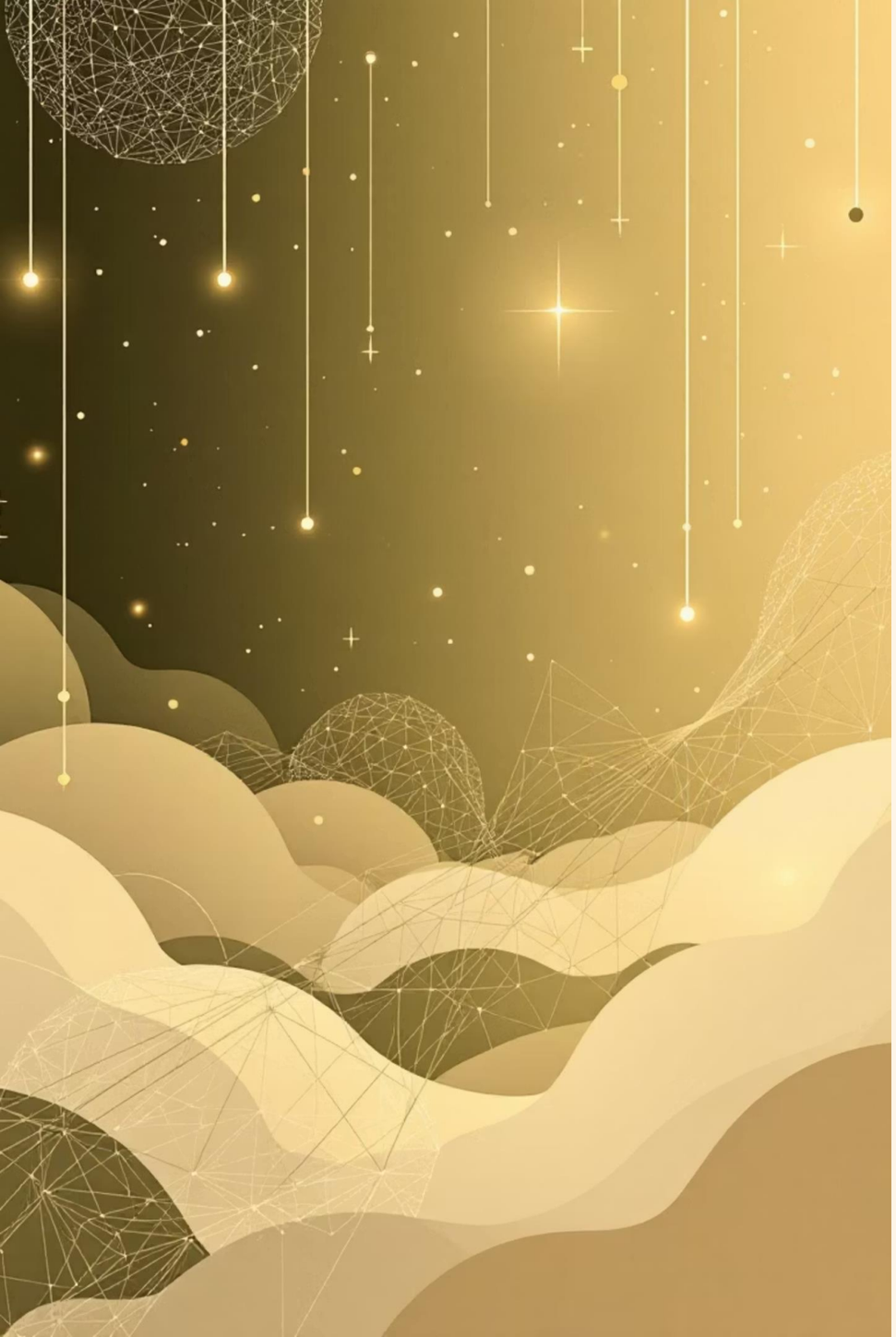


4 февраля – Всемирный день безопасности в интернете

«Шагните безопасно в цифровой мир»

Урок безопасности: «Основные правила охраны личной границы человека»

ОСНОВЫ БЕЗОПАСНОСТИ

Почему безопасность в интернете важна?

Мир возможностей и рисков

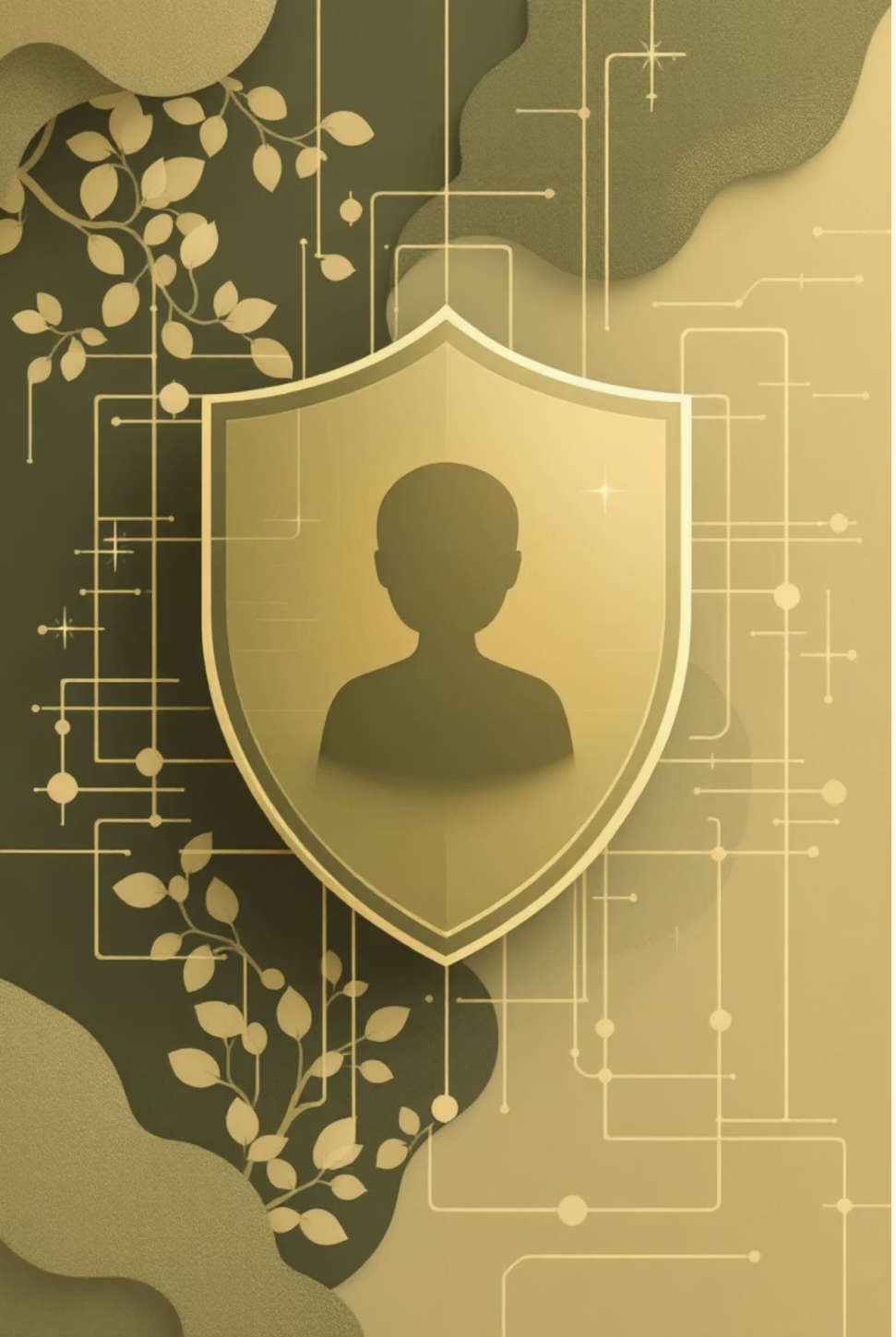
Интернет — это безграничное пространство для обучения, общения и развлечений, но также источник потенциальных опасностей.

Защита подрастающего поколения

Ежедневно миллионы детей и подростков активно используют сеть. Наша задача — научить их ориентироваться в этом мире безопасно.

Охрана личного пространства

Безопасность в интернете означает защиту твоих личных данных и границ в цифровом пространстве от нежелательного вторжения и угроз.



Что такое личная граница в цифровом мире?

В цифровом пространстве твоя личная граница — это всё, что связано с твоей личностью и чем ты не хочешь делиться без разрешения.

Личная информация

Твои фотографии, видео, переписки, контактные данные, пароли и местоположение — всё это составляет твою личную информацию.

Принцип неприкосновенности

Личная граница определяет, какая информация остается только твоей и не подлежит распространению.

Нарушение границ

Кибербуллинг, попытки мошенничества, несанкционированный доступ к твоим данным — это примеры нарушения личных границ.

ЗОЛОТЫЕ ПРАВИЛА

Основные правила охраны личной границы

1 Конфиденциальность паролей

Никогда и никому не сообщай свои пароли и личные данные, особенно незнакомым людям.

2 Осторожность с ссылками

Не открывай подозрительные ссылки, вложения или файлы, которые приходят от незнакомых отправителей. Они могут содержать вредоносные программы.

3 Контроль над публикациями

Будь предельно осторожен с тем, что ты публикуешь в социальных сетях. Любая информация становится частью твоего цифрового следа и может быть использована против тебя.

4 Сообщай взрослым

Если что-то в интернете кажется тебе подозрительным, неприятным или вызывает беспокойство, не стесняйся сразу же рассказать об этом родителям или учителю.

ЦИФРОВОЙ СЛЕД

Цифровой след: что это и почему он важен?

Что такое цифровой след?

Каждое твое действие в интернете — посещение сайтов, публикации, комментарии, скачивания — оставляет уникальный «след».

Управление доступом

Важно постоянно контролировать, какую информацию ты делаешь публичной и кому даешь доступ к своим данным.

Риски использования данных

Эти данные могут быть собраны и использованы мошенниками, рекламными компаниями или просто незнакомцами для самых разных целей.

Долговечность информации

Помни, что информация, однажды опубликованная в интернете, остается там навсегда, даже если ты ее удалил.

НАДЕЖНЫЕ ПАРОЛИ

Как создать надёжный пароль?

Сложная комбинация

Используй комбинацию из заглавных и строчных букв, цифр и специальных символов. Чем длиннее и разнообразнее пароль, тем он надежнее.

Избегай очевидного

Не используй личные данные (дату рождения, имя питомца) или простые слова. Они легко подбираются хакерами.

Разные пароли

Для каждого аккаунта используй уникальный пароль. Так, если один аккаунт взломают, остальные останутся в безопасности.

Двухфакторная аутентификация

Включай двухфакторную аутентификацию (2FA) везде, где это возможно. Это добавит дополнительный уровень защиты твоему аккаунту.

ОНЛАЙН-ОБЩЕНИЕ

Общение в интернете: правила безопасности

Избегай переписок с незнакомцами: *Не начинай общение с теми, кого не знаешь в реальной жизни, без разрешения родителей.*

Не делись личным: *Никогда не передавай свои личные данные, фото или видео незнакомым людям в сети.*

Откажись от встреч: *Категорически нельзя соглашаться на встречи с людьми, с которыми ты познакомился в интернете.*

Будь бдителен: *Помни, что в интернете человек может выдавать себя за кого угодно. Не верь всему, что тебе говорят.*

За какие слова в интернете грозит наказание

В Казахстане действует ряд законодательных мер, которые предусматривают ответственность за комментарии или репосты в Сети. Чего нельзя делать уже в 14 лет.

Какие высказывания влекут уголовную ответственность?

В Уголовном кодексе Казахстана указаны несколько статей, которые предусматривают ответственность вплоть до лишения свободы за различные высказывания.

Статья 130 УК РК - Клевета

Например, за клевету предусмотрены штрафы (до 2000 МРП, размер одного МРП – 3932 тенге), исправительные работы и ограничение/лишение свободы до двух лет.

Клевета - распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. Клевета может быть распространена через разговоры, публикации в интернете, мессенджеры и другие каналы коммуникации

Статья 131 УК РК Оскорбление

За оскорбление, выраженное в неприличной форме, через медиа/интернет, можно получить штраф в 200 МРП или общественные работы на 180 часов.

Оскорбление – намеренное унижение достоинства человека с использованием грубых и неприличных слов и жестов. Оскорбление может выражаться не только в устной или письменной форме, но и в физических действиях, например, в пощечине, плевке, неприличных жестах.

Разжигание розни и ложная информация

Разжигание розни

Статья 174 УК РК - Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни карается ограничением или лишением свободы сроком от двух до семи лет.

Любое грубое высказывание о человеке или группе людей, в котором затронута национальность, раса и вера человека – риск получить уголовное наказание.

Распространение заведомо ложной информации

Статья 274 УК РК - Распространение заведомо ложной информации карается штрафом до 5000 МРП, либо исправительными работами, либо ограничением/лишением свободы от двух до пяти лет. В 2025 году в Казахстане возбудили 71 уголовное дело по статье 274-й УК РК. Все чаще под эту статью попадают дела, связанные с использованием дипфейков.

Статья 402 УК РК - Действия, провоцирующие к продолжению участия в незаконной забастовке караются штрафом до 1000 МРП, исправительными работами, либо ограничением/лишением свободы на один год.

Использование подобной лексики в Сети и соцсетях даже опаснее, чем устный разговор офлайн, ведь интернет помнит все – сказанное человеком в онлайне в любой момент может быть использовано против него.

Что касается подростков с 14-лет?

Да, за словами нужно следить даже тем, у кого еще не наступил 16-летний возраст. В некоторых случаях уголовная ответственность касается и граждан не младше 14 лет.

Как сказано в Уголовном кодексе Казахстана, тюремные сроки могут получить 14-летние юноши и девушки, если их признали виновными в разжигании социальной, национальной, родовой, расовой, сословной или религиозной розни (статья 174-я). Также риск тюрьмы грозит за пропаганду терроризма и ложное сообщение о теракте (статьи 256-я и 273-я).

ЧТО ДЕЛАТЬ, ЕСЛИ...

Что делать, если тебя обижают или просят что-то подозрительное?

01

Не отвечай

Игнорируй грубые, странные или пугающие сообщения. Не вступай в диалог с обидчиком.

02

Сохрани доказательства

Сделай скриншоты переписки или страницы. Это поможет взрослым разобраться в ситуации.

03

Расскажи взрослым

Обязательно поделись тем, что произошло, с родителями, учителем или психологом колледжа. Они помогут тебе.

04

Ты не один

Помни, что ты не одинок. Существуют службы поддержки и люди, готовые помочь тебе справиться с любой проблемой в интернете.

ЗАКЛЮЧЕНИЕ

Итог: шагай безопасно в цифровой мир!

Соблюдай правила

Следуй основным принципам безопасности и уважай личные границы других пользователей.

Будь внимателен

Помни о своем цифровом следе и контролируй информацию, которую ты размещаешь в сети.

Используй с умом

Применяй критическое мышление и осторожность при использовании интернет-ресурсов.

Твоя ответственность

Безопасность в интернете — это личное дело каждого. Твоя бдительность — залог твоей защиты.