ПРОФИЛАКТИКА
федеральный центр

Принципы беседы о безопасности с детьми

ПРОФИЛАКТИКА
федеральный центр

Учёт возраста ребёнка

Дошкольники (до 6 лет)

Малыши должны усвоить базовые навыки безопасного поведения. Для усвоения и выработки оптимального поведения в большей степени подходят игровые формы обучения, имитирующие поведение на кухне, на улице, на детской площадке.

Младшие школьники (7–11 лет)

В этом возрасте список потенциальных угроз становится больше: появляются социальные и информационные. Это также период введения новых понятий: ответственности за поступки и понимание последствий тех или иных действий.

Подростки (11–18 лет)

Самый сложный период в плане осознания ценности жизни, личных способностей и границ, отсутствия критичного мышления, смены авторитетов, огромного негативного или подражательного информационного потока. Задачей родителей становится соблюдение баланса между контролем и доверием. Важно привлекать подростка к обсуждению, поощрять высказывание личного мнения, и, если позволяет ситуация, давать возможность принимать решения самостоятельно.

ПРОФИЛАКТИКА
федеральный центр

Поддержка эмоционального состояния

Важно в ежедневном общении семьи создавать атмосферу доверия и открытости, поддерживать открытый диалог.

! *Разговоры об опасностях вызывают сильные чувства, это может быть и тревога, и показная смелость.*

Родителям необходимо отслеживать собственные эмоции во время общения поддерживать и принимать ребёнка в любой ситуации, совместно принимать решения при возникающих проблемах.

ПРОФИЛАКТИКА
федеральный центр

Последовательность

- ✅ Правила устанавливаются для всей семьи.
  Взрослые должны соблюдать то, что требуют от подростков: быть вежливыми, в быту аккуратными, разумными на дороге, уважительными к старшим.

- ✅ Обучение навыкам безопасности начинается с простых, самых распространённых примеров и переходит к более сложным темам.

Использование наглядных примеров

- ✅ Визуальный ряд воспринимается детьми наиболее ярко, поэтому можно использовать видеоматериалы, примеры из книг или СМИ.

- ✅ Можно рассказать о реальных случаях, которые произошли со знакомыми людьми.
  Обсудите, как можно было избежать неприятностей в приведённом примере.

ПРОФИЛАКТИКА
федеральный центр

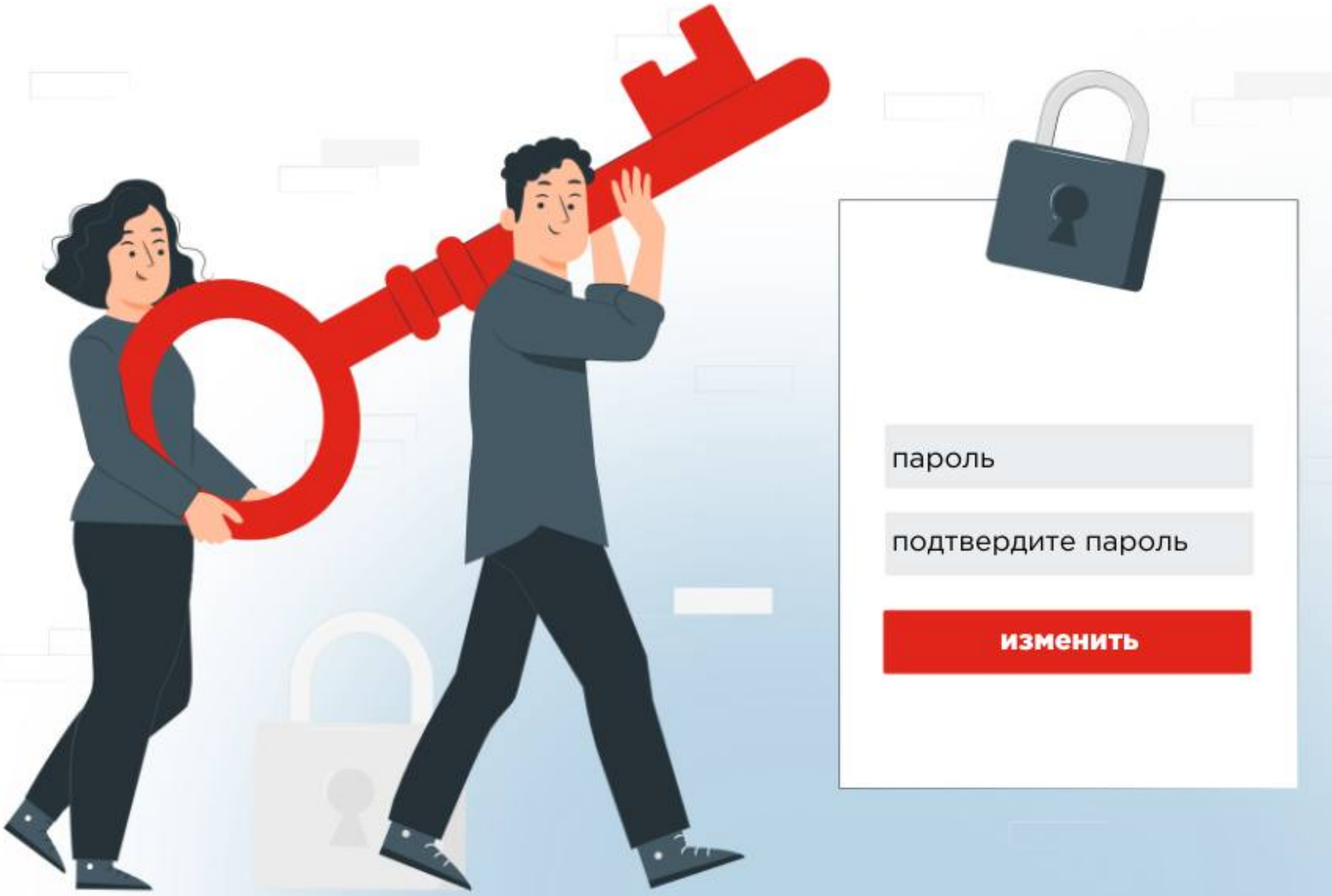
Отработка навыков

Только предупредительной беседой невозможно достичь результата, необходимо практиковать и систематически повторять, какие реакции на угрозу будут максимально эффективны.

Помимо общих правил безопасности важно научить ребёнка навыками самозащиты, он должен знать, как связаться с экстренными службами, как вести себя с агрессивными людьми, помнить наизусть телефоны родителей.

! Навыки отрабатываются в безопасной обстановке.

БЕЗОПАСНОСТЬ ПАРОЛЕЙ: ЧТО НУЖНО ЗНАТЬ?



ЗАЧЕМ ВООБЩЕ НУЖЕН СЛОЖНЫЙ ПАРОЛЬ? КОМУ НУЖНЫ МОИ СТРАНИЦЫ, Я ЖЕ НЕ ЗНАМЕНИТОСТЬ?

Переписка пользователей, их личные данные всегда была объектом интереса различных сторон. В социальных сетях мы часто делимся самым сокровенным, а для мошенников это отличная возможность узнать о нас побольше, чтобы потом использовать данные в преступных целях.

Взламывают не только аккаунты известных личностей, но и простых людей. ***Поэтому защищать свою страницу нужно вне зависимости от того, как много у вас подписчиков и как часто вы общаетесь в сети.***

КАК МОГУТ УКРАСТЬ МОЙ ПАРОЛЬ?

Злоумышленники изобрели целую плеяду способов хищения цифровых данных. Вот лишь несколько из них:

ТРОЯН

Эти тихие шпионы, которые могут попасть на ваше устройство через **программу, загруженную в Интернете.** Чем дольше они остаются незамеченными, тем дольше смогут выполнять свою работу — передавать злоумышленникам украденные у вас данные.

ПУБЛИЧНАЯ СЕТЬ WI-FI

Злоумышленники могут перехватить данные, отправляемые по сети, если вы используете сеть Wi-Fi **без шифрования или защищенную старым протоколом WEP.**

КАК МОГУТ УКРАСТЬ МОЙ ПАРОЛЬ?

Злоумышленники изобрели целую плеяду способов хищения цифровых данных. Вот лишь несколько из них:

ФИШИНГ

Обычно фишинговые ссылки ведут на поддельные сайты, на которых требуется ввести личные данные. Неважно, кто отправил вам письмо: **всегда внимательно смотрите на веб-адреса**, которые вам присылают.

АТАКИ ЧЕРЕЗ БРАУЗЕР

Нередко пароли крадут через **уязвимости** браузеров или через браузерные расширения.

ВНЕШНИЕ УТЕЧКИ

Утечки часто происходят и в удаленных интернет-сервисах, которыми мы пользуемся. В результате взлома такого сайта хакеры могут получить огромную базу пользователей вместе с их паролями и персональными данными. **Поэтому стоит обновлять пароль хотя бы раз в 2-3 месяца**

Я ЗАБЫЛ СВОЙ ПАРОЛЬ, А СЕРВИС ЗАСТАВЛЯЕТ МЕНЯ СОЗДАВАТЬ НОВЫЙ. ПОЧЕМУ МНЕ НЕ МОГУТ НАПОМНИТЬ ПРОШЛЫЙ?

Ни один сервис не знает, какой у вас на самом деле пароль. По ту сторону экрана он выглядит как **хэш-значение** — рандомный набор букв и цифр определенной длины.

Вот пример преобразования одного из знаменитых паролей:

admin ⇄ **21232f297a57a5a743894a0e4a801fc3**

Такие хэш-значения хорошо известны взломщикам, именно поэтому не стоит использовать просты пароли при защите аккаунта.

КАК ТОГДА ЗАЩИТИТЬ СВОЙ АККАУНТ ПРАВИЛЬНО?

Для начала запомните, что не стоит использовать простые слова: клички любимых питомцев, дата рождения, футбольный клуб, за который вы болеете — всю эту информацию часто можно найти в открытом доступе.

Не стоит пользоваться и известными фразами:

123456

123456789

qwerty

password

admin

ПРОФИЛАКТИКА
федеральный центр

ПРАВИЛА ЗАЩИТЫ ВАШЕГО АККАУНТА:

1. Чем больше символов, тем пароль надежней.

2. Идеальный пароль содержит всего понемножку: цифры, большие и маленькие буквы, специальные символы. Буквы не должны образовывать слово.

3. Хороший пароль невозможно запомнить, поэтому лучше довериться менеджеру паролей.

4. Для пароля сойдёт и длинная фраза, только никаких цитат.

5. Один аккаунт – один пароль.

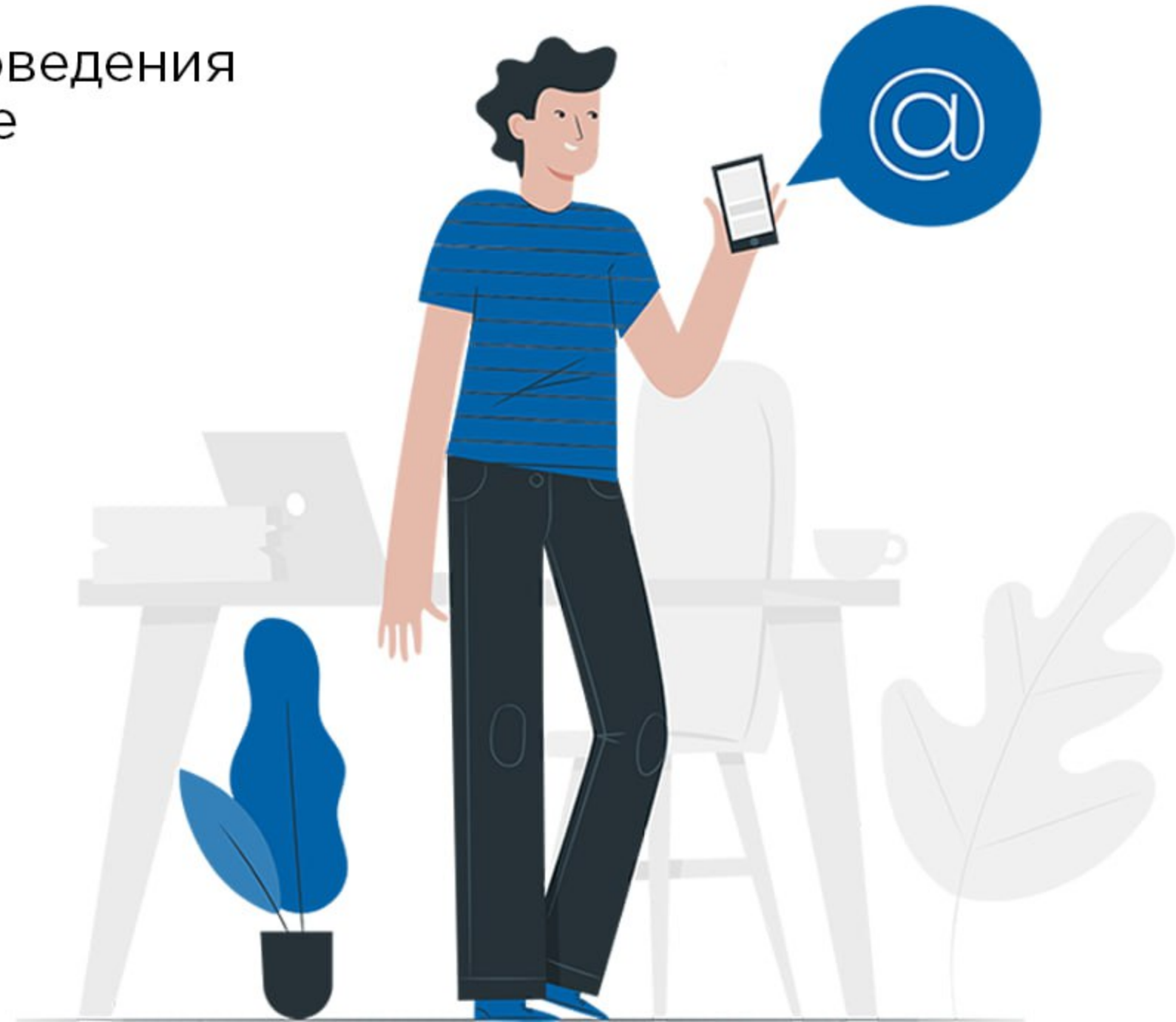
6. Не забывайте периодически менять пароль.

Профилактика

ПРОФИЛАКТИКА
федеральный центр

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Правила поведения в интернете



ПРОФИЛАКТИКА
федеральный центр

1 Настройте родительский контроль

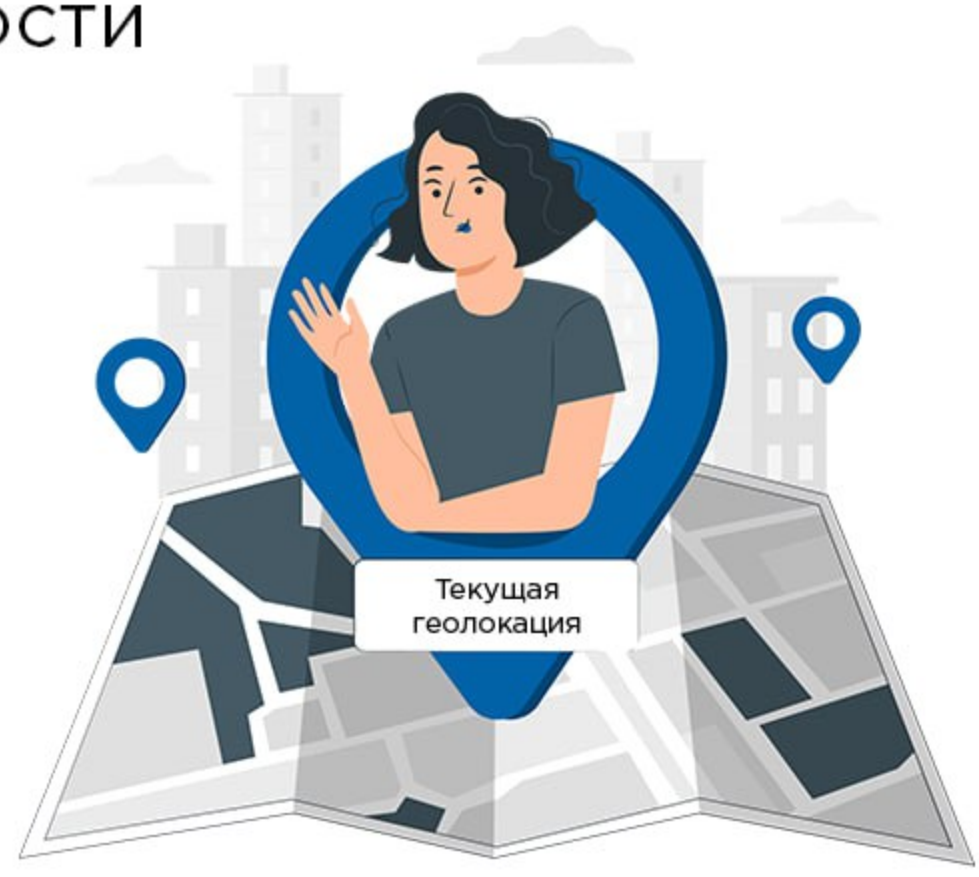
Вы можете:

- ✅ ограничить экранное время;
- ✅ установить фильтры на поисковую выдачу и материалы;
- ✅ получить отчёты об активности ребёнка.

ПРОФИЛАКТИКА
федеральный центр

2 Включите службы геолокации

Это поможет в случае экстренной необходимости узнать, где находится ребёнок, а в случае кражи телефона его удастся скорее найти.



ПРОФИЛАКТИКА
федеральный центр

3 Помогите ребёнку установить пароль

Это поможет предотвратить взлом личных страниц и утечку данных.

ПРОФИЛАКТИКА
федеральный центр

4 Расскажите о правилах поведения в интернете и сетевом этикете

- [x] Расскажите про травлю в Сети и помните:
ребёнок должен знать, что он может вам доверять, и не бояться обратиться за помощью.

- [x] Изучите правила поведения с мошенниками и расскажите ребёнку, как он может действовать в случае столкновения с ними.

Полезное

ПРОФИЛАКТИКА
федеральный центр

ЦИФРОВАЯ БЕЗОПАСНОСТЬ: РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

ЦИСМ

ПРОФИЛАКТИКА
федеральный центр

Что может повлечь сетевые риски:

временное отсутствие учебной деятельности

→ меньшая включенность в сообщества, связанные с учебой, поиск новых интересов в сетевом пространстве

отсутствие систематического общения с одноклассниками

→ возможное ощущение социальной изоляции, поиск новых знакомств в социальных сетях

нарушение режима сна, повышение активности в Интернете, гейминг в ночное время

→ риск возникновения депрессивного состояния

ПРОФИЛАКТИКА
федеральный центр

Рекомендации родителям:

★ организуйте онлайн-досуг ребенка в освободившееся от учебы время, это могут быть:

· развивающие занятия, соответствующих интересам,

· видеоуроки на проверенных цифровых платформах,

· фильмы, каналы с видеоконтентом (их, например, рекомендует Центр экспертизы Института воспитания);

рекомендации Центра экспертизы Института воспитания

★ Для детей **до 14 лет,** установите соответствующие настройки («семейные», «детские»), минимизирующие встречу с деструктивным контентом

ПРОФИЛАКТИКА
федеральный центр

Рекомендации родителям:

- способствуйте вовлечению ребенка в реальные группы сверстников, объединенных общей конструктивной деятельность:

  это могут быть кружки, секции, лагеря

- обратите внимание подростка **на опасности общения** в Интернете с незнакомцами, которые могут скрываться за чужими фотографиями

- договоритесь с ребенком о допустимом количестве сетевой активности в сутки

ПРОФИЛАКТИКА
федеральный центр

Рекомендации родителям:

- развивайте цифровую грамотность вашего ребенка:
  расскажите, что в случае, если он встретился в Интернете с неприятным или пугающим контентом, он может поделиться этими фактами с родителями

- при обнаружении признаков вовлеченности ребенка в деструктивное поведение в офлайн и онлайн среде следует обратиться за помощью к специалистам – психологам, службам горячих линий.

Кибербезопасность

ПРОФИЛАКТИКА
федеральный центр

Как противостоять вербовке в сети?

ПРОФИЛАКТИКА
федеральный центр

ЧТО ТАКОЕ ВЕРБОВКА?

Вербовка — это процесс, в ходе которого злоумышленник пытается убедить человека присоединиться к незаконной или опасной деятельности.

Это могут быть:

- участие в экстремистских или террористических группировках;
- участие в несанкционированных акциях или митингах;
- сбор информации или выполнение задач в интересах злоумышленников.

КТО В ЗОНЕ РИСКА?

Чаще всего вербовщики обращают внимание на людей, которые:

- нуждается в эмоциональной поддержке и одобрении;
- сталкивается с трудностями, такими как стресс или финансовые проблемы;
- открыто выражает недовольство социальной или политической обстановкой в обществе;
- является подростком или молодым человеком, активно пользующимся интернетом.

ОСНОВНЫЕ ПЛОЩАДКИ ДЛЯ ВЕРБОВКИ

Социальные сети

Мессенджеры

Онлайн-игры

Чаты на форумах
и образовательных платформах

ПРОФИЛАКТИКА
федеральный центр

ПРИЗНАКИ ВЕРБОВКИ: НА ЧТО ОБРАТИТЬ ВНИМАНИЕ?

Общение с вербовщиком может начаться с невинного предложения, но есть признаки, которые должны вызвать подозрения:

- неожиданное сообщение от незнакомого человека с предложением дружбы, сотрудничества или заработка;
- попытки вызвать сильные эмоции: чувство несправедливости, страха, жалости или гнева;
- шокирующий контент;
- сомнительные предложения, которые обещают быструю и лёгкую прибыль или участие в «важной миссии»;
- давление, когда требуют быстрых решений или утверждают, что это «единственный шанс».

ПРОФИЛАКТИКА
федеральный центр

КАК ПРОТИВОСТОЯТЬ ВЕРБОВКЕ?

✔ Развивать критическое мышление, расширять кругозор и ставить глобальные жизненные цели — это поможет сохранять устойчивость в ситуациях, когда вас или ребёнка пытаются завербовать.

✘ Не вступать в разговоры с незнакомыми людьми и не соглашаться на сомнительные предложения.

✘ В случае, если пользователь оказывает давление, необходимо заблокировать его аккаунт.

✘ Сообщить администрации социальной сети о подозрительном профиле.

✘ Сохранить сообщения, чтобы при необходимости предоставить их правоохранительным органам.

БОТ/РЕАЛЬНЫЙ ЧЕЛОВЕК В СОЦИАЛЬНЫХ СЕТЯХ: КАК ОТЛИЧИТЬ?

Профиль-бот

аккаунт, созданный с целью распространения, пропаганды или отстаивания информации для достижения определенных целей организаций, конкретного человека или групп людей в интернет-пространстве, распространения ложной информации и разжигание конфликтов в сети Интернет

Для бота характерно:

- Отсутствие аватара/реальной фотографии, автарка в виде абстрактной картинки, мема, изображения знаменитости или животного

- Бот может копировать личность реального человека.
  Имя пользователя тоже может быть украдено или сгенерировано, при этом личная информация, посты отсутствуют

- Профили-боты не публикуют собственный контент.
  На стенах таких аккаунтов можно найти репосты, по которым невозможно понять увлечение человека, рекламу, посты по тематике, ради которой и создан этот профиль.

Для бота характерно:

- В друзьях по большей части
  такие же страницы-боты или реальные люди
  с большим количеством друзей, которые
  добавляют всех бесконтрольно, уже удаленные
  или заблокированные страницы

- На стене пользователем размещены публикации
  с коротким временным промежутком
  (например, много публикаций за один день,
  через день)

Боты активно проявляют себя в комментариях:

- используют одни и те же формулировки
- распространяют рекламу и спам
- распространяют ложную информацию, которая может спровоцировать конфликты в комментариях
- размещают комментарии через короткие промежутки времени

Как самостоятельно выявить профиль бота:

1 **Опечатки и орфографические ошибки мешают боту воспринимать текст.** Если обратиться к нему с помощью сообщения, содержащего несколько ошибок в слове, может последовать ответ, отходящий от логики беседы

Как самостоятельно выявить профиль бота:

2 **Отсутствие реакции на аббревиатуры и сокращения.**

Бот не чувствует эмоциональный или саркастический контекст, поэтому не смогут поддержать беседу

Важные правила:

НИКОГДА НЕ ВЕДИТЕ ДИАЛОГИ ЛИЧНОГО ХАРАКТЕРА С НЕЗНАКОМЫМИ ВАМ ЛЮДЬМИ

ЕСЛИ ЕСТЬ ХОТЬ МАЛЕЙШЕЕ ПОДОЗРЕНИЕ В ДОСТОВЕРНОСТИ АККАУНТА В СОЦСЕТИ ИЛИ НА ФОРУМЕ, ТО ОБХОДИТЕ ЕГО СТОРОНОЙ

Полезное

ПРОФИЛАКТИКА
федеральный центр

7 ПОЛЕЗНЫХ ЦИФРОВЫХ ПРИВЫЧЕК

ЦИСМ

1. СМАРТФОН НЕ ДОЛЖЕН МЕШАТЬ ВАЖНЫМ ДЕЛАМ

Часто выполнению уроков, занятиям с репетитором мешает бесконечный поток уведомлений на телефоне. Чтобы эффективнее погружаться в важные занятия и не отвлекаться каждые 5 минут на смартфон, **отрегулируйте оповещения.**

СОВЕТ

Можно отключить их или установить приложение, которое в течение установленного времени блокирует все функции телефона и просто выращивает виртуальное дерево.

2. ИЗУЧИТЕ ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ СВОЕГО ТЕЛЕФОНА

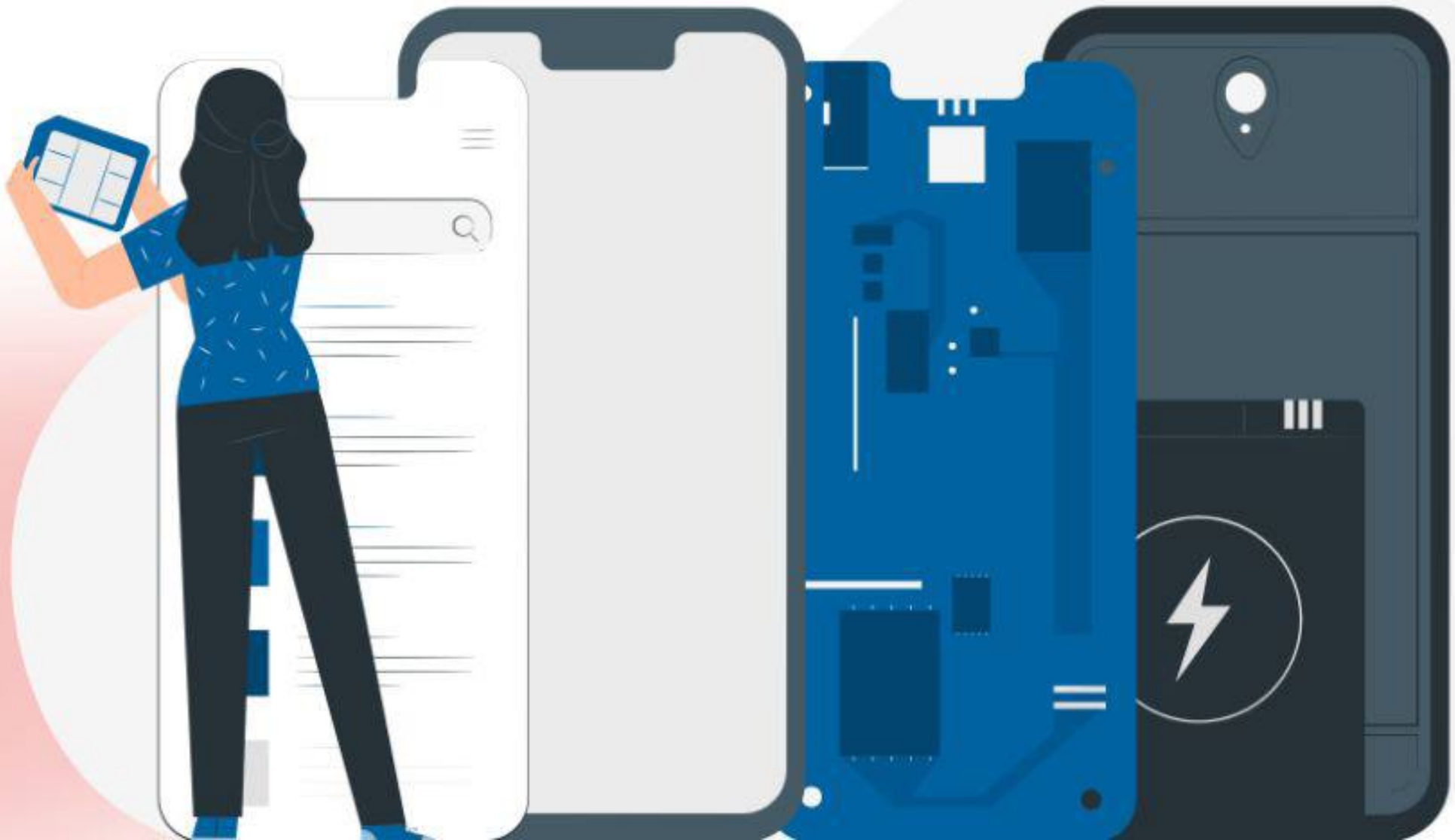
Отключение микрофона, увеличение ресурса батареи, копирование настроек для фотографий – это лишь малая часть того, что «умеет» смартфон, стоит лишь **чуть глубже изучить вопрос.**

3. ЦИФРОВОЙ ЭТИКЕТ

В сети тоже есть свои правила и нормы этикета. Соблюдая их, вы можете сделать общение комфортнее. Не забывайте, например, уточнить у собеседника, **удобно ли ему прослушать голосовое сообщение** или посмотреть видео, прежде чем его отправлять.

4. РЕЗЕРВНЫЕ КОПИИ

Чтобы не терять важные данные, научитесь систематизировать информации на устройствах. Привычка создавать резервные копии важной информации с помощью **флешек, жестких дисков и облачных хранилищ,** однажды может точно вам пригодиться.



5. НАДЕЖНЫЕ ПАРОЛИ

При регистрации аккаунтов не стоит использовать одинаковые пароли во всех социальных сетях и мессенджерах.

Пароли с высокой надежностью обычно состоят из большого количества знаков, содержат цифры, специальные символы, маленькие и большие буквы латинского алфавита.

Не нужно включать в пароль личную информацию о себе, своих друзьях и членах семьи – даты рождения, номера телефонов и т.д.

Примеры ненадежных паролей:

qwerty
12345abc
098765
password

Примеры надежных паролей:

ab6Tjdvn*9
kl_12NmOll3
8Bm__cxr6*sq!
lo*!bNml56c

6. БДИТЕЛЬНОСТЬ ПРИ ОБЩЕНИИ В СЕТИ

В интернете, также как и на улице, не стоит отвечать на вопросы людей, **которых вы не знаете**, рассказывать им о себе и своих близких. Если вам предлагают совершить действия, которые кажутся **странными и подозрительными,** всегда сохраняйте бдительность и сообщайте о проблеме в соответствующие органы.

7. ВСЕ, ЧТО ПОПАЛО В ИНТЕРНЕТ, ОСТАЕТСЯ ТАМ НАВСЕГДА

Научитесь внимательно относиться к тому, какой контент вы выкладываете, заботьтесь **о своей цифровой репутации.** В случае возникновения сомнений всегда можно воспользоваться отложенной публикацией, чтобы через время спросить себя ещё раз: **«Точно ли я хочу это выложить?»**