

«Практикалық тапсырма: Электронды күнделіктер мен білім беру платформаларында құпиялылықты баптау»

Тренинг сценарийі:

«Практикалық тапсырма: Электронды күнделіктер мен білім беру платформаларында құпиялылықты баптау»

Ұзақтығы: 60 минут

Аудитория: Мұғалімдер, IT-мамандар, әкімшілік қызметкерлер, ата-аналар

Тренингтің мақсаты:

1. Қатысушыларды электронды күнделіктер мен білім беру платформаларында құпиялылық параметрлерін дұрыс баптауға үйрету.
2. Оқушылардың, мұғалімдердің және ата-аналардың деректерін цифрлық жүйелерде қорғау әдістерімен таныстыру.
3. Білім беру платформаларында жұмыс істеу барысында қауіпсіздікті қамтамасыз ету дағдыларын дамыту.

1. Тақырыпқа кіріспе (5 минут)

- Қатысушылармен сәлемдесу және тренингтің мақсаттарын қысқаша түсіндіру.
- Электронды күнделіктер мен білім беру платформаларындағы құпиялылық параметрлерінің маңыздылығы туралы айту.
- Қысқаша қауіптерге шолу: деректердің таралуы, рұқсатсыз қол жеткізу, фишинг шабуылдары.

Тренингтің мақсаты: Қатысушылардың құпиялылық жөнінде хабардарлығын арттыру және білім беру платформаларында қауіпсіздікті баптау дағдыларын қалыптастыру.

2. Электронды күнделіктер мен білім беру платформаларына шолу (10 минут)

Мектепте жиі қолданылатын платформаларды талқылау:

«Электронды күнделік», Moodle, Google Classroom және т.б.

Бұл платформаларда қандай деректер сақталады: оқушының аты-жөні, бағалары, кестесі, байланыс ақпараты, үй тапсырмалары және т.б.

Талқылау: Осы деректердің таралуымен қандай қауіптер байланысты болуы мүмкін? Білім беру платформаларына жасалған шабуылдардан мысалдар келтіру.

3. Электронды күнделіктер мен платформаларда құпиялылықты баптау (25 минут)

Жалпы нұсқаулық:

Құпиясөз жасау:

- Кемінде 8 таңбадан тұруы керек, бас әріптер, сандар мен белгілер болуы тиіс.
- Құпиясөздерді жиі өзгертіп отыру және олардың таралмауын қамтамасыз ету жолдары.
- Қауіпсіз құпиясөздер генераторлары арқылы мысалдар келтіру.

Қосфакторлы аутентификация (2FA):

Бұл не үшін қажет?

Мобильді қосымшалар арқылы 2FA орнату мысалы.

Қол жеткізу құқықтарын баптау:

Кім қандай деректерге қол жеткізе алады? (мұғалім, оқушы, ата-ана, әкімшілік)

Қол жеткізу шектеулерін көрсету мысалдары (ата-аналар мен оқушылар үшін).

Деректерді шифрлау:

Білім беру платформаларындағы шифрлау функцияларына шолу.

Хабарламалар мен құжаттар алмасу кезінде шифрлауды қалай іске қосуға болатынын көрсету.

Практикалық бөлім:

Қатысушылар шағын топтарға бөлініп, таңдалған платформада құпиялылықты баптауға арналған нұсқаулық алады (мысалы, «Электронды күнделік» немесе Google Classroom).

Баптау кезеңдері: Қауіпсіз құпиясөз жасау → Қосфакторлы аутентификацияны қосу → Қол жеткізу шектеулерін орнату.

Уақыты: 10–15 минут.

Тренер көмегі: Жаттығу барысында қатысушыларға көмек көрсетіледі және сұрақтарға жауап беріледі.

4. Оқушылар мен мұғалімдердің деректерін қорғау шаралары (10 минут)

1. Деректердің білім беру платформалары арқылы таралуының алдын алу.
2. Бағдарламалық қамтамасыз етуді үнемі жаңартып отыру.
3. Күдікті әрекеттерді қадағалауға арналған ескертулерді баптау.
4. Деректердің резервтік көшірмесін жасау.

Ұсыныстар мысалдары:

Мұғалімдер мен ата-аналар қауіпсіздік параметрлерін және белсенділік туралы хабарламаларды жүйелі түрде тексеруі керек. Оқушылар өз құпиясөздерін өзгелерге, тіпті сыныптастарына да бермеуі керек.

Практикалық бөлім:

Егер платформада бар болса, күдікті әрекеттер туралы ескертулерді баптау (мысалы, бейтаныс құрылғылардан кіру немесе деректердің өзгеруі туралы хабарламалар).

5. Сұрақтар мен жауаптар (5 минут)

Қатысушылардың құпиялылықты баптау бойынша сұрақтарына жауап беру.

Қосымша ұсыныстар мен кеңестер.

Талқылау сұрақтары:

1. Ата-аналар мен оқушылармен құпиялылықты сақтау бойынша жұмысты қалай дұрыс ұйымдастыру керек?
2. Құпиялылық дұрыс бапталмаса қандай мәселелер туындауы мүмкін және олардан қалай сақтануға болады?

6. Қорытынды (5 минут)

Қорытынды:

- Құпиясөздерді жиі жаңартып отыру және 2FA-ны қосу маңыздылығы.
- Қол жеткізу құқықтарын дұрыс баптау арқылы оқушылар мен мұғалімдердің деректерін қорғау.
- Платформалардағы белсенділікті бақылау — таралудың алдын алу құралы.
- Қатысушыларға белсенді қатысқандары үшін алғыс білдіру.
- Келесі тренингтер мен кеңестер туралы ақпарат беру.

Таратылатын материалдар:

1. Электронды күнделіктер мен білім беру платформаларында құпиялылықты баптау бойынша жадынама.
2. Қауіпсіз құпиясөздер жасау және 2FA қосу жөніндегі нұсқаулық.
3. Хабарламалар мен деректерді шифрлау бойынша қысқаша нұсқаулық.