Автор: Administrator
23.07.2019 16:57 -

В 2019 году Центр кибербезопасности в Великобритании опубликовал список наиболее небезопасных паролей. Вдумайтесь, комбинацию «123456» используют 23 с лишним миллионов человек. Для того чтобы максимально защитить ваш личный кабинет в онлайн пространстве, нужно хорошенько подумать над паролем. Люди уделяют недостаточно внимания этому пункту, что ведет к потере конфиденциальных данных, а также личные профили таких людей используются мошенниками в корыстных целях.

Примитивные числовые комбинации

1. Цифры в порядке убывания или возрастания – первое «нет» в нашем списке. Простота в запоминании часто является причиной выбора подобных цепочек. Что может быть проще 5678 или 4321.
2. Одна цифра, повторяющаяся несколько раз — «нет» номер два. 11111111 или 777777 – слишком примитивно.
3. Числа + буквы – «нет» номер три. Такие комбинации зачастую встречаются в виде abc789 или 789abc.
4. Так же не стоит использовать несколько одинаковых паролей, если вы

скомпрометируете один, то другие будут тоже скомпрометированы.

Дата рождения.

Этот вид пароля изжил себя давным-давно. Особенно опасно ставить такую комбинацию, если дата вашего рождения находится в открытом доступе на страничке. Использовать ее не рекомендуется в любом сочетании – день/месяц/год, год/месяц/день, месяц/день/год и так далее.

Графические пароли.

Современные смартфоны прибегают к защите мобильного устройства при помощи графического ключа. Казалось бы, этот способ более сложен, однако след от вашего пальца на экране телефона это только один из способов узнать ваш пароль и взломать смартфон.

1. Ключ, похожий на букву или цифру. Не стоит использовать схему ключа, напоминающую какую-либо букву алфавита. Очень легко отгадать подобный пароль, если вы, например, придумали в качестве него первую букву своего имени или фамилии.
2. Короткий ключ. Не нужно скупиться и делать графический пароль коротким.Постарайтесь использовать как можно больше соединений точек. Существуют последовательности, которые могут соединить все 9 из 9 точек.

Ваше стремление сделать ключ легким и запоминающимся может привести к печальным последствиям. Поэтому, если вы хотите защитить свою персональную информацию, то не ленитесь придумать комбинацию, которую нельзя угадать. Используйте цепочки, состоящие из заглавных, строчных букв, нескольких цифр, специализированных знаков.