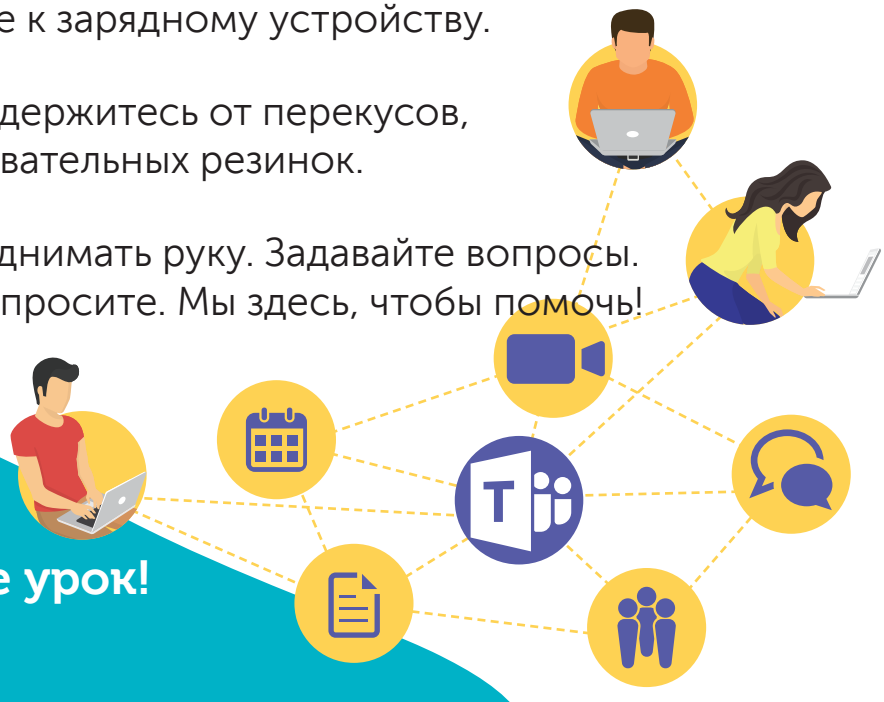
Microsoft Teams

Nazarbayev Intellectual Schools NIS

Правила работы в классах Teams

Базовый этикет для онлайн-класса

- ✓ Подключитесь к уроку в запланированное по расписанию время.
- ✓ Отключите микрофон, не разговаривайте во время урока. Прежде чем начать говорить, спросите разрешение у учителя, написав в чат.
- ✓ Уберите в сторону все, что вас отвлекает, в том числе телефон, если вы не используете его на уроке. Лучше всего работать, не отвлекаясь на другие вещи. Многозадачность – это миф, одновременное выполнение нескольких задач (работ) займет у вас больше времени, а качество работы будет хуже.
- ✓ Приготовьте заранее все необходимое для урока. При организации своего рабочего пространства приготовьте все ресурсы так, чтобы вы могли дотянуться до них легко и вам не нужно было отрываться от работы, чтобы взять их.
- ✓ Убедитесь, что рядом есть розетка. Проверьте уровень заряда компьютера (планшета, ноутбука), при необходимости подключите к зарядному устройству.
- ✓ Во время онлайн-урока воздержитесь от перекусов, употребления напитков, жевательных резинок.
- ✓ Не бойтесь писать в чат, поднимать руку. Задавайте вопросы. Если вы что-то не поняли, спросите. Мы здесь, чтобы помочь!



Помни!
Онлайн-урок – это тоже урок!

Рекомендации для работы в классах Teams

Технические рекомендации по улучшению качества участия на онлайн уроках

Для стабильного подключения к онлайн уроку рекомендуется:

- использовать персональный компьютер или ноутбук;
- минимизировать количество подключенных устройств к домашнему интернету, чтобы снизить нагрузку на модем/роутер;
- выключить видеокамеру, т.к. видеопоток поглощает значительную часть интернет-трафика, включать при необходимости;
- всегда выключать микрофон во избежание звуковых помех, включать его следует при необходимости, а затем вновь выключать;
- закрыть все сторонние приложения на используемом устройстве для снижения нагрузки;
- по возможности использовать проводное (LAN) соединение с интернетом;
- по возможности улучшить тарифный план домашнего интернета.

Для полноценного использования всех возможностей приложения Microsoft Teams на онлайн уроках рекомендуется:

- использовать десктоп-версию Teams, предварительно установив ее на свой компьютер;
- очищать временные файлы (кэш) приложения Teams;
- если у Вас слабые технические характеристики компьютера:
  - удалите все ненужные программы для снижения нагрузки;
  - используйте веб-версию приложения Teams на браузере Google Chrome;
  - перед каждым уроком очищайте временные файлы (кэш) браузера.

Для эффективной организации дистанционного обучения придерживайтесь следующих правил:

- Познакомьте всех членов семьи с режимом своего обучения. Предупредите их о том, что во время уроков у вас могут быть включены камера и микрофон;
- Какие бы устройства и технологии вы не использовали для доступа к онлайн урокам, пожалуйста, поставьте их в режим «Не беспокоить», чтобы исключить появление отвлекающих уведомлений во время урока;
- Для удобства учителя и быстрой визуальной идентификации своих учащихся, установите свое реальное фото на аватар учетной записи;
- Используйте чат для вопросов.

! В случае технических неполадок онлайн уроки записываются учителем и позднее доступны в классе для последующего пересмотра учащимися.

Все инструкции по организации дистанционного обучения посредством Microsoft Teams можно найти в открытых источниках, либо в нашем Telegram-боте @Teams_manual_bot

Microsoft Teams

Безопасность паролей и аккаунтов учащихся

Каждый из нас может подумать: «Зачем кому-то нужен мой аккаунт?».

Взлом аккаунтов – это очень выгодный (и незаконный!) бизнес. Некоторые кибермошенники взламывают максимальное количество случайных аккаунтов, чтобы потом отправлять рассылки с мошенническим умыслом (просьбой положить деньги на телефон/платёжную карту/электронный кошелёк, для вирусных рассылок, использовать в социальных сетях). Также на почтовый ящик может быть зарегистрирована куча других вещей: те же социальные сети, аккаунты в онлайн магазинах, онлайн банкинг.

Так как защитить аккаунт?

Нужно использовать сильные/хорошие пароли. Нельзя использовать пароли типа Password или 123456 – такие пароли хакеры перебирают с помощью специальных словарей. Рекомендуется использовать пароли длиной от 8 символов, в которых присутствуют большие и маленькие символы, цифры и знаки препинания. Чем пароль длиннее и чем больше в нем разных символов, тем сложнее его взломать. Для каждого аккаунта нужно использовать отдельный пароль!

Но при этом пароль еще могут украсть по-другому:

Например, если вводить его на сайте без шифрования, особенно в открытой Wi-Fi сети. Или если пользоваться компьютером, зараженным вирусом, на компьютере может оказаться вредоносная программа-кейлоггер – она будет записывать все, что ты печатаешь, и отправлять владельцу (злоумышленнику). Поэтому нужно использовать антивирус, никогда не стоит заходить в свои аккаунты с чужих компьютеров.

И еще, хакеры используют социальную инженерию, или попросту обман. Мошенники рассылают письма с предупреждениями, что, если ты сейчас же не перейдешь на сайт и не подтвердишь свой аккаунт посредством ввода пароля, твой аккаунт будет заблокирован. Такие рассылки называются фишинговыми. Как правило, письма максимально похожи на официальные. Если вдруг получишь подобное письмо – не торопись. Нужно посмотреть, с какого адреса отправлено письмо. Если это какой-нибудь steam@steampowered.com.freewebsites.org, то это явный фейк – просто проигнорируй письмо. Если же адрес настоящий, то, перейдя по ссылке, внимательно посмотри на адрес в строке браузера и наличие HTTPS-шифрования – адрес в электронном письме можно подделать, а вот оригинальный домен вместе с сертификатом – нет.

«А что, если я все-таки заражусь вирусом или поведусь на фишинг?»

Никто из нас не идеален, и иногда немного невнимательности может привести к утере пароля. Поэтому многие сервисы предлагают использовать для логина так называемую двухфакторную аутентификацию – это дополнительное подтверждение с помощью СМС на номер телефона.

Правила безопасности в сети Интернет

- ✓ Ограничьте объем информации о себе
- ✓ Не выкладывайте личную информацию о друзьях
- ✓ Не отправляйте свои персональные данные незнакомцам
- ✓ Не забывайте выходить из своих аккаунтов
- ✓ Заведите себе два адреса электронной почты
- ✓ Не пишите грубостей, оскорблений
- ✓ Не реагируйте на хамство и грубость других пользователей
- ✓ Не используйте Сеть для распространения сплетен, угроз или хулиганства
- ✓ Не оставляйте без присмотра компьютер с важными сведениями на экране
- ✓ Используйте только сложные пароли и старайтесь чаще менять их