АНТОН ШУСТИКОВ

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

ГРАМОТНОЕ ПОВЕДЕНИЕ В СЕТИ

БОМБОРА
ИЗДАТЕЛЬСТВО
Москва

ОГЛАВЛЕНИЕ

ПРОЛОГ

Здравствуйте, дорогие читатели! В ваших руках своего рода путеводитель по современному цифровому миру. Его цель — популяризация и распространение простых и эффективных методик самозащиты в цифровом пространстве, доступных каждому без специальной подготовки и знаний. Конечно же, расширение охвата, облегчение доступа к всемирной сети — это хорошо. Но нельзя забывать об обратной стороне этой медали — интернет сегодня наводнен злоумышленниками различного уровня, знакомыми нам как мошенники.

Их главная цель — получение прибыли. И речь не только о деньгах (цифровых кошельках, платежных системах и прочем), но и об информации — она может стоить гораздо больше любых денег, а временами и жизни. Именно поэтому в современном мире необходимо прибегать к информационной гигиене и хотя бы поверхностно ознакомиться с ее основными постулатами. Также не следует забывать о кибербезопасности — науке о действиях, направленных на сохранение ваших нервов и здоровья, финансов и конфиденциальной информации, которая находится на ваших компьютерах.

Немаловажно знать и основные правила нахождения в цифровом пространстве, ведь современные дети, да и взрослые, проводят в сети немало времени. Причем проводят его в социальных сетях, где принято пуб-

ликовать статусы, фотографии, события из жизни и т.д. Таким образом, пользователи сами распространяют конфиденциальную информацию, а также дают «пищу для ума» злоумышленникам, которые используют социальную инженерию — науку, основанную на психологии. В контексте книги эта наука может быть воспринята негативно, ведь ее главная задача — грамотное воздействие на конкретного человека с помощью его слабостей. А узнать о них можно в том числе через интернет (что чаще всего и происходит). В этом руководстве вы найдете способы защититься от сего явления.

Кому полезна эта книга? Ответ прост — любому пользователю интернета. Особенно тем, кто имеет высокую деловую активность, медийность. Она принесет пользу и в качестве наглядного пособия по профилактике цифровой безопасности и мошенничества, которые преодолевают цифровые барьеры и выходят в реальный мир. Если вы пользуетесь онлайн-банкингом, то эта книга для вас. Если вы ведете маленький бизнес на маркетплейсе, или любите простейшие компьютерные игры, или смотрите телепередачи в интернете, или пользуетесь социальными сетями, то получите информацию, которая убережет вас от манипуляций мошенников. Если вы бизнесмен или публичная личность, то эта книга сохранит вам невероятное количество нервов и денег. Если у вашей бабушки есть мобильный телефон, то подарите ей это пособие и можете быть спокойны: она узнает, как мошенники ловко выуживают информацию и манипулируют и как могут навредить ей.

Значительную часть карьеры в информационной безопасности я занимался обеспечением персональной безопасности первых лиц и готов поделиться с вами своим опытом. Конечно, в моем путеводителе вы можете встретиться с новыми терминами и непонятными

концепциями. Но я приложил весь свой опыт общения с людьми, далекими от технологий, и постарался рассказать о проблемах цифрового и стремительно развивающегося современного мира доступным и понятным языком. Нередко для этого пришлось жертвовать академической точностью в пользу доступности материала. И все для того, чтобы эта книга стала понятной даже совсем несведущему и далекому от информационных технологий человеку. Мы изучим правила безопасности в сети, чтобы каждый мог построить вокруг себя безопасную среду, — это сохранит не только ваш покой, но и здоровье и благосостояние. В качестве ориентиров в текстах каждой главы используются общепринятые правила личной безопасности и конфиденциальности.

Моя цель — познакомить вас с популярными в наше время угрозами безопасности в сети. Без лишней мишуры, на реальных примерах и личном опыте. Хотите понимать тонкости информационной безопасности и узнать, как грамотно подходить к вопросам цифровой гигиены? Тогда эта книга для вас.

Следует усвоить главное правило.

Безопасность данных как для физических, так и для юридических лиц начинается с пользователя.

Эта книга рекомендуется к прочтению всем реальным и потенциальным жертвам цифровых злоумышленников. То есть каждому пользователю компьютера, планшета, ноутбука, смартфона, да и интернета в целом. Ведь, по статистике, каждый хотя бы раз сталкивался с сетевыми угрозами: кибersталкингом, воровством, взломами учетных записей, мошенничеством и компьютерными вирусами.

Иными словами, виной большинства бед, связанных с цифровым миром, становится человек. И относится

это не только к физическим лицам, но и к юридическим. К сожалению, немногие это осознают.

Важность информационной безопасности в современных условиях не надумана. В сети можно найти множество экспертных мнений, которые складываются в ужасающую картину, — цифровая криминогенная среда беспощадна. По словам тех же специалистов информационного мира, именно в цифровой среде формируются негативные для народа и государства явления — создание «пятой колонны», появление альтернативных точек зрения (рискующих превратиться в точки влияния). Мы не будем касаться вопросов политики и не станем обсуждать намерения государства сделать эту среду подконтрольной. Тем не менее, если взять в расчет различные конспирологические теории, почти все сетевые ресурсы находятся «под колпаком», а значит, и все их пользователи тоже. Задача этой книги — помочь пользователям научиться использовать сетевые ресурсы грамотно и без последствий — как цифровых, так и материальных.

Приглашаю окунуться в этот удивительный мир, позволяющий нам быть самими собой в сети и сохранять в безопасности свое здоровье, финансы и конфиденциальные данные. Это не так сложно, как кажется, и весьма увлекательно — главное начать!

Но прежде чем мы погрузимся в эту тему, позвольте представиться. Меня зовут Антон Шустиков. Я ментор и ИТ-специалист С-уровня; автор просветительского некоммерческого проекта; активный и едва ли не первый «киберхранитель»; специалист в сфере информационной безопасности с 15-летним стажем; технический директор и директор по маркетингу; прожженный стартапер; разработчик систем безопасности для частного и корпоративного сегмента; специалист в сфере

искусственного интеллекта (ИИ). Я поистине обожаю все, что связано с цифровым миром.

Прежде чем идея о создании книги пришла мне в голову, я прошел долгий путь от специалиста до топ-менеджера крупной компании. Хоть карьера моя и развивалась очень своеобразно, это позволило мне увидеть мир информационных технологий с разных сторон.

ЧТО ТАКОЕ ЦИФРОВАЯ ГИГИЕНА

Если рассматривать информацию в интернете в качестве главного «орудия» в киберпространстве, то цифровая гигиена исполнит роль инструмента создания безопасного пространства во всемирной сети.

Как вы понимаете, информация может нести как добро, так и зло — в зависимости от метода ее преподнесения. Таким образом, появилось понятие «инфодемия» — лавина бесполезной и несущей угрозу для психики информации, которая распространяется как эпидемия. Такое бывало и ранее. Например, после знаменитого землетрясения в Ташкенте, произошедшего в 1966 году, по улицам города ходили несколько человек, которым «кто-то сказал по секрету», что вот-вот произойдет еще одно землетрясение, мощнее и дольше предыдущего. Кто распространял эти слухи, с какой целью — выяснить не удалось даже сотрудникам КГБ, которые занялись этим вопросом, пресекая распространение паники в городе. Из относительно недавних событий, подходящих под определение инфодемии, стало распространение слухов о наночипах, которые вместе с вакциной от COVID вводятся в кровь и могут влиять на поведение человека, вплоть до полного перехода на «внешнее управление». Конечно, люди, знакомые

с техническим миром и/или биологическими аспектами вопроса, лишь смеялись над этими слухами, но среди остальной части населения происходили вспышки параноидальных настроений.

Возникает вопрос «зачем?». Причины могут быть разными — от повышения уровня паники среди людей и, как следствие, продвижения некоторых платных услуг или товаров, до глобальных, которые понятны лишь инициаторам. Но, как мы уже выяснили, действия людей, распространяющих подобные слухи, — это социальная инженерия, еще одно ответвление психологической науки. Мы поговорим о ней позже, когда разберемся с основными целями информационной гигиены.

Согласитесь, в таких условиях использование информационной гигиены становится едва ли не делом первой очереди. Но следует понимать, что она работает не в одну сторону. Одно из главных правил, сформированных по опыту применения новой науки, — это сокрытие информации не только «в себя», но и «от себя». То есть не следует открывать информацию о себе, которая может вызвать беспокойство или причинить серьезный вред здоровью или имуществу конкретного человека.

Наверняка у вас возник вопрос: а чем же грозит распространение информации о себе? Ведь все уже привыкли к социальным сетям, где без задней мысли люди размещают свои контактные данные, фотографии, делятся событиями из жизни. Именно это может сыграть с пользователем злую шутку, а вот какую, я расскажу чуть позже.

Подытоживая вышесказанное, понятие цифровой гигиены можно трактовать как навык фильтрации поступающей и исходящей информации, исключая таким образом все возможные потери — репутации, здоровья,

финансов. А ведь при сопряжении с еще одним «злом» современных информационных сетей (о котором я также расскажу) можно стать и причиной утечки важных и конфиденциальных данных, принадлежащих иным лицам или организациям. Выражаясь проще, это искусство скрывать необходимое и ограждать себя от излишнего.

Кибергигиена

Понятие гигиены в киберпространстве, чаще называемой кибергигиеной для краткости, схоже с понятием информационной гигиены. Кибергигиена подразумевает комплекс мер и действий, направленных на повышение безопасности конкретного сетевого узла как в локальной, так и во всемирной сети, а также поддержку работоспособности компьютера. Но это еще и образ мышления, сфокусированный на безопасности, предотвращающий различные сетевые нарушения. Нередко кибергигиену сравнивают с повседневной личной гигиеной, обыгрывая девиз «В здоровой сети — здоровый компьютер!», или «Профилактика — лучшее лечение», или «Мойте руки перед едой».

Кибергигиена, путем применения различного антивирусного и прочего программного обеспечения (ПО), а также методик противостояния приемам цифровых мошенников, получила развитие во время карантинных ограничений COVID-19. Тогда же случился «бум» удаленной работы — повинуясь требованиям ВОЗ, многие работодатели перевели своих сотрудников в домашние офисы. Удаленные работники для своего удобства использовали различные методы доступа к рабочей информации, в том числе мессенджеры и почтовые про-

граммы, большинство из которых не имеют защиты трафика. Злоумышленники, в свою очередь, вычислив или узнав данные некоторых удаленных сотрудников, сумели взломать или обойти системы безопасности, получив тем самым доступ к огромным массивам данных.

Заметив это, многие руководители схватились за голову: позволив сотрудникам работать так, как хочется им, они навлекли на себя немало бед. Пришлось срочно обращаться к специалистам по кибербезопасности в поисках путей решения этой проблемы. С их помощью ситуацию удалось исправить, но до некоторых удаленных работников приходилось долго доносить истину о необходимости соблюдать постулаты гигиены в цифровом пространстве — выйти из зоны придуманного комфорта куда сложнее, чем в нее войти. Но в целом они справились, и сегодня ситуация с безопасностью в сети потихоньку выправляется и входит в правильное русло даже без помощи внешних специалистов.

Гигиена в цифровом пространстве работает одновременно в трех направлениях:

- с нарушениями безопасности компьютерных сетей, предотвращая множество неприятных событий, связанных со взломом компьютеров или сетей, нарушением работоспособности инфраструктуры, а также с хищением данных;
- над безопасностью хранения данных, будь то локальные хранилища или хранилища с доступом через сеть. Весьма полезна гигиена в цифровом пространстве для крупных компаний с большим штатом удаленных сотрудников, а также физическим лицам, хранящим на своих компьютерах немалые массивы конфиденциальной информации;
- над программным обеспечением — своевременное обновление ПО помогает закрыть обнаруженные

в системе прорехи, тем самым уменьшая вероятность проникновения в компьютер вирусов, а также исключая прямое влияние посторонних на работу операционной системы и связанных с ней сетей и хранилищ.

Итак, кибергигиена — это комплекс мер и задач, обеспечивающих безопасность в цифровом пространстве. Учитывая обилие факторов, угрожающих безопасности, кибергигиена должна стать выработанной привычкой, чем-то вроде безусловного рефлекса.

Что общего у информационной гигиены, кибергигиены и психологии

Перейдем к основной фабуле повествования — принципам формирования у каждого человека привычки защищать себя в цифровом пространстве. Оно, повторюсь, как и окружающий мир, может принести различные заболевания (по большей части неврологические или психологические), а также вполне способно создать угрозу финансовому состоянию. Психология в данном случае является связующим звеном, ведь именно на психологическом уровне формируется самодисциплина. А неприятности, которые можно испытывать, находясь в сети, также проявляются на психологическом уровне или продиктованы психологией конкретного пользователя.

Психология — наука объемная и для постороннего человека весьма размыта. Однако в нашем случае она имеет весьма явные очертания, впрочем, как и в любой конкретной области — границы ее пролегают в зоне комфортного. Разумеется, границы у каждого свои — кому-то комфортно в «Одноклассниках», кому-то

в мессенджерах, а кто-то и вовсе не пользуется ни тем, ни другим, предпочитая кнопочный телефон. Важно отметить, что когда мы говорим о высоких технологиях, то даже телеграф и виниловые пластинки подпадают под это определение. Иные пользователи сети и вовсе заходят только почитать/посмотреть новости (зачастую сугубо по интересующей теме). В этом и есть проявления информационной гигиены — человек сознательно ограничивает себя в ресурсах, получая только необходимую информацию. Как же воспитать в себе такую привычку? Для начала разберем три принципа.

Принцип 1. Фильтрация «исходящей» информации

Гигиена в цифровом пространстве подразумевает ограничение не только транслируемой в сеть информации — необходимо следить за тем, что именно вы передаете. Отсеивание передаваемой информации не позволит посторонним составить ваш психологический портрет, увидеть нежелательную в тот или иной момент жизни информацию. Допустим, некая медиаперсона ежедневно публикует контент, где она бывает, что и когда делает. Спустя какое-то время она начинает прятаться от вездесущих папарацци, которые, изучив ее маршрут по публикуемым в интернете данным, начинают ее буквально преследовать, чтобы сделать снимки, а временами и украсть какие-то вещи, чтобы обогатиться на их продаже. И вот уже персона вынуждена маскироваться, чтобы выйти за стаканчиком кофе. Просто посидеть в кафетерии уже не получается — слишком много внимания. В таком режиме проблемы даже на психологическом уровне не заставят себя долго ждать.

Любая публикуемая или передаваемая вами информация может стать граалем для злоумышленников. Позже я расскажу, как работают социальная инженерия