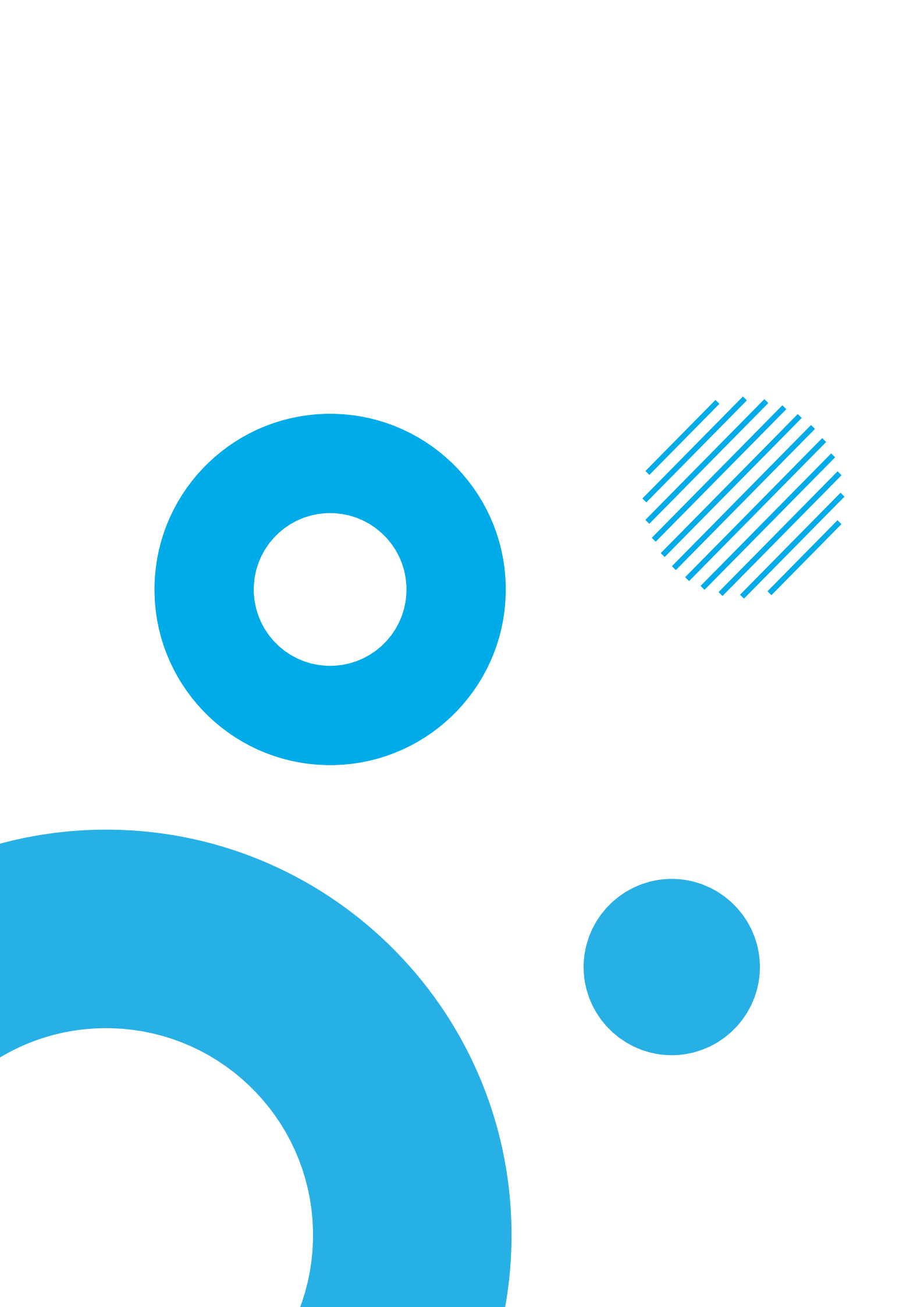
ВАШ НАДЕЖНЫЙ ПАРОЛЬ!

Личная цифровая безопасность начинается с пароля. Придумать себе надежный и качественный пароль – первое, что должен сделать любой пользователь Интернета.



Основные правила,
которые необходимо соблюдать, чтобы пароль был достаточно надежным и его было очень трудно подобрать:

1. **В пароле не должны содержаться личные данные** – дата рождения или любые другие даты, которые имеют к вам отношение, имена, фамилии, в том числе близких людей, клички домашних питомцев, никнеймы, а лучше вообще не использовать в пароле какие-либо слова.
2. **Пароль не должен быть коротким.** На сегодняшний день эксперты по безопасности в Интернете рекомендуют создавать пароли из 12-14 символов, однако такой пароль будет трудно запомнить.
3. **Чем больше разных символов содержится в пароле, тем лучше.** Важно, чтобы символы были разного типа – не только буквы или цифры, а их сочетание. Важно использовать не только строчные буквы, но и прописные (заглавные). Также рекомендуется добавить в пароль специальные символы – восклицательный или вопросительный знак, точку с запятой, «собаку» и т.д.

Практика показывает, что пароль из 8 символов достаточно надежен!

Основные ошибки,
которые допускают пользователи при создании пароля:

1. **Делают пароль таким, чтобы его было легко запомнить.** В результате получаются простые пароли, основанные на личных данных пользователя – имени, дате рождения, номере телефона, домашнем адресе и так далее. Например: **Ivan2005** или **katya2007**. Такие пароли очень легко может подобрать человек, который с вами знаком, а незнакомый злоумышленник может просто получить всю необходимую информацию из вашей страницы в социальных сетях.
2. **Делают пароли такими же, как и логины.** Например, если адрес электронной почты: **pochta.dima.2008@mail.ru**, то и пароль хозяин почты может придумать такой же: **pochta.dima.2008**. Это очень удобно, ведь такой пароль точно не получится забыть, достаточно помнить лишь сам адрес почтового ящика, но поверьте, мошенники знают об этом и это будет первая комбинация, которую они опробуют, чтобы взломать вашу почту, социальные сети или другой аккаунт.
3. **Делают длинный пароль, а не качественный.** Многие люди уверены, что длинный пароль = надежный пароль, на самом деле это не так. Злоумышленники для подбора пароля могут использовать специальные программы, а такой программе абсолютно все равно, сколько символов в вашем пароле. Длинную комбинацию из 21 цифры такая программа угадает всего лишь за несколько секунд.

Как создать надежный пароль:

1. **Придумайте случайную комбинацию** букв таким образом, чтобы вы могли ее запомнить. Лучше, чтобы это не было настоящее слово. Запишите ее буквами двух регистров (заглавными и строчными). Например: **LamaEk**.

1. **Добавьте к этим буквам несколько цифр.** Цифры не должны быть вашим возрастом, датой рождения, номером документа или чем-либо еще, что имеет смысл. Например: **LamaEk857**.

1. **Добавьте один или несколько символов,** например: **LamaEk857@**. Такой пароль достаточно сложен и гораздо надежнее, чем привычные нам пароли «admin», «password» или «1234». Его невозможно просто угадать, а подбор пароля с помощью специальных программ займет очень много времени.

Альтернативный способ: найдите в Интернете любой генератор случайных паролей. Там вы можете настроить пароль какой хотите длины, какие символы вы хотите в нем видеть и иные меры предосторожности. Выбирайте случайные пароли, пока не найдете такой, который сможете запомнить.

Внимание!

Не используйте в пароле слова с заменой букв на символы. Например: p@ssword или $vetlana. Такие пароли очень легко и быстро подбираются с помощью программ. Делайте разные пароли для разных сайтов. Можно сделать несколько вариаций одного и того же пароля. Например: LamaEk857@, LamaEk857!! и LomoEk857!!! – три разных пароля, при этом их хозяин сможет запомнить каждый из них.

Чаще меняйте пароли. К сожалению, на сегодняшний день большинство аккаунтов взламываются не с помощью подбора пароля, а в результате утечки данных. С сайтов, которыми мы пользуемся, иногда утекает большое количество информации о пользователях, в том числе логины, пароли и т.д. В этом случае злоумышленникам не нужно ничего взламывать, они просто узнают ваш пароль из утечки, независимо от того, насколько он длинный и сложный.

Следите за новостями. Если сайт, сервис, социальную сеть или приложение, которым вы пользуетесь, взломают, информация об этом может появиться в новостях. В таком случае очень важно сразу же поменять пароли на этих сайтах!

Любой пароль можно взломать или обойти. Рекомендуем подключать функцию «двухфакторной аутентификации»: подтверждение входа с помощью кода из СМС или письма на почте. На сегодняшний день эта функция доступна для большинства популярных сайтов. Она очень сильно повысит вашу безопасность.

Эксперты в сфере информационной безопасности рекомендуют менять пароли раз в месяц и даже чаще. Можно не придумывать совершенно новый пароль, а взять старый, поменять в нем некоторые символы, цифры, добавить новые.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru