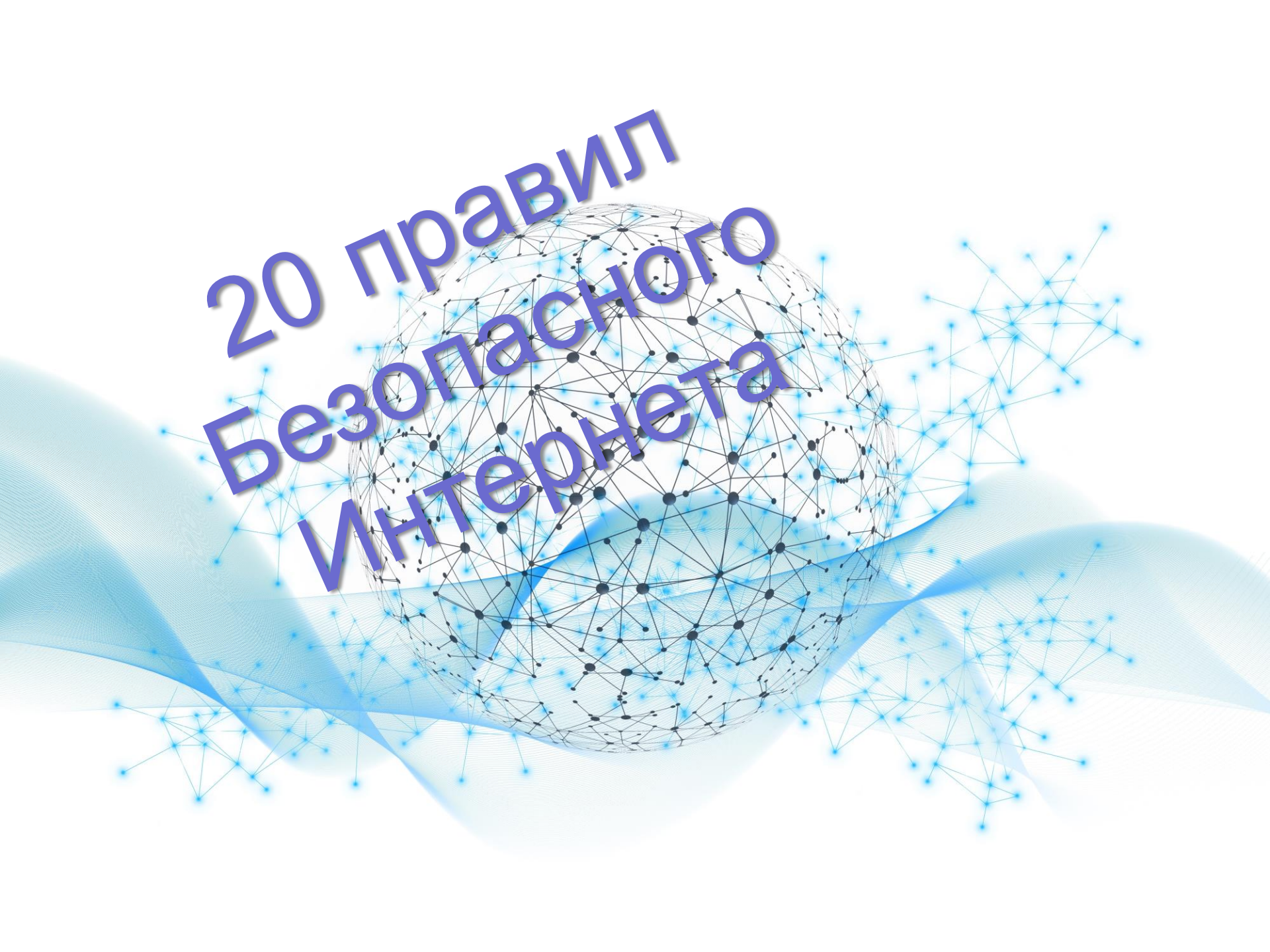
20 правил
Безопасного
Интернета

1. Установите антивирусные программы

Для защиты от вирусов существуют антивирусы. Важно не просто пользоваться ими, но и периодически обновлять их базы данных, ведь создатели вредоносных программ то и дело запускают в интернет свои новые разработки.

2. Используйте сложные логины и пароли

Хороший логин и пароль – это сложная комбинация, в которой используются заглавные и строчные буквы, цифры и символы. Лучше задействовать специальные программы, которые генерируют их, запоминают и надежно хранят. И желательно пользоваться разными сочетаниями логинов и паролей для разных сайтов.

3. Разлогинивайтесь на чужих устройствах

Воспользовались чужим компьютером? После этого недостаточно просто закрыть страницу, на которую вы заходили. Не забывайте предварительно выходить из всех аккаунтов, соцсетей и мессенджеров на устройстве. В противном случае человек, который сядет за этот компьютер после вас, получит возможность войти в вашу учетную запись и сделать с ней все, что ему заблагорассудится.

4. Проверяйте безопасность соединений

Всегда обращайте внимание на то, что написано в адресной строке. Если вы видите, что адрес сайта начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP – это значит, что соединение не защищено. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию во всплывающем окне.

5. Будьте внимательны к соединениям Wi-Fi

Общедоступные соединения есть, например, в кафе, торговых центрах и аэропортах. Не используйте их, если собираетесь вводить логины, пароли, либо совершать оплату услуг и товаров через интернет. Либо вообще не пользуйтесь ими ни при каких обстоятельствах и ограничьтесь обычным мобильным интернетом.

6. Организуйте безопасный режим для ребенка

На многих компьютерах и мобильных устройствах предусмотрен безопасный «Детский режим». Также можно настроить ограничения с помощью домашнего роутера – обычно эта функция называется «Родительский контроль». Еще один вариант – использование специальных детских расширений для браузеров. Любой из перечисленных выше вариантов сводит к минимуму вероятность того, что ребенок попадет на опасный сайт. И, конечно, заведите ему собственную учетную запись.

7. Создайте две почты – для работы и личную

Это не только удобно. Это еще и помогает отслеживать мошенников. Если на рабочую почту приходит письмо, в котором утверждается, что его автор учился с вами в одном классе и вы сами дали ему этот адрес – сразу ясно, что дело нечисто.

8. Не передавайте конфиденциальные сведения

Не пересылайте пароли, логины, паспортные данные, ПИН-коды и прочую подобную информацию в мессенджерах, чатах или по электронной почте.

9. Не храните сканы документов в почте

Лучше вообще не пересылать сканы и фотографии документов по электронной почте, в чатах и мессенджерах. Если такая необходимость все же возникла, например, по работе или если нужно дистанционно направить заявление, после удалите письмо или сообщение в мессенджере. Но перед этим убедитесь, что адресат получил документы.

10. Ограничьте информацию о себе в интернете

Лучше не выкладывать на всеобщее обозрение свой номер телефона, адрес электронной почты и другую контактную информацию.

11. Не открывайте подозрительные письма

Прежде чем открыть письмо, пришедшее на электронную почту, прочитайте заголовок и посмотрите, с какого адреса оно было отправлено. Если тема вам неинтересна, заголовок составлен с грубыми ошибками, адрес представляет собой хаотичное нагромождение символов или напоминает название вашего банка, но с переставленными буквами, сразу отправляйте письмо в корзину. И никогда не открывайте файлы .exe в подозрительных письмах.

12. Не переходите по подозрительным ссылкам

Даже если всплывающая ссылка обещает что-то очень интересное и выгодное, лучше не кликать на нее. Если ссылку прислал вам знакомый, причем без каких-либо комментариев, сначала уточните, что он имел в виду. Возможно, его взломали, и теперь мошенники используют его профиль для рассылки вредоносных программ.

13. Не отправляйте предварительные SMS

Вам предлагают скачать красивую картинку или интересный рингтон в интернете за SMS? Проверьте номер, на который просят отправить сообщение, в любом поисковике. Возможно, это мошенничество, и вам пришлют файл с вирусом или попросту спишут со счета телефона солидную сумму денег.

14. Не устанавливайте сомнительные приложения

Есть два безопасных источника приложений:

официальные магазины, созданные Apple, Google, Microsoft и другими подобными компаниями;

официальные сайты компаний, разработавших приложения.

Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов.

15. Будьте аккуратны в интернете с незнакомцами

Виртуальная красавица (или красавец) предлагают обменяться интимными фотографиями? Не торопитесь соглашаться. Вы рискуете тем, что ваши снимки в жанре ню станут доступны в интернете всем желающим. Если вам предлагают личную встречу, тоже подумайте несколько раз. Романтическое свидание вполне может обернуться обычным ограблением.

16. И со знакомыми будьте аккуратнее

Люди и общение бывают разными: сегодня вы лучшие друзья, а завтра злейшие враги. И совместные фотографии, видео, цитаты из переписок могут быть использованы против вас. Поэтому прежде чем отправить что-то личное даже хорошо знакомому человеку, подумайте, не превратится ли в последующем этот контент в компромат.

17. Блокируйте подозрительных пользователей

Если у вас появились подозрения, что тот, кто пишет вам в интернете – мошенник, смело блокируйте его. Это не займет много времени, но поможет сберечь нервы и денежные средства. Многие из мошенников знают, как вызвать жалость, обмануть, запугать и заговорить человека. Поэтому с такими людьми лучше даже не вести бесед и смело отправлять в черный список. Также у нас есть удобная услуга «Безопасный режим», подключив которую, нежелательные сообщения, спам и интернет-подписки будут блокироваться автоматически – обратите внимание.

18. Будьте осторожны с бесплатными предложениями

Видите слова «бесплатно», «заработок без вложений», «скидки 99%» или что-нибудь еще в этом роде? Обходите такие сайты стороной. Все они предлагают золотые горы, но на деле вы либо потеряете деньги, либо заплатите солидную сумму за дешевую китайскую подделку.

19. Создайте отдельную карту для платежей в интернете

Необязательно вводить данные вашей основной банковской карты в интернет-магазинах. Зарегистрируйте отдельную, с которой вы будете оплачивать все онлайн-покупки, и не храните на ней большие суммы. Если ее реквизиты как-то попадут к мошенникам, ваши финансовые потери не будут слишком серьезными.

20. Постарайтесь ничего не покупать в социальных сетях

Сейчас немало товаров и услуг предлагается через «ВКонтакте». Если вас заинтересовали серьги ручной работы или торт, убедитесь, что человек, который их продает, реален. Может, у него уже делали заказ ваши знакомые. По крайней мере, если вы совершаете покупку впервые, не переводите предоплату на карту физического лица. Скажите, что отдадите деньги только при личной встрече и когда увидите товар. Следуйте этим рекомендациям, чтобы сохранить конфиденциальность, деньги и нервы.