50 правил безопасного Интернета

1) Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.

2) Если заходите в соцсеть или почту с чужого компьютера, не забудьте разлогиниться.

3) Выключайте Wi-Fi, когда им не пользуетесь. И себя защитите, и заряд батареи сэкономите. Обязательно отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.

4) Не доверяйте непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.

5) Не заходите в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Воспользуйтесь мобильным интернетом.

6) Помните: банки, сервисы и магазины никогда не рассылают писем с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные!

7) Отключите Сири на айфоне. Скорее всего, вы ей не пользуетесь, а вот мошенники уже научились выводить деньги через интернет-банк голосовыми командами.

8) Заведите несколько адресов электронной почты: личная, рабочая и развлекательная (для подписок и сервисов).

9) Придумайте сложный пароль, для каждого ящика разный. О том, как это сделать, мы писали здесь.

10) Везде, где это возможно, включите двухфакторную аутентификацию.

11) Регулярно меняйте пароли, обновляйте браузер и спам-фильтры.

12) Установите и обновляйте антивирусные программы. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.

13) Кликать по ссылкам, пришедшим в сообщениях от незнакомых людей — верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.

14) Не запускайте неизвестные файлы, особенно с расширением .exe

15) Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений.

16) Никогда не отвечайте на спам.

17) Если вам в мессенджер пришла просьба от знакомого с просьбой срочно выслать денег, ничего не отправляйте! Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.

18) Прочитайте книгу Кевина Митника «Искусство обмана». Митник — культовая фигура в среде информационной безопасности, его книга, как и история жизни, одновременно увлекательна и поучительна. Вы узнаете, как киберпреступники втираются в доверие к людям, манипулируя их чувствами.

19) Минимум личной информации: не публикуйте в сети домашний адрес, не пишите, в какое время вас не бывает дома, не описывайте свой постоянный маршрут, не хвалитесь крупными покупками и вообще постарайтесь не афишировать уровень достатка.

20) Регулярно выполняйте резервное копирование данных. Следуйте правилу «3-2-1»: создайте одну основную копию и две резервные. Сохраните две копии на разных физических носителях, а одну — в облачном хранилище (Google Диск, Яндекс.Диск, специальные решения от Акронис). Не забывайте бэкапить все устройства: смартфоны, планшеты, компьютеры/ноутбуки.

21) Чтобы никогда не терять деньги на незаметных платежах, не покупать дополнительных услуг по ошибке и точно заплатить за нужные, всегда читайте правила перед тем, как поставить галочку напротив чекбокса «согласен» и перейти к оплате.

22) Если в секретном вопросе вы указали девичью фамилию матери, которая сейчас есть в открытом доступе на ее страницах в соцсетях, обязательно поменяйте секретный вопрос.

23) Установите безопасный режим для ребенка. Для этого создайте отдельную учетную запись на сайте выбранной вами поисковой системы или используйте детские поисковики: Гогуль или Спутник.дети.

24) Говорите с ребенком об интернете: договоритесь, чтобы он сообщал вам о найденной нежелательной информации. Объясните, что не вся информация в сети достоверна, и приучите советоваться с вами по любому непонятному вопросу.

25) Не скачивайте сомнительные приложения и не пытайтесь это делать по неизвестным ссылкам. Пользуйтесь только официальными магазинами App Store, Google Play и Windows Market.

26) Совет для пользователей Google Chrome, Firefox и Opera: если вы часто путешествуете и выходите в сеть с ноутбука в общественных местах, установите специальное расширение для браузера для безопасного выхода в интернет. Рекомендуем HTTPS Everywhere от Electronic Frontier Foundation (EFF). По умолчанию этот плагин обеспечивает безопасное соединение для Yahoo, eBay, Amazon и некоторых других веб-ресурсов. Вы также можете добавить сайты по вашему выбору.

27) Постарайтесь ничего не покупать в социальных сетях, особенно с предоплатой. Мы вообще не рекомендуем переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).

28) Покупая в интернет-магазинах, сохраняйте здоровый скептицизм. Помните: цена не может быть слишком низкой, тем более, если вы рассчитываете приобрести оригинальную продукцию бренда.

29) Изучите историю магазина в сети, проверьте наличие контактов, выясните, можно ли туда приехать и познакомиться вживую. Читая отзывы, обратите внимание, чтобы они были разными. Заказные отзывы пишут люди, которым приходится делать это много раз в день, поэтому такие тексты будто написаны по шаблону.

30) Посмотрите, как на отзывы реагируют продавцы. Обратите особое внимание на негативные: если их отрабатывают, это хороший знак (причем ситуация должна быть конкретная, содержать номер заказа и т.п.).

31) Платите безопасно! Классический случай — вас переадресуют на защищенную страницу (адрес начинается с «https://»). Если нет, лучше не рисковать. По правилам эквайринга на сайте продавца должна быть информация о том, кто принимает платеж. Прочтите ее и сверьте с тем, что написано на следующей странице.

32) Заведите отдельную (можно виртуальную) карту для платежей в интернете.

33) Если для оплаты в интернете вы пользуетесь своей обычной картой, не храните на ней крупные суммы денег.

34) Подключите в своем банке СМС-информирование о всех операциях по картам и счетам. Так вы сможете быстро заметить, если ваша карта будет скомпрометирована, и заблокировать ее.

35) Страницы ввода конфиденциальной информации любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес

сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета.

36) Куда обращаться, если что-то пошло не так? Деятельность интернет-магазинов контролируется теми же организациями, что и обычных: Роспотребнадзором, Обществом защиты прав потребителей. Обязательно напишите на Горячую линию Рунета: www.hotline.rocit.ru

37) Будьте осторожны при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.

38) Халявы, случайных многомиллионных наследств и неизвестных богатых родственников, которые просто так хотят поделиться, не бывает.

39) Не делайте репостов жалостливых объявлений про милого котика, который срочно ищет дом (а в посте — телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.

40) Логотип известного благотворительного фонда еще не означает, что деньги пойдут туда — реквизиты счета могут быть подделаны. Если хотите помогать людям, делайте это только для лично знакомых или, например, с проектом dobro.mail.ru.

41) Не покупайте авиабилеты на незнакомых сайтах, особенно если они стоят гораздо дешевле, чем на всех остальных. Зайдите на настоящийбилет.рф и удостоверьтесь в подлинности ресурса. Также не лишним будет посетить сайт авиакомпании, которой вы хотите улететь, и сравнить цену билета на нужное направление.

42) Обращайте внимание на адрес страницы, где вы оказались: если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно.

43) Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чем проблема. Возможно, кто-то получил дубликат вашей симки и ее нужно срочно заблокировать.

44) По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт. Злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

45) Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту.

46) Лучше не пользоваться торрентами: если вы скачиваете нелегальный контент, вы не только обкрадываете любимого автора, но и можете загрузить зараженный вирусом файл.

47) Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать приглянувшийся фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

48) Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.

49) Не участвуйте в акциях с призами, где надо что-то оплатить, а потом попросить сделать то же самое еще нескольких людей. Это пирамида!

50) Всегда блокируйте экран компьютера, даже если отходите «всего на минуточку».