## **Рекомендаций для защиты своих данных в сети**

# **Защищайте свои пароли**



Самый важный и, наверное, самый известный совет. Речь не только о том, чтобы вы никому не сообщали свои пароли, это, я думаю, известно каждому.

Так же нужно помнить ещё несколько правил:

Не устанавливайте один и тот же пароль для нескольких аккаунтов. Используйте разные пароли на всех аккаунтах соц. сетей, электронных почт и т.п.

Не ленитесь придумывать сложные пароли: чем больше символов в пароле, тем труднее будет вас взломать, используйте как строчные, так и заглавные буквы, желательно использовать разрешенные спец. символы.

А если боитесь запутаться в своих паролях — используйте менеджеры паролей. Есть множество бесплатных приложений для хранения паролей в зашифрованном виде.

# **2. Используйте двухэтапную аутентификацию**



Двухступенчатая (или двухэтапная) аутентификация подразумевает, что для доступа к своему аккаунту вам приходится вводить информацию двух видов: та, которая у вас есть, и ту, которую вы знаете. Чаще всего это сводится к тому, что у вас просят заранее установленный пароль, а также код, присланный по СМС. Таким образом, даже если кто-то украдёт у вас пароль, этого будет недостаточно, чтобы использовать вашу учётную запись.
Конечно, двухступенчатая аутентификация занимает чуть больше времени, что многих раздражает (такую схему использует большинство интернет-банков, и порой очень хочется её отключить, но сделать это невозможно). Советуем подключить двойную проверку доступа там, где это можно сделать добровольно (например, у аккаунта в Gmail).

**3. Используйте SSL**

Многие сайты используют протокол SSL, обеспечивающий обмен данными между ними и пользователями в зашифрованном виде. Конечно, можно полагаться на эту защиту, но лучше установить специальное SSL-расширение для браузера.

В таком случае обмен зашифрованной — а значит, недоступной злоумышленникам — информацией будет производиться практически со всеми сайтами, которые вы посещаете.

 Пример таких расширений:

* HTTPS Everywhere
* KB SSL Enforcer
* HTTP Nowhere

# **4. При подключении к общественным Wi-Fi сетям используйте VPN**

Безопаснее всего пользоваться общественным интернетом через VPN (эта аббревиатура расшифровывается как virtual private network—частная виртуальная сеть). VPN проводит трафик через безопасную сеть, даже когда вы подключены к бесплатному Wi-Fi.



**5. На забывайте про антивирус!**

Регулярный запуск антивирусных программ (естественно, своевременно обновлённых) позволит вовремя обнаружить, если кто-то получил доступ к вашей системе и совершает подозрительные действия — например, редактирует системные файлы. Также антивирус сообщит о подключении к небезопасной сети.
 Существует множество хороших бесплатных антивирусов, занимающих немного места и не тормозящих работу системы. Не игнорируйте этот совет! Некоторые вирусы могут привести устройство в негодность!

**6. Уточняйте название сети**
 Порой мошенники создают сеть для кражи данных, которая по названию похожа на настоящую. Например, помимо официальной сети Starbucks вы можете увидеть Free Starbucks Wi-Fi.
 Если обнаруженный в кафе Wi-Fi вызывает у вас хоть малейшее сомнение, не стесняйтесь обращаться к работникам заведения и уточнять у них, как должна называться сеть.

# **7.  Меньше личной информации в сети**

Благодаря личной информации, которую вы вводите в интернете, Вас становится легче взломать.

Киберпреступники - умелые психологи. Вся ваша личная информация помогает им больше узнать о вас. И в дальнейшем использовать собранную информацию, чтобы получить доступ к вашим аккаунтам.

 

****

***Как обезопасить себя***

***в сети***

 ***ИНТЕРНЕТ***

****

***Как не стать жертвой киберпреступника***

***г. Кострома,***

***ул. Центральная, 25,***

***тел. 8(4942) 411231***

***http://www.kdm44.ru/***

[***https://vk.com/kostroma\_friends***](https://vk.com/kostroma_friends)

***mckostroma@yandex.ru***

***2019 год***