Безпека вашої організації в Інтернеті

Чому кібербезпека важлива для громадських груп та організацій?

На цій сторінці надані поради та деякі кроки, які ви можете зробити, щоб захистити свою громадську групу чи організацію від загроз кібербезпеці. Також існує окремий посібник для приватних осіб щодо безпеки в Інтернеті.

Ці поради ґрунтуються на найбільш поширених і серйозних загрозах.

- Оновлення – оновлюйте програмне забезпечення на своїх пристроях, щоб виправити будь-які прогалини в безпеці.
    - Оновлюйте пристрої своєї громадської групи або організації. Сюди входять телефони, комп'ютери, WiFi-роутери та все інше, що підключається до Інтернету, включно зі смарт-пристроями.
    - Де це можливо, використовуйте автоматичні оновлення.
- Двофакторна автентифікація (2FA) – додає додаткову безпеку вашим обліковим записам, вимагаючи введення пароля і ще одного кроку, наприклад, коду із застосунку на вашому телефоні.
    - Примітка: Це також називається багатофакторною автентифікацією (MFA), двоетапною перевіркою (2SV) та багатьма іншими назвами.
    - Увімкніть двофакторну автентифікацію для всіх облікових записів громадської групи або організації.
    - Якщо можливо, спробуйте використати форму 2FA, яка є стійкою до фішингу, що означає, що вас не зможуть обманом змусити передати її. Це може бути фізичний ключ безпеки або щось на кшталт ідентифікації за відбитками пальців чи обличчям.
- Слідкуйте за своїми обліковими записами в Інтернеті – переконайтеся, що колишні члени не зберігають доступ до облікових записів після виходу з громадської групи чи організації.
    - Якщо у вас більше ніж одна особа має доступ до одного облікового запису, переконайтеся, що всі вони мають різні логіни та ввімкнену форму 2FA.
    - Зберігайте список усіх облікових записів користувачів і дезактивуйте непотрібні, наприклад, коли співробітники звільняються.
    - Ведіть реєстр усіх пристроїв, які ви надали своїм членам, і не забувайте повертати їх назад і скидати до заводських налаштувань, якщо ця особа залишає організацію. Вам також може знадобитися змінити фізичні коди доступу до будівлі.
- Перевірте, хто має доступ до ваших облікових записів в Інтернеті – особи у вашій громадській групі чи організації повинні мати доступ лише до того, що їм потрібно.
    - Якщо обліковий запис однієї особи буде зламано, ці кроки обмежать шкоду, яку може завдати зловмисник.

    - Регулярно перевіряйте та видаляйте непотрібні дозволи.
    - Якщо у вас є один обліковий запис адміністратора, яким користуються декілька осіб, відстежуйте його на предмет незвичної активності. Намагайтеся обмежити наявність таких облікових записів, особливо для повсякденних завдань.
    - Ці правила також поширюються на доступ адміністратора до пристроїв, наприклад, роутерів.
- Перегляньте свої контракти з постачальниками послуг — якщо ви найняли когось для надання вам IT-послуг.
    - Переконайтеся, що вони мають засоби захисту кібербезпеки, які відповідають потребам вашої громадської групи чи організації.
- Дізнайтеся, як усі ваші облікові записи та системи працюють разом – розуміння зв’язків допоможе вам зрозуміти, куди може проникнути зловмисник.
    - Перевірте зв'язки між вашими системами, наприклад, електронною поштою, хмарним сховищем і бухгалтерськими платформами.
    - Розгляньте можливість використання віртуальної приватної мережі (VPN) для додаткової безпеки в Інтернеті. Використання VPN приховує вашу онлайн-активність від будь-кого, хто може спробувати вас відстежити. Це особливо добре, якщо хтось із членів вашої громадської групи чи організації підключається віддалено.
- Слідкуйте за тим, щоб ваші співробітники були «кіберрозумними» – особи у вашій громадській групі чи організації з більшою ймовірністю можуть стати мішенню, ніж ваші системи.
    - Навчіть весь персонал основам кібербезпеки. Веб-сайт Own Your Online | NCSC пропонує широкий спектр порад і підказок, які допоможуть персоналу захистити себе в Інтернеті та виявити шахрайство.
    - Нагадайте їм, що це важливо для їх особистих облікових записів, а також для тих, які вони використовують для вашої організації.
    - У нас також є посібник для приватних осіб про те, як захистити себе в Інтернеті.
- План на випадок інциденту – наявність плану реагування важлива для того, щоб люди не панікували, якщо трапляється якийсь інцидент.
    - У плані реагування на інциденти зазначено, хто і що робить під час інциденту. Шаблони доступні тут Управління інцидентами | NCSC
    - Додайте план дій у разі виходу з ладу телефонів, комп'ютерів або інших систем. Оновлюйте цей план.
    - Зберігайте контактні дані всіх необхідних осіб і резервні дані, якщо основний спосіб зв’язку з ними не працює (наприклад, електронна пошта).
    - Також зберігайте план десь за межами вашої системи на той випадок, якщо ви не зможете отримати до нього доступ.