РЕКОМЕНДАЦІЇ ДЛЯ ВЧИТЕЛІВ ЩОДО БЕЗПЕКИ ВИКОРИСТАННЯ ПЛАТФОРМИ ДЛЯ ДИСТАНЦІЙНОГО НАВЧАННЯ

1. Для унеможливлення несанкціонованих входів під час онлайн-конференцій користувачів, які не є членами групи, необхідно надавати посилання-запрошення тільки в закриті групи спілкування.
2. Для приєднання учасників відеоконференцій, проведення різних типів опитування та тестування рекомендується відправляти посилання на заходи на електронну пошту.
3.Під час онлайн-спілкування адміністратор (учитель) повинен користуватись інструментом, що дає можливість керувати приладами учасників зустрічі: мікрофонами, транслюванням екранів та, за потребою, вилучати учасників конференції.
4. Надати рекомендації учням щодо спілкування між собою через Інтернет. Учням варто використовувати такі самі ресурси, які використовуються навчальним закладом для проведення дистанційного навчання. Поширення спілкування через мережу Інтернет надає можливість зловмисникам видати себе за іншу особу. Тому варто обережно відкривати повідомлення від невідомих адресатів, переходити за посиланнями, які знаходяться в таких листах, або відкривати вкладені файли до листа.
5. Не варто використовувати ресурси, які не підтримують шифрування даних, наприклад, через протокол https.

РЕКОМЕНДАЦІЇ ДЛЯ УЧНІВ ЩОДО БЕЗПЕКИ ВИКОРИСТАННЯ ПЛАТФОРМИ ДЛЯ ДИСТАНЦІЙНОГО НАВЧАННЯ

1. Ніколи не давати приватної інформації про себе без дозволу батьків.
2. Нікому не давати свій пароль, за виключенням дорослих вашої родини.
3. Завжди бути ввічливими у електронному листуванні.

РЕКОМЕНДАЦІЇ ДЛЯ БАТЬКІВ ЩОДО БЕЗПЕКИ ВИКОРИСТАННЯ ПЛАТФОРМИ ДЛЯ ДИСТАНЦІЙНОГО НАВЧАННЯ

1. Допомагати своїм дітям при реєстрації в Інтернет-сервісах.
2. Контролювати поведінку своїх дітей у соціальних мережах.
3. Дотримуватися правил інформаційної безпеки, зокрема кібербезпеки.
4. Якщо в сім'ї використовується один комп'ютер різними членами сім'ї, варто створити окремий обліковий запис для кожного з них. Причому учням варто створити обліковий запис з обмеженими правами.

5. При реєстрації на різних онлайн-ресурсах учасникам дистанційного навчання варто вводити мінімальну кількість персональних даних, або вказувати недостовірні дані. Для цього не завадить створити окрему електронну скриньку, яку можна використовувати при реєстрації.
6. Слід обережно використовувати онлайн-тести та опитування, якщо вони пропонуються на різних відкритих онлайн-ресурсах.
7. Ніколи і нікому не повідомляти паролі від ресурсів, де користувачі мають облікові записи. Якщо можна, не вказувати дійсний номер мобільного телефону при реєстрації.