# Правила информационной безопасности в интернете

Значительную часть своей жизни мы проводим онлайн, сидя за компьютером и не выпуская из рук мобильного. Все чаще мы проводим время в интернете, но при этом забываем про бдительность, чем пользуются мошенники или наши враги. Какие ошибки делает 95% пользователей? Правила информационной безопасности в интернете, которые должен знать каждый.

Все больше мы уходим из реальной жизни в виртуальную, но люди совсем не представляют себе опасность, идущую от информационной среды. Мы слишком наивны и беспечны, что приводит к отрицательным последствиям.

Вспомни,  как часто обманывают бабушек и дедушек разные мошенники, которые ходят по домам. Сейчас есть много современных жуликов, которые охотятся в интернете на людей, похожих на тебя.

Современный мир сделал мошенников более изощренными, коварными и хитрыми. В ход идут многочисленные способы, которые невозможно предусмотреть или ожидать. Но можно быть более подкованным в информационной безопасности.

## Какие опасности есть в интернете?

«Для человеческой глупости нет патча». Кевин Митник

Какая исходит опасность в цифровом пространстве? Это же просто интернет! Существует море опасностей, которые могут причинить значительный вред обычному пользователю. Это может быть даже хуже, чем хулиганы на улице. Что тебе грозит?

- Анонимность и приватность, когда может пострадать репутация, карьера и жизнь.
- Финансовые онлайн-транзакции и снятие денег со счетов.
- Кибербуллинг и преследование другими людьми.
- Потеря аккаунтов в социальных сетях, управление группами или сайтами.
- Кража конфиденциальной информации: фотографии, паспортные данные, номер банковской карты.
- Рассылка СПАМа со своих аккаунтов или почты.
- Причинение вреда ближнему окружению, которое введено в заблуждение киберпреступниками.

## Правила информационной безопасности в интернете

Прочитай и запомни правила, которые важно знать каждому. Дай почитать близким, детям и всем, за кого переживаешь. Поехали. Не давай преступности воспользоваться доверчивостью хороших людей.

1. Используй безопасные и разные пароли везде. Регулярно их меняй. Отдавай предпочтение двухфакторной аутентификации и сверке по отпечатку пальца там, где наибольшие риски.

2. Не давай незнакомым людям позвонить. Они могут сделать что угодно, а не только сбежать с телефоном.

3. Никогда не оставляй своей телефон без присмотра. Всегда блокируй компьютер, даже когда отходишь на секунду.

4. Меньше рассказывай о себе любимом в интернете. Эту информацию могут использовать совсем не в хороших и корыстных целях злоумышленники.

5. Не открывай незнакомые письма, а особенно подозрительные. Не переходи по ссылкам в письме. Все это чревато тем, что подвергаешься повышенному риску. Это как есть еду, которую нашел в мусоре. Можно, но очень глупо и опасно.

6. Не покупайся на слова «халява», «бесплатно», «free», «скидка», «скачать бесплатно и без регистрации». Бесплатный сыр бывает в мышеловке.

7. Не принимай в друзья незнакомых людей. В лучшем случае это будет спам, а про худшие рассказывает интернет и скандальные передачи по телевизору.

8. Установи и обновляй антивирусные программы. Это важнейший шаг к улучшению информационной безопасности. Пользуйся бесплатными версиями антивирусов, если нет денег на платные версии.

9. Не пиши в социальных сетях, когда тебя не бывает дома. Не размещай фотки из отпуска до возвращения из него. Именно так очищают многие квартиры от всего ценного.

10. Общаясь с человеком будь готов к тому, что вы с ним можете войти в конфликт. Мужчина и женщина могут разойтись, друзья поссориться, коллеги позавидовать, а близкие предать. Не давай на себя компромат в информационном пространстве. Это могут быть фото, видео, сообщения или записи.

11. Регулярно обновляй программы на компьютере и приложения на телефоне. В старых версиях могут быть уязвимости, которые выйдут тебе боком. Если пользуешься старым телефоном, то имеет смысл сменить на новый, чтобы заменить старые и не поддерживаемые приложения. Это очень важно.

12. Не хвастайся покупками и уровнем благосостояния в интернете. Зачем привлекать к себе внимание хищников и меркантильных людей?

13. Когда заходишь в социальные сети или на почту с чужого компьютера, то не забудь выйти. Но лучше избегай это делать. Это повышенный риск.

14. Не пересылай конфиденциальную информацию через почту или социальные сети. Сразу удаляй сканы паспорта и документов от греха подальше.

15. Избегай пользоваться публичными Wi-Fi. С их помощью легко уведут пароли и другую конфиденциальную информацию. Лучше потратить немного денег на мобильный трафик, чем потом жалеть.

16. Тщательно проверяй программы и все, что скачиваешь с интернета, антивирусным обеспечением.

17. Крепость цепи определяется крепостью самого слабого звена. Часто твоим слабым звеном будут близкие. Поговори с близкими и детьми, чтобы они не стали жертвой обманщиков и жуликов.

18. Не отвечай на спам и подозрительные сообщения. Игнорируй.

19. Банки, сервисы и магазины не рассылают подозрительных писем. В них может быть просьба перейти по ссылке или сообщить какую-то информацию. Это киберпреступники тебе пишут.

20. Заведи несколько адресов электронной почты: личная, рабочая, развлекательная. Это значительно повысит уровень безопасности в сети.

21. Заведи отдельную карту для оплаты в интернете, а не используй зарплатную. Это позволит избежать многих проблем в будущем.

22. Проверяй внимательно адреса ссылок. Часто мошенники выбирают схожие названия, которые отличаются только одним символом или раскладкой.

23. Не запускай неизвестные программы, особенно с расширением .exe или .bat

24. Выключай Wi-Fi и блютуз, когда им не пользуешься. Это повысит информационную безопасность.

25. Не публикуй фото билетов и другой конфиденциальной информации.

26. Установи безопасный режим для ребенка, который взял твой телефон. Это избавит от многих неприятностей.

27. Почитай книги по кибербезопасности. Можно почитать книги консультанта по компьютерной безопасности и бывшего хакера Кевина Митника (Kevin Mitnick). Ты узнаешь, как мошенники втираются в доверие и обманывают людей. Соблюдай правила информационной безопасности в интернете и не доверяй никому.

28. Всегда читай правила при оплате в интернете. Самое важное могут написать самыми маленькими буквами.

29. Многие поддельные сайты копируют дизайн известных порталов. Не покупайся на это. Именно так теряют пароли. Лучше всегда вводи название через поиск и переходи по ссылке.

30. Не сохраняй в браузере пароли и номера банковских карт.

31. Анализируй какие мобильные приложения получают доступ к твоей информации. Зачем им знать контакты, получать фото, определять местоположение, давать доступ к камере или микрофону? Думай прежде.

32. Не храни большую сумму на карточке, которой платишь в интернете.

33. Внимательно проверяй адреса и контакты, на которые посылаешь важную информацию.

34. Скачивай на телефон только с App Store, Google Play и Windows Market.

35. Пришло сообщение с просьбой денег? В 99,99% случаях это мошенники. Перезвони человеку по телефону или сообщи его близким, что идет рассылка СПАМа.

36. Низкая цена в интернете может говорить о мошеннике или подделке товара.

37. Ничего не покупай с предоплатой и не переводи деньги на непонятные счета.

38. Хочешь скачать программу или что-то полезное, но взамен требуют номер телефона? Номер телефона попадет в базу спаммеров, а деньги за SMS могут снять с тебя.

39. Ищи негативную информацию про интернет-магазины или фирмы, перед покупкой или заключением сделки. Не доверяй фейковым отзывам.

40. Храни резервную информацию на разных носителях. Пусть будет три копии. Одна на компьютере, другая на внешнем жестком диске и третья у близких, которым доверяешь. Вместо последнего можно пользоваться облачными хранилищами.

41. Подключи SMS сообщения о всех операциях по картам и счетам.

42. Заблокируй смену SIM карты у оператора. Это будет мешать мошенникам поменять симку, заполучить информацию или увести деньги.

43. Избегай пользоваться взломанными программами. В них может быть много уязвимостей. Лучше не скачивай бесплатные приложения с интернета.

44. Не переходи по подозрительным ссылкам в интернете. Легко потерять информацию или подхватить парочку вирусов.

45. Общаясь в интернете, даже со знакомыми людьми, будь бдителен. Вместо знакомого человека может оказаться киберпреступник.

46. Многие приложения бывают бесплатные только несколько месяцев. Для этого они просят привязать свою карточку. После тестового периода услуги становятся платными, а деньги начинают списываться незаметно.

47. Потерял телефон, к которому привязаны карточка и все аккаунты? Срочно блокируй карту и меняй пароли.

48. Установи блокировку на телефон, чтобы при утере им не смогли сразу воспользоваться. Поставь программу для защиты украденного телефона и удаления информации.

49. Отключи голосовые интернет-помощники, которые могут использовать данные в своих целях.

50. Лох не мамонт — не вымрет. Не участвуй в пирамидах типа МММ, Кэшбери, бинарных опционах и прочем шлаке.

51. Не делай репостов про помощь для больных, животных или на другие благие дела. Делать это можно только в том случае, если лично знаешь организацию или человека. В противном случае ты становишься соучастником киберпреступления.

52. Тебе присылают сообщение, что компьютер был взломан? А теперь нужно выслать им деньги, чтобы компромат с камеры, микрофона или телефона не попал в посторонние руки? Это мошенники.

53. Заклеивай камеру, когда не пользуешься ей и отключай микрофон. Правила информационной безопасности в интернете помогут сохранить конфиденциальность и деньги.

54. Регулярно проверяй компьютер и телефон антивирусным обеспечением. Обращай внимание на подозрительное поведение компьютера или телефона.

55. Пользуйся только официальными сайтами драйверов производителей.

56. Часто выходишь в интернет со своего ноутбуку в незнакомых сетях? Установи предложение для безопасного выхода в интернет.

57. Девичья фамилия матери является плохим паролем. Как и другие простые словосочетания. Криптографическая стойкость важна для личной безопасности.

58. Регулярно проверяй услуги за интернет, мобильную связь и телевидение. Тебе могут навязать лишние услуги, которые будут стоить денег.

59. Если приходит сообщение о снятии денег или восстановлении аккаунта, то сразу действуй. Многие считают, что это ошибка, а потом становятся жертвами.

60. Лотереи, наследные принцы, казино и выигрыши посетителя №10000 рассчитаны на лохов. Правила информационной безопасности в интернете игнорируются только такими людьми.

61. Анализируй интернет-магазины. Насколько он реальный? Отдавай предпочтение проверенным и известным вариантам.

62. Часто за известными фамилиями, компаниями и организациями скрываются мошенники.

63. Все безопасные сайты сейчас начинаются с «https://», а не «http://». Особенно при оплате смотри на это. Также такие сайты помечены закрытым замочком в адресной строке.

64. Не набирай пароль в транспорте или общественном месте, когда могут подсмотреть через плечо.

65. Тебе пишет красотка и просит обменяться интимными фотографии? Ты хочешь отдать компромат на тебя в руки проходимцев? У тебя будут вымогать деньги, а иначе разошлют знакомым или распространят в интернете.

66. При столкновении с мошенничеством не бойся обращаться в правоохранительные органы или общество защиты прав потребителей. Защищайся, а не сдавайся.

**Правила информационной безопасности в интернете важно знать каждому. Если ты проявляешь беспечность в инете, то будь готов к самым негативным последствиям. Рост киберпреступлений будет только расти все сильнее с каждым годом.**

**Следование правилам информационной безопасности поможет сохранить конфиденциальность, деньги и нервы.**

А вы готовы к жизни в новом информационном пространстве?