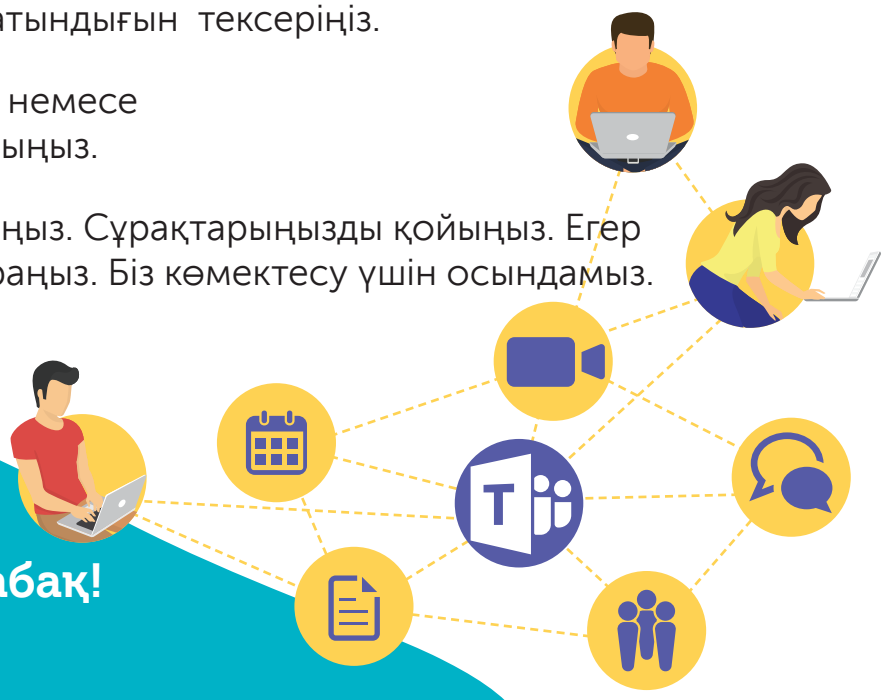
Microsoft Teams

Nazarbayev Intellectual Schools NIS

Teams сыныптарында жұмыс жасаудың ережесі

Онлайн-сынып үшін базалық этикет

- ✓ Сабаққа кесте бойынша жоспарланған уақытта қосылыңыз.
- ✓ Микрофонды өшіріңіз, сабақ уақытында сөйлеспеңіз. Мұғалімнен рұқсат сұрап қана сөйлеңіз.
- ✓ Көңіліңізді аулайтын заттарды алып тастаңыз. Сіз сабақта телефонды пайдаланбайсыз, сондықтан телефонды басқа жерге қойыңыз. Басқа нәрселерге алаңдамай, жұмыс істеген жақсы. Көп міндеттілік – бұл миф, бір уақытта бірнеше тапсырмаларды (жұмыстарды) орындау көп уақытты алады және орындау сапасы нашар болады.
- ✓ Сабаққа қажеттілердің бәрін алдын ала дайындаңыз. Жұмыс кеңістігіңізді ұйымдастыру кезінде барлық ресурстарды оңай ала алатындай етіп дайындаңыз және оларды алу үшін жұмысты тоқтатудың қажеті болмауы керек.
- ✓ Жаныңызда розетка бар екеніне көз жеткізіңіз. Компьютеріңіз (планшет, ноутбук) қуатталғанын немесе қуаттау құрылғысын оңай қосуға болатындығын тексеріңіз.
- ✓ Камера қосылған кезде тамақ немесе сусындарды ішуден аулақ болыңыз.
- ✓ Қолыңызды көтеруге қорықпаңыз. Сұрақтарыңызды қойыңыз. Егер сіз бір нәрсе түсінбесеңіз, сұраңыз. Біз көмектесу үшін осындамыз.



Жадыңда болсын!
Онлайн-сабақ – ол да сабақ!

Teams сыныптарында жұмыс істеу жөніндегі ұсыныстар

Онлайн сабақтарға қатысу сапасын жақсартуға қатысты техникалық ұсыныстар

Онлайн сабаққа тұрақты қосылу үшін төмендегідей кеңес береміз:

- дербес компьютерді немесе ноутбукті пайдалану;
- модем/роутер жүктемесін азайту үшін үйдегі интернетке қосылған құрылғылардың санын қысқарту;
- бейне камераны өшіру, өйткені бейне ағын интернет трафигінің біраз мөлшерін кетіреді, оны тек қажет болған жағдайда ғана қосу;
- дыбыстық кедергілерді болдырмау үшін әрдайым микрофонды өшіріп тастау, оны тек қажет болған жағдайда ғана қосып, кейін қайтадан өшіру;
- жүктемені азайту үшін пайдаланылатын құрылғыдағы барлық басқа қосымшаларды жабу;
- мүмкіндігінше Интернетке желі (LAN) арқылы қосылу;
- үйдегі интернеттің тарифтік жоспарын мүмкіндігінше жақсарту.

Онлайн сабақтарда Microsoft Teams бағдарламасының барлық мүмкіндіктерін толық пайдалану үшін төмендегідей кеңес беріледі:

- Teams-тің десктоп нұсқасын алдын ала компьютерге орнатып алып, пайдалану;
- Teams бағдарламасының уақытша файлдарын (кэш) тазарту;
- егер сіздің компьютеріңіздің техникалық сипаттамалары әлсіз болса:
  - жүктемені азайту үшін барлық қажетсіз бағдарламаларды жойыңыз;
  - Google Chrome браузерінде Teams қосымшасының веб-нұсқасын пайдаланыңыз;
  - әр сабақ алдында браузердің уақытша файлдарын (кэш) тазалаңыз.

Қашықтықтан оқытуды тиімді ұйымдастыру үшін келесі ережелерді қолданыңыз:

- Барлық отбасы мүшелерін өзіңіздің оқу режиміңізбен таныстырыңыз. Сабақ барысында камера мен микрофонның қосылатынын ескертіңіз;
- Онлайн сабақтарға кіру үшін қандай құрылғылар мен технологияларды пайдалансаңыз да, сабақ кезінде алаңдататын хабарламалар пайда болмас үшін оларды «Мазаламау» режиміне қойыңыз;
- Мұғалімнің ыңғайлылығы және оқушыларды тез тану үшін, аватарға өз фотосуретіңізді қойыңыз;
- Сұрақтар үшін чатты пайдаланыңыз.

! Техникалық ақаулықтар болған жағдайда мұғалім онлайн сабақтарды жазып алады және кейін оқушылар оны қайта қарай алады.

Microsoft Teams арқылы қашықтықтан оқытуды ұйымдастыру жөніндегі барлық нұсқаулықтарды ашық дереккөздерде немесе Біздің Telegram-ботта табуға болады @Teams_manual_bot

Microsoft Teams

Оқушылардың құпия сөздері мен аккаунттарының қауіпсіздігі

«Аккаунтымның біреуге қажеті қанша?» деп ойлауымыз мүмкін.

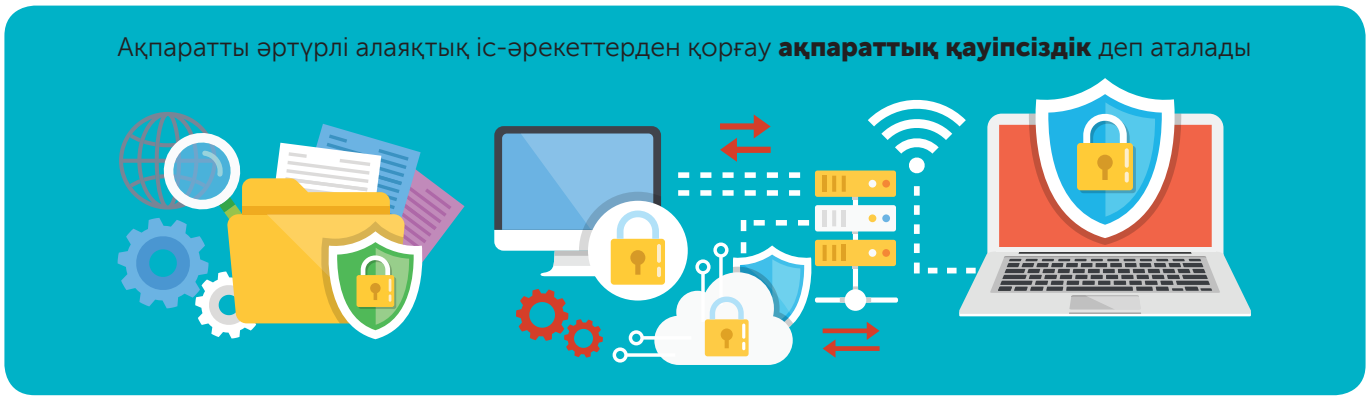
Десек те аккаунттарды бұзу – өте тиімді (және заңсыз!) бизнес. Кейбір киберайлакерлер барынша көп кездейсоқ аккаунттарды бұзып, алаяқтық оймен жалған хаттар таратады (телефонға/төлем картасына/электрондық әмиянға ақша салып жіберуді сұрау, вирус тарату, әлеуметтік желілерде қолдану мақсатымен). Оның үстіне пошта жәшігіне әлеуметтік желілер, онлайн дүкен аккаунттары, онлайн банкинг сияқты әртүрлі нысандар тіркелуі мүмкін.

Аккаунтты қалай қорғауға болады?

Күшті/берік құпия сөздерді пайдалану керек. Password немесе 123456 түріндегі құпия сөздерді пайдалануға болмайды – мұндай құпия сөздерді хакерлер арнайы сөздіктер арқылы оңай ашып алуы мүмкін. Үлкен және кіші таңбалар, сандар мен тыныс белгілері бар, кем дегенде 8 таңбадан тұратын құпия сөздерді пайдаланған дұрыс. Құпия сөз неғұрлым ұзын, әрі алуан түрлі таңбаларды қамтыған сайын, оны бұзу соғұрлым қиынға түседі. Әрбір аккаунт үшін жеке құпия сөзді пайдалану керек!

Бірақ құпия сөзді басқаша жолмен де ұрлауға болады:

Мысалы, егер сен оны белгілі бір сайтта, әсіресе ашық Wi-Fi желісінде шифрлаусыз енгізсең. Немесе вирус жұққан компьютерді пайдалансаң, онда зиянды кейлоггер-бағдарлама болуы мүмкін – ол сенің басқан таңбаларыңның бәрін жазып алып, иесіне (зиянкестерге) жібереді. Сондықтан антивирусты пайдалану керек, өз аккаунтыңа бөтен компьютерлерден кіруші болма.



Сонымен қатар, хакерлер әлеуметтік инженерияны пайдаланады, басқаша сөзбен айтқанда олар адамдарды алдайды. «Мына сайтқа кіріп, құпия сөзді енгізу арқылы өз аккаунтыңды растамасаң, аккаунтың бұғатталады» дейтін хаттар таратады. Бұл фишинг деп аталады. Әдетте, мұндай жалған хаттар ресми хаттарға ұқсайды. Егер кенеттен осындай хат алсаң – асықпа. Хат қандай мекен-жайдан жіберілгенін көру керек. Егер ол steam@steampowered.com.freewebsites.org деген сияқтылардан келсе, онда бұл нағыз фейк – хатқа көңіл бөлме. Егер мекенжай шынайы болса, онда сілтеме бойынша өтіп, браузер жолындағы мекенжайға және HTTPS-шифрлеуінің бар жоғына мұқият қара – электрондық хаттағы мекенжайды қолдан жасауға болғанымен, сертификатталған түпнұсқалық доменді жасауға болмайды.

«Сонда да вирус жұқтырсам немесе фишингке түсіп қалсам не істеуім керек?»

Мінсіз адам болмайды, кейде сәл ғана мұқиятсыздық нәтижесінде парольді жоғалтып алуға болады. Сондықтан көптеген сервистер логин үшін екі факторлы аутентификацияны пайдалануды ұсынады – бұл телефон нөміріне СМС жіберу арқылы жүргізілетін қосымша растау.

Интернет желісіндегі қауіпсіздік ережелері

- ✓ Өзіңіз жайлы ақпарат көлемін азайтыңыз
- ✓ Достарыңыз жайлы жеке ақпаратты жарияламаңыз
- ✓ Бейтаныс адамдарға жеке ақпараттарыңызды жібермеңіз
- ✓ Аккаутыңыздан шығуды ұмытпаңыз
- ✓ Екі электрондық пошта ашыңыз
- ✓ Ерсі және балағат сөздерді қолданбаңыз
- ✓ Басқа пайдаланушылардың балағат сөздеріне жауап қайтармаңыз
- ✓ Желіні өсек, қорқыту және бұзақылық үшін қолданбаңыз
- ✓ Компьютерді маңызды ақпарат экранда ашық күйінде қалдырмаңыз
- ✓ Күрделі құпия сөздерді қолданып, оларды жиі ауыстырып тұрыңыз