

У коледжі стартував місяць кібербезпеки. Долучайтесь до заходів, отримуйте поради та нові знання.

Місяць кібербезпеки — період, присвячений підвищенню цифрової обізнаності здобувачів освіти та покликаний поліпшити знання про кібергігієну, сформувати культуру безпечної поведінки у віртуальному просторі.

Долучитися до місяця кібербезпеки може кожен, пройшовши навчання на платформі «Дія .Освіта» у розділі «Кібергігієна», де у зрозумілій формі зібрані корисні поради та практики, які допоможуть зробити онлайн-досвід безпечним.

Кібербезпека – наша спільна відповідальність. Виконуючи прості правила цифрової гігієни, кожен із нас робить внесок у безпечне майбутнє країни.

ПОРАДИ ЩОДО БЕЗПЕЧНОЇ ПОВЕДІНКИ В ІНТЕРНЕТІ ТА КІБЕРБЕЗПЕКИ

Як подбати про кібербезпеку?

Соціальні мережі і електронні сервіси – місця, де на легковажних користувачів полює чимало інтернет-шахраїв та представників спецслужб рф. Вони шукають вразливі паролі та підключення, щоб зламати їх та використати вашу персональну чи службову інформацію. Електронні пристрої – це найбільше джерело інформації про вас, тож подбайте про власну кібербезпеку.

Безпека електронних пристроїв:

- Регулярно оновлюйте системи захисту ваших пристроїв.
- Систематично робіть резервне копіювання важливих файлів.
- Встановіть режим конфіденційності та безпеки для вебсайтів.
- Під час оплати в інтернеті звертайте увагу на електронну адресу: «https://» - це означає, що сайт вживає додаткові заходи для безпеки своїх клієнтів; «http://» - посилання не є безпечним.
- Не використовуйте службові електронні скриньки для приватного листування.
- Скануйте перед підключенням USB та інші зовнішні пристрої на наявність шкідливих додатків і вірусів.

Безпечне підключення до Wi-Fi

Безкоштовне підключення до Wi-Fi у публічних місцях часто відбувається без введення паролів. Це робить ваш пристрій вразливим для зламу.

- Під час входу до мережі Wi-Fi використовуйте лише ті точки доступу до Wi-Fi, які мають протоколи безпеки для захисту бездротового з'єднання WPA чи WPA-2 (як мінімум, - прим.ред).

- Оптимальний варіант – користуватись особистим Wi-Fi модемом або здійснювати вхід в Інтернет за передплаченим пакетом послуг мобільного оператора.
- Вимикайте функцію «Автоматичного підключення до Wi-Fi».

Захист смартфона від програм-шпигунів

Більшість шпигунських програм «вшиваються» саме в мобільні додатки. Коли ви встановлюєте їх на смартфон, то власноруч дозволяєте зчитати вашу геолокацію, список контактів, акаунти у соцмережах та поштові скриньки.

- Встановлюйте додатки лише з офіційних та перевірених сервісів: Chrome Store, Add-ons та Play Market для Android, App Store для OS.
- Не дозволяйте операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел.
- Періодично видаляйте додатки, якими не користуєтесь.

Безпека електронного листування

Якщо зловмисники «зламають» вашу електронну пошту, вони можуть спробувати змінити паролі, отримати доступ до особистих фотографій та відео, розсилати спам від вашого імені.

- Увімкніть двофакторну автентифікацію за допомогою мобільного пристрою. Якщо стороння особа спробує отримати пароль до вашої поштової скриньки, ви автоматично отримаєте SMS-повідомлення про несанкціонований вхід.
- Встановіть надійний пароль і не використовуйте для його відновлення російські сервіси «Yandex.ru», «Mail.ru».
- Не відкривайте на пристроях вкладення підозрілих листів, що мають такі розширення як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо.

ПОРАДИ ЗДОБУВАЧАМ ОСВІТИ

1. Нікому без дозволу батьків не давати особисту інформацію: домашню адресу, номер телефону, робочу адресу батьків, їхній номер телефону, назву й адресу місця навчання, свої паролі.
2. Якщо знайдете якусь інформацію, що турбує вас, негайно сповістіть про це батьків.
3. Ніколи не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті. Якщо все ж таки це необхідно, то спочатку потрібно спитати дозволу батьків, а зустріч повинна відбутися в громадському місці й у присутності батьків.
4. Не відповідати на невиховані і грубі листи. Якщо одержите такі листи не з вашої вини, то сповістіть про це батьків, нехай вони зв'яжуться з компанією, що надає послуги Інтернет.

5. Розробити з батьками правила користування Інтернетом. Особливо домовитися з ними про прийнятний час роботи в Інтернеті і сайти, до яких ви збираєтесь заходити.
6. Не заходити на аморальні сайти і не порушувати без згоди батьків ці правила.
7. Не робити протизаконних вчинків і речей в Інтернеті.
8. Не шкодити і не заважати іншим користувачам.

ПОРАДИ БАТЬКАМ

1. Розташуйте комп'ютер вашої дитини в місці загальної доступності: їдальні або вітальні. Так вам буде простіше стежити за тим, що роблять діти в Інтернеті.
2. Звертайте увагу на те, які сайти відвідує дитина. Поговоріть з дітьми про сайти, які вони відвідують, і обговоріть, що припустимо, а що ні у вашій родині. Список сайтів, які відвідує дитина, можна знайти в історії браузера . Крім того, ви можете скористатися інструментами блокування небажаного контенту, такими як, наприклад, безпечний пошук Google або безпечний режим на YouTube.
3. Розкажіть дітям про безпеку в Інтернеті. Ви не зможете весь час стежити за тим, що вони роблять в мережі. Їм необхідно навчитися самостійно користуватися Інтернетом безпечним і відповідальним чином.
4. Використовуйте налаштування конфіденційності та управління доступом до вашого розташування. На YouTube, Blogger, в соціальних мережах і на багатьох інших сайтах користувачі можуть розміщувати власний контент. Зазвичай автору надається можливість обмежити доступ до особистого блогу, фотографій, відео та інформації в профілі. Особливо важливо обмежувати доступ до таких даних, як ім'я, адреса або номер телефону, які дитина розміщує на загальнодоступних сайтах.
5. Зберігайте паролі в таємниці. Нагадуйте дітям, що паролі не можна нікому повідомляти.
6. Не довіряйте незнайомцям. Поясніть дітям, що не слід призначати особисті зустрічі з людьми, з якими вони познайомилися в Інтернеті, і повідомляти їм особисту інформацію, тому що незнайомці можуть видавати себе за когось, ким вони насправді не є.
7. Встановіть захист від вірусів. Використовуйте і регулярно оновлюйте антивірусне програмне забезпечення. Навчіть дітей не завантажувати файли з файлообмінних сайтів, а також не приймати файли і не завантажувати вкладення, що містяться в електронних листах від незнайомих людей.
8. Навчіть дітей відповідальної поведінки в Інтернеті. Пам'ятайте золоте правило: те, що ви не сказали б людині в обличчя, не варто відправляти йому по SMS, електронною поштою, в чаті або розміщати у коментарях на його сторінці в Мережі.
9. Оцінюйте Інтернет-контент критично. Те, що міститься в Інтернеті, не завжди правда. Діти повинні навчитися відрізняти надійні джерела інформації від ненадійних і перевіряти інформацію, яку вони знаходять в Інтернеті. Також

пояснить дітям, що копіювання і вставка змісту з чужих веб -сайтів можуть бути визнані плагіатом.

10. Отже, Інтернет-залежність є актуальною проблемою, дослідження якої зумовлене запитами суспільства, що пояснюється швидким темпом розвитку комп'ютерних технологій, отриманням вільного доступу все більшої кількості людей до Інтернету. Але якщо батьки разом зі своїми дітьми будуть дотримуватись правил «Безпечного Інтернету» можна уникнути багатьох проблем.

Нормативно-правова база щодо кібербезпеки

Перелік наказів, законів України та постанов Кабінету Міністрів України:

- [Закон України "Про основні засади забезпечення кібербезпеки України"](#), який визначає правові та організаційні основи забезпечення захисту важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.
- [Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" від 26 серпня 2021 року № 447/2021"](#)
- [Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»](#)
- [Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94](#), яким затверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»; наказ зареєстровано в Міністерстві юстиції України 07.07.2008 за № 603/15294.
- [Постанова Кабінету Міністрів України від 16.11.2002 № 1772](#), якою затверджено «Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах».
- [Постанова Кабінету Міністрів України від 29.03.2006 № 373](#), якою затверджено «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».
- [Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660](#), яким затверджено «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»; наказ зареєстровано в Міністерстві юстиції України 28.01.2015 за № 90/26535.
- [Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20](#), яким затверджено «Порядок сканування на предмет вразливості державних інформаційних

ресурсів, розміщених в Інтернеті»; наказ зареєстровано в Міністерстві юстиції України 05.02.2016 за № 196/28326.

- [Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563](#), якою затверджено «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».
- [Закон України «Про телекомунікації»](#)
- [Постанова Кабінету Міністрів України від 11.04.2012 № 295](#), якою затверджено «Правила надання та отримання телекомунікаційних послуг»; пункт 36 підпункти 1-7,13-15, пункт 54 підпункти 5-6;
- [Постанова Кабінету Міністрів України від 19.06.2019 № 518](#), «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».
- [Постанова Кабінету Міністрів України від 09.10.2020 № 943](#), «Деякі питання об'єктів критичної інформаційної інфраструктури».
- [Постанова Кабінету Міністрів України від 09.10.2020 № 1109](#), «Деякі питання об'єктів критичної інфраструктури».
- [Постанова Кабінету Міністрів України від 23.12.2020 № 1295](#), «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».