<https://news.clever-lab.pro/2024/01/09/chto-nuzhno-znat-o-cifrovoj-bezopasnosti-i-kak-nauchit-ej-svoih-detej/>

Рекомендации от Клевер-лаборатории:

**Что нужно знать о цифровой безопасности и как научить ей своих детей**

**Что такое кибербезопасность и цифровая гигиена и как сделать так, чтобы последняя вошла у родителей и детей в привычку?\* Об этом нам рассказали руководитель экосистемы «Самолет Образование» и участник «Альянса искусственного интеллекта» Андрей Комиссаров, преподаватель информатики Томского гуманитарного лицея, вошедшего в топ-30 лучших школ России, Наталья Балясова и заботливый папа, больше 15 лет работающий в сфере IT, Александр Оболенский.**

## *****Цифровая гигиена: как научить ребенка защищать себя от опасностей Сети*****

Сегодня в мире нет ни одного человека, который бы не пользовался интернетом. Многие беспечно доверяют ему все подробности своей жизни. Но злоумышленники не дремлют.

## *****Что такое кибербезопасность?*****

Это защита данных от утечки. В рамках семьи — это защищенность собственной информации (личных данных, фотографий, переписок, финансовых данных) от несанкционированного доступа.

## *****Нарушение кибербезопасности*****

Хакеры могут не только несанкционированно получить доступ к вашим электронным девайсам, взломать личные аккаунты ваши и ваших детей в соцсетях или на различных сервисных сайтах и получить доступ к вашим данным. Если, например, сервера школы окажутся уязвимы, то данные всех детей станут доступны злоумышленникам. Взломщики узнают, во сколько дети приходят в школу, во сколько уходят, где они живут и как проводят свое время в кружках. Обладая такой информацией, можно влиять уже на родителей.

## *****Что такое «цифровая гигиена»?*****

Это умение и знание про то, как не оставлять большое количество данных в интернете, защищать их. Цифровая гигиена должна войти в привычку и стать неотъемлемой частью нашей повседневной жизни, построенной на постоянном взаимодействии с гаджетами и интернетом.

## *****Как соблюдать цифровую гигиену?*****

— **Обращайте внимание при подписке на разные сервисы на то, что они запрашивают разрешение на доступ.** Не «окайте» все подряд, особенно на случайных сайтах. Нужно знать, что это может быть запрос на просмотр истории вашего браузера. Зная историю браузера, возможно вычислить расписание дня, в какое время и из каких мест вы заходили в Сеть.

— **Не упоминайте логин и пароль от своих устройств, личных кабинетов и сервисов в общих чатах или переписке в мессенджерах.** Оттуда их легко украсть и использовать в неблаговидных целях ваши данные — номера и скрины документов, результаты анализов, суммы заказов в тех или иных сервисах, адреса проживания и работы. Все это может быть использовано в противоправных действиях, в целях телефонного мошенничества или шантажа. Например, при регистрации от вашего имени в каршеринге.

**— Стоит очень аккуратно общаться с друзьями, которые написали вам внезапно спустя долгое время.** Их аккаунт могли взломать или создать подложный аккаунт от их имени. Перезвоните им, увидев странную просьбу (например, о деньгах) или внезапное стремление активно «залезть в душу». Это могут быть как мошенники, выманивающие деньги, так и «агенты влияния» (особенно актуально для подростков). Такие «агенты» — это либо реальные люди, с которыми вы или ваши дети познакомились в Сети, либо боты, которые «общаются по душам», «хотят» подружиться и завоевать доверие. В отличие от людей, боты не устают и могут писать 24/7. Таким образом создается ложное ощущение, что «новому другу не наплевать», ведь он регулярно выходит на связь. А когда появляется доверие, на человека уже можно влиять — заставлять что-то делать или выманивать деньги.

— **Не открывайте непонятные ссылки.** Например, в мессенджере мама просит проголосовать за дочь в конкурсе пения и хореографии. Или на почту приходит письмо, содержащее ссылку на подарок. Если открыть эту ссылку или файл на домашнем компьютере, то может запуститься программа, которая зашифрует все данные, находящиеся на вашем устройстве. А потом позвонят злоумышленники и попросят денег за дешифровку.

— **При совершении онлайн-оплаты покупок внимательно проверяйте, действительно ли вы находитесь на странице надежного банка, а не на ее поддельной копии.** Такие странички создаются, чтобы получить данные ваших карт и коды доступа к ним. Этот вид интернет-мошенничества называется фишингом. Не покупайте ничего онлайн на сайтах, вызывающих малейшее недоверие. Лучше пользоваться только проверенными крупными торговыми площадками.

## *****Что произойдет, если…*****

— **Кто-то узнает только ваш логин и пароль** и введет его, то станет возможным написать от вашего имени или получить доступ к личному контенту. Ничего более серьезного не произойдет. Практически все значимые финансовые и юридические действия требуют двухфакторной аутентификации, например кода из смс или одноразового пароля, высланного лично вам;

— **К вашей камере или микрофону получили доступ злоумышленники.** Наши гаджеты слушают нас через свои микрофоны. Да, это так, но в рекламных целях, чтобы более эффективно предложить нам товар или услугу. И тем не менее злоумышленники могут получить дистанционный доступ к микрофонам и камерам ваших устройств. Если вы хотите поговорить приватно, то лучше находиться в помещении без устройств с микрофонами и камерами. И когда вы не пользуетесь видеосвязью, камеры ваших компьютеров лучше закрывать — злоумышленники смогут подсматривать за вашими детьми или получить прекрасный ролик с вами в главной роли для шантажа;

— **Вы пользуетесь мессенджерами, например WhatsApp.** Продукты компании Меtа (признана экстремистской организацией на территории РФ) сохраняют 100 % переписки, аудиосообщений, видео и фото и постоянно отправляют их на свои сервера. Потом эти данные используются для анализа и рассылки контекстной рекламы. Но где гарантия, что они не попадут в руки злоумышленников? О крупных утечках персональных данных мы слышим постоянно;

— **Вы пользуетесь открытыми общедоступными сетями wi-fi**, например, в кафе. Помните — через них возможно своровать данные. Поэтому при работе с банковскими приложениями, серьезными личными данными в общественном месте лучше wi-fi отключать и переходить на мобильный интернет;

— **Кто-то «слил» в Сеть базу, в которой содержались и ваши данные.** Если «слили» только имя и почту — то, скорее всего, вам будет приходить спам, если номер карты — то без введенного вами кода верификации снять деньги не получится. Если злоумышленники узнали ваше имя, фамилию и паспортные данные, то на ваше имя могут оформить кредит в банке. Но для такого мошенничества нужен соучастник в банке, потому что без вашей подписи, личного присутствия и проверки сотрудником ваших документов это сделать невозможно. Поэтому вероятность того, что вам удастся избавиться от такого кредита, стремится к ста процентам.

## *****Правила «цифровой гигиены» для паролей и онлайн-покупок*****

* **Не стоит иметь единственный пароль для всех сервисов.** Можно вводить один универсальный для интернет-магазинов, но для «Госуслуг» лучше иметь отдельный пароль.
* **Важные пароли лучше помнить, а не записывать в заметках телефона или хранить в файлах на компьютере.** К ним могут получить доступ хакеры.
* **Обращайте внимание на технические оповещения о попытке взлома учетной записи или утечке пароля** и в таком случае менять пароль.
* **Используйте только проверенные и внушающие доверия ресурсы.** Помните, что злоумышленники часто создают «подставные» копии известных сайтов и сервисов.
* **Не пересылайте никому свои пароли и коды из смс.**
* **Создайте виртуальную карту для оплаты покупок в интернет-магазинах** и переводите на нее ровно ту сумму, которую планируете потратить в настоящий момент. Стоимость такой операции около 100 рублей в большинстве банков, оформление происходит за минуты, не требуется никаких походов в отделения.

Важно понимать, что без компьютера и гаджетов современный ребенок не может расти. Поэтому нужно говорить с ним, рассказывать о возможных последствиях выхода в Сеть, показывать видео про интернет-мошенничество, например фишинг, учить не принимать звонки с незнакомых номеров. Сегодня мы живем в мире тотальной прозрачности. Поэтому у современного пользователя должен быть высокий уровень цифровой грамотности и гигиены.

Женя Сазонова

\*«Клевер Лаборатория» готовит серию статей, которые дадут ответы не только на вопросы о кибербезопасности, но и расскажут о том, почему ребенку важно уметь пользоваться помимо смартфона еще и компьютером. Как научить его критически мыслить и отсеивать вредный и непроверенный контент и как найти приемлемый контент для своего ребенка? Как объяснить ему, что многие блогеры несут откровенную чушь, а их смотрят миллионы, и как помочь своему ребенку самому стать блогером, чтобы это было приятно, безопасно и не отнимало много времени?