ПАМ’ЯТКА

щодо захисту дистанційної форми навчання в Державному навчальному закладі «Професійно – технічне училище № 40 м. Новоукраїнка»

У ведення в Україні воєнного стану позначилося на всіх сферах суспільного життя. Війна негативно впливає на організацію освітнього процесу, що в свою чергу, зумовлює потребу в гнучкій трансформації діяльності освітньої сфери на період дії воєнного, стану. Передусім постала, необхідність для убезпечення учасників освітнього процесу, а саме: вжиття заходів щодо підвищення захисту інформації під час дистанційної форми навчання, зокрема.

1 .Перед початком розмови необхідно переконатись, що у полі зору веб-камери немає жодних конфіденційних даних.

2 .Використовувати платформи які дозволяють створювати групи користувачів або обмежувати доступ через Інтернет-домен.

3. Не надсилати пароль до зустрічі разом з посиланням на зустріч.

4. Контролювати несанкціоноване підключення до розмови.

5. Налаштувати безпечну передачу файлів.

6. Встановити шифрування каналу передачі даних.

7. Встановити обмеження каналу передачі даних.

8. Встановити обмеження щодо файлів, які учасники можуть надсилати.

9. Обмежити доступ до спільного використання екрана для хоста або людини, яка вибирає хост.

9. Під час спільного використання екрана не поширювати весь робочий стіл, а лише необхідні вкладки.

10. Використовувати актуальну версію програм та регулярно встановлювати оновлення, які можуть містити важливі виправлення вразливостей безпеки.

11.Не використовувати програмне забезпечення для відеоконференцій, без ознайомленням з усіма параметрами в установках системи.

12. Не поширювати посилання або ID конференцій у соціальних мережах.

13. Захистити облікові записи придумавши складний унікальний пароль та активувати двофакторну автентифікацію.

14. Завантажувати програми для відеоконференцій лише з офіційних джерел для програмного забезпечення.

15. Встановити максимальну кількість учасників (по кількості класу).

16. Використовувати Personal Meeting ID (PMI).

17. Забезпечити захист персональних даних учасників освітнього процесу відповідно до Закону України «Про захист персональних даних» (як приклад - Нікнейм).

18. Встановити антивірусне програмне забезпечення та брандмауер й регулярно їх оновлювати.

19. Забезпечити фільтрацію та моніторинг даних, що передаються через під’єднання до Інтернету.

20. Установити чіткі приписи як для співробітників, так і для учнів щодо підготовки робочого місця для віддаленого зв’язку.

21. Створити окремі облікові записи або окремих користувачів, електронні поштові скриньки розмежовуючи власне електронне середовище та робоче.