в интернете рекламу, в которой известный доктор Александр Мясников рекомендует использовать новый препарат от диабета.

Ваши действия

Наберите в поисковой строке «Мясников рекламирует новый препарат от диабета». На первой же странице вы увидите статью под названием «[Доктор Мясников предупредил о фейках от его имени](#)», в которой он говорит, что не

занимается рекламой препаратов. Также необходимо проверить сам рекламируемый препарат — изучить официальную инструкцию и прочитать отзывы людей, которые его принимали.

Что будет, если не проверить информацию

Если вы не проверите информацию и кликнете на рекламу, то на экране может открыться окошко для ввода ваших ФИО и номера телефона. Через некоторое время вам перезвонят мошенники и с помощью манипуляций уговорят купить у них препарат. В лучшем случае, от него не будет никакого толка, а в худшем — он нанесёт вред вашему здоровью.

Более того, ваши контактные данные — это очень ценная информация. Получив её, киберпреступники соберут о вас максимум сведений в интернете. И через некоторое время ваш телефон будет разрываться от мошеннических звонков.

Хорошей практикой может стать проверка информации о товаре по отзывам на крупных маркетплейсах. Как правило, на хороший товар будет порядка 100 положительных отзывов, но будут и отрицательные. Всегда найдётся несколько покупателей, которых товар разочарует.

Если вы выбираете подрядчика для строительства дома или ремонта, то найдите реальных клиентов компаний, к которым хотите обратиться, и посмотрите на качество работы. Только после этого можно заключать договор.

Не платите все деньги сразу и не давайте больших авансов. Разбейте платежи на этапы согласно графику работ в приложении к договору. Проверьте название компании или ФИО индивидуального предпринимателя по открытым источникам — подавались ли к ним судебные иски, много ли негативных отзывов от клиентов.

Правило №3

Ставьте под сомнение все сообщения в мессенджерах

Не принимайте на веру присланные в мессенджеры сообщения, будь то родительские чаты или группы по интересам в социальных сетях. Во-первых, даже знакомый человек может отправить вам непроверенные сведения. Во-вторых, его аккаунт могли взломать мошенники. Всегда проверяйте полученную информацию и не переходите по ссылке, пока не удостоверитесь, что её действительно прислал ваш знакомый, и что она безопасна.

Прежде чем отреагировать на сообщение в мессенджере:

- Оцените, не принесёт ли вред вам или вашим близким выполнение действия, о котором вас просят?
- Подумайте, вызывает ли сообщение сильные эмоции: страх, любопытство, алчность, азарт, сострадание? Это признак мошеннического сообщения.
- Оцените контекст переписки. Например, если от малознакомых людей приходит просьба проголосовать за ребёнка в конкурсе — это странно. Это типичная уловка мошенников для кражи аккаунтов в мессенджерах.

Ситуация

Знакомый прислал вам сообщение, что Президент во время телеобращения анонсировал единовременные выплаты семьям с детьми от 3 до 16 лет в размере

10 тыс. рублей. Для получения надо присоединиться к официальной группе в социальных сетях по выплате пособий семьям с детьми.

#### Ваши действия

Наберите в поисковой строке «Единовременные выплаты семьям с детьми в размере 10 тыс. рублей». На первой же странице вы увидите сообщения о новой мошеннической схеме, когда деньги и данные выманивают под предлогом выдачи таких пособий.

#### Что будет, если не проверить информацию

Если вы присоединитесь к группе, мошенники попросят вас предоставить персональную информацию якобы для заполнения заявления, а затем продиктовать им данные банковской карты и код из СМС для зачисления пособия. Персональные данные они смогут продать на чёрном рынке, и уже через несколько дней вам будут звонить мошенники всех видов и мастей. А с банковской карты они просто снимут все деньги.

#### Правило №4

Будьте бдительны при просмотре фото и видео

В качестве подтверждения реальности события нередко используются фото- и видеоматериалы. Однако им нельзя верить безоговорочно, поскольку они могут быть сделаны совсем в другое время и в другом месте. Изображение может быть смонтировано. Более того, технология [deepfake](#) позволяет создавать фейковые фото и видео, которые очень сложно отличить от настоящих.

#### Ситуация

Вам прислали фотографию засыпанной снегом пустыни. В комментарии говорилось, что изменения климата привели к двадцатиградусным морозам в Африке.

#### Ваши действия

Первым делом найдите первоисточник фотографии. Для этого можно воспользоваться сервисом поиска по изображению, например, «Яндекс.Картинки». Затем можно проверить фото на deepfake с помощью [специальной программы](#). И, конечно, не забудьте проверить саму новость — если это событие действительно произошло, то о нём наверняка написали крупнейшие СМИ.

#### Что будет, если не проверить информацию

Конечно, если вы поверите, что в Африке зимой теперь так же холодно, как и в России — ничего страшного не произойдет. Однако нельзя забывать, что фейковые фото и видео стали распространённым инструментом в руках мошенников. Их цель — посеять панику, заставить людей совершать необдуманные поступки.