
## Что такое двухфакторная аутентификация?

Двухфакторная аутентификация это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.

На практике это обычно выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.

## Какие еще существуют виды двухфакторной аутентификации?

Выше я уже упомянул рассылку специального кода в виде SMS и email-сообщений и USB-ключи и смарт-карты, используемые преимущественно для доступа к некоторым видам интернет-ресурсов и VPN-сетям. Кроме того, существуют еще генераторы кодов (в виде брелока с кнопкой и небольшим экранчиком), технология SecureID и некоторые другие специфические методы, характерные в основном для корпоративного сектора.

Возможно, вы даже сталкивались с ними, если были клиентом какого-нибудь не самого прогрессивного банка: при подключении интернет-банкинга клиенту выдавалась бумажка с заранее сформированным списком одноразовых паролей, которые вводятся один за другим при каждом входе в систему и/или совершении транзакции. Кстати, ваша банковская карта и PIN тоже формируют систему двухфакторной аутентификации: карточка — «ключ», которым вы владеете, а PIN-код к ней — «ключ», который вы запоминаете.


## Как защититься от компьютерных вирусов?

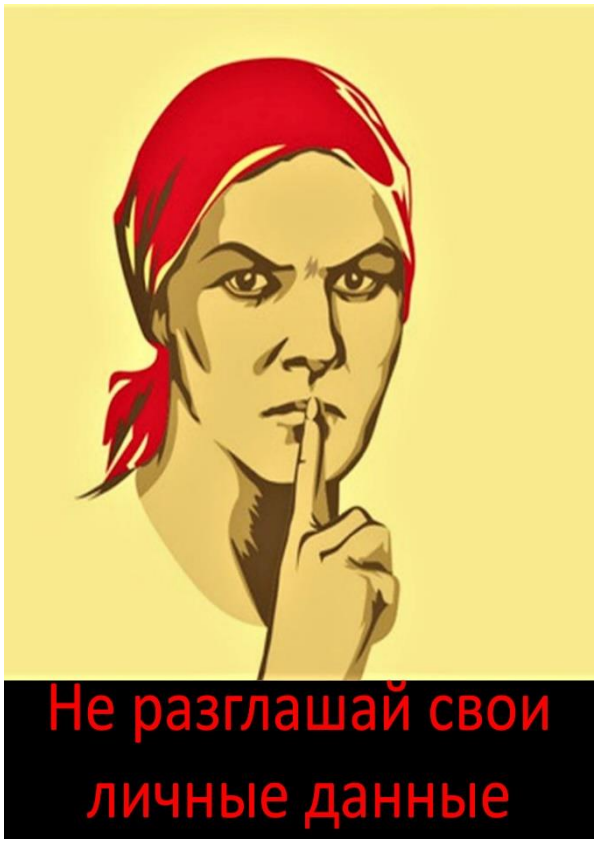
Рекомендуется установить антивирус: программное обеспечение для защиты от вредоносных программ на все свои устройства

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера.

1. Вирусы (Вредоносное ПО предназначеное для хищение ваших данных)
2. Черви (Вредоносное ПО, ухудшающее работу вашей системы)
3. Рекламное ПО (Всплывающая реклама в разных приложения)
4. Боты (Запрограммированные вирусы на управление вашим пк)
5. Баги (Ошибки в системе)
6. Майнеры (Вирус использующий ваше устройство в качестве добычи криптовалюты)

## Признаки заражения

Самый первый из них - снижение производительности, т.е. процессы происходят медленные, загрузка окон занимает больше времени, в фоновом режиме работают какие-то случайные программы. Еще одним настораживающим признаком может считаться измененных домашних интернет-страниц в вашем браузере.




## Как защитить личные данные в интернете?

Даже если вы используете безопасное соединение, Яндекс или другой интернет-гигант может отслеживать ваши действия в Сети. Даже ваш провайдер может это делать. Кстати, во многих странах провайдеры обязаны сохранять истории поиска своих клиентов, чтобы затем их можно было по требованию передать правоохранительным органам. Так что если вы хотите защитить свои данные в интернете, вам стоит позаботиться о том, чтобы в Сети за вами никто не следил.

Наконец, не забывайте выходить из своих аккаунтов, когда вы их не используете. При этом недостаточно просто закрыть вкладку или браузер. Например, ВКонтакте отслеживает своих пользователей, даже если в их браузере нет открытой вкладки с социальной сетью. Чтобы это прекратить, нужно полностью выйти из аккаунта – это особенно важно для аккаунтов онлайн-банков и брокерских счетов.

## Как обезопасить ваши персональные данные?

Для защиты онлайн-данных нужно обезопасить свои устройства и подключаться только к надежным сетям. Мы уже говорили о некоторых инструментах, которые помогут вам в этом, включая менеджер паролей. А теперь мы расскажем, как еще вы можете защитить свою личную информацию от хакеров.

1. Включите двухфакторную аутентификацию в своих учетных записях.
2. Не загружайте неофициальные приложения на свой смартфон.
3. Регулярно обновляйте программное обеспечение.
4. Не забывайте выходить из системы!