Оцінка цифрових ризиків

Шаблон

Ця "Оцінка цифрових ризиків" допоможе вам визначити та оцінити потенційні загрози цифрової безпеки, пов'язані з вашою історією або завданням.

Під час оцінювання ви знайдете посилання на відповідні розділи нашої **"Інструкції з цифрової безпеки"**. Це надасть вам додаткову інформацію стосовно того, як ви можете пом'якшити різні цифрові ризики та зменшити ризик потенційних загроз.

Перегляньте ресурси з **ЦИФРОВОЇ БЕЗПЕКИ**, які допоможуть вам виконати це оцінювання.

Будь ласка, збережіть копію цієї форми для довідки.

RORY PECK TRUST

WWW.RORYPECKTRUST.ORG

Дата

1. Опишіть своє завдання

Перш ніж ви зможете правильно визначити основні ризики для вашої цифрової безпеки, доцільно розбити своє завдання на складові та розглянути його ключові елементи. Спробуйте визначити всі основні компоненти: розповідь, респонденти, організація подїздки та будь-які інші дії, які є життєво важливими для ваших планів. Після того, як ви це зробите, вам буде легше визначити всі сфери, які вам потрібно враховувати при оцінюванні ризиків.

Перелічіть і надайте якомога більше інформації про таке:

Опис сюжету

Ключові респонденти

Плани поїздок

Проживання

Ключові дії

2. Які цифові загрози виникають під час висвітлення цієї історії?

Тепер подумайте про свої основні ризики, загрози та противників.

Пам'ятайте, що вам не потрібно висвітлювати суперечливу чи делікатну історію, щоб стати вразливим з точки зору цифрових технологій. Ви повинні набути звичку виконувати оцінку ризиків для всіх завдань або сюжетів, оскільки під час цього процесу можна виявити потенційні загрози, про які ви навіть не думали.

Обміркуйте таке:

a) Чи будете ви контактувати або брати інтерв'ю у вразливих людей?

Якщо так:

- Як ви будете зберігати та захищати дані людей, у яких берете інтерв'ю?
- Як і де ви будете зберігати ваші нотатки та матеріали?

Додаткові питання про безпечний контакт з людьми дивіться нижче у розділі "Комунікація".

---

b) Ви висвітлюєте делікатну або суперечливу тему?

Якщо так:

- Чи містить вона інформацію, яка має залишитись секретною та конфіденційною?
- Чи ви розумієте та знаєте, як користуватись безпечними методами досліджень?
- Коли ви наражатиметесь на найбільшу небезпеку?
- Коли ваші джерела наражатимуться на найбільшу небезпеку цілеспрямованого спостереження: під час вивчення чи виробництва матеріалу, коли історія завершена чи коли вона стане доступною для широкого загалу?

Додаткові питання про безпечнішу роботу в Інтернеті дивіться нижче в розділі "Дослідження та онлайн-доступ"

---

c) Якою є локація вашого завдання/історії?

- Що відомо про державний нагляд/цензуру в Інтернеті та мобільним зв'язком у цій місцевості?
- Якими є закони про використання шифрування, VPN або свободи слова у соціальних мережах?
- Що було опубліковано стосовно переслідувань чи прав журналістів, викривачів або активістів через їх онлайн-діяльність?

d) Ким є противники, які можуть становити загрозу вашій цифровій безпечці?

Поміркуйте про противників у двох категоріях:

i) НАВМИСНІ ПРОТИВНИКИ:

Це можуть бути уряди, підприємства, злочинні організації чи окремі особи, які виступають проти вашої роботи зокрема або викриття у ЗМІ в цілому. Подумайте, хто може зазнати певних втрат (юридичних, репутаційних, професійних тощо) у результаті виконання вашого завдання.

ii) НЕНАВМИСНІ ПРОТИВНИКИ:

Це можуть бути несвідомі хакери, які націлились на сервіс, яким користуються тисячі людей включно з вами. Це може хтось, хто зламає бездротову мережу або викраде ваше обладнання.

Онлайн-інструкція для подальшого читання:

ШИФРУВАННЯ→

ШКІДЛИВІ ПРОГРАМИ →

3. Ваше обладнання

Перерахуйте усі засоби зв'язку, які ви берете з собою.

Для кожного предмету зазначте:

- Які типи повідомлень ви будете надсилати та отримувати за допомогою пристрою (наприклад, SMS, електронна пошта, миттєві повідомлення, телефонні дзвінки)?
- Чи є або була якась конфіденційна інформація на цьому пристрої, яка може наразити вас на ризик або яку потрібно захистити?
- Чи завжди ви будете мати з собою свої пристрої?
- Чи залишатимете ви пристрій там, де хтось зможе отримати до нього доступ?
- Чи налаштовано на вашому пристрої перевірки безпеки (наприклад, паролі, шифрування тощо), щоб запобігти несанкціонованому доступу?
- Чи будете ви використовувати чиїсь засоби зв'язку або користуватися загальнодоступною Інтернет-мережею під час виконання завдання?
- Які заходи будете вживати для зменшення ризиків, пов'язаних з використанням цього обладнання?

Онлайн-інструкція для подальшого читання:

МОБІЛЬНІ ТЕЛЕФОНИ →

КОМП'ЮТЕРИ →

4. Ваші матеріали

Поміркуйте, які матеріали ви будете збирати або записувати під час завдання.

Для кожного матеріалу зазначте:

- В якому форматі матеріал (наприклад, фільм, текст, аудіо, фото тощо)?
- Чи є контент суперечливим? Якби до нього отримали доступ недоброзичливо налаштовані особи, чи створило б це загрозу вам або комусь іншому причетному до репортажу?
- Де/як цей матеріал зберігається? Чи вжили ви будь-яких заходів для захисту цієї інформації?
- Чи потрібно вам буде надсилати матеріал?
- Що ви робите для мінімізації ймовірності та серйозності загрози, яку може становити запис/передача матеріалу?
- Як ви переміщуєте свій матеріал через кордони?

Онлайн-інструкція для подальшого читання:

ЗАХИСТ ВАШИХ МАТЕРІАЛІВ →

ПЕРЕТИН КОРДОНУ ТА КОНТРОЛЬНІ ПУНКТИ →

5. Комунікації

Перерахуйте всіх людей, з якими вам потрібно буде контактувати під час виконання завдання, наприклад, респонденів, колег-фрілансерів, джерела та редакторів.

Для кожного контакту зазначте:

- Хто вони і хто може здійснювати за ними нагляд (роботодавець, уряд тощо)?
- Як ви будете з ними зв'язуватися? Чи з'ясували ви, який спосіб зв’язку є найбільш безпечним?
- Чи потрібно буде вам надсилати чи отримувати від них будь-яку конфіденційну інформацію?
- Чи перебування з ними в контакті наразить на ризик вас чи когось іншого? Що ви зробите для зменшення ймовірності та серйзності ризику?
- Чи є у вас план резервного копіювання та видалення повідомлень? Чи обговорювали ви цей план зі своїм джерелом?

Онлайн-інструкція для подальшого читання:

ЕЛЕКТРОННА ПОШТА→ | ШИФРУВАННЯ → | МОБІЛЬНІ ТЕЛЕФОНИ →

6. Дослідження та онлайн-доступ

Обміркуйте, до яких сайтів, інформації та контенту вам потрібен онлайн-доступ та зважте на всі потенційні ризики при цьому. Якщо доступ до онлайн-контенту може спричинити проблеми, складіть список, який допоможе вам врахувати небезпечні моменти.

Для кожного зазначте:

- Чи вивчали ви компанію, яка надає вам доступ до Інтернету та мобільного зв'язку? Чи мають вони тісні стосунки з урядом країни, в якій ви живете/працюєте?
- Чи вивчали ви законодавство, щоб дізнатися, як довго ці компанії зобов'язані зберігати ваші дані?
- Чи заблоковано цей контент у країні/регіоні, в якому ви будете працювати?
- Якщо вам потрібен доступ до заблокованого контенту, як ви це зробите?
- Яка вирогідність того, що за вашою діяльність здійснюється нагляд?
- Які заходи ви вживатимете для зменшення цих ризиків?

Онлайн-інструкція для подальшого читання:

НАВІГАЦІЯ В ІНТЕРНЕТІ →

ШКІДЛИВІ ПРОГРАМИ→

7. Ваш цифровий профіль

a) Чи перевіряли ви свій онлайн-профіль щодо контенту, який може становити загрозу вам чи вашим контактам?

- Чи вивчали ви себе в Інтернеті, щоб дізнатися, яка інформація про вас є відкритою, і чи вжили ви заходів для видалення даних, які не хотіли б бачити у загальному доступі?
- Чи публікували або коментували ви щось, де критикується ваш противник?
- Якщо так, то що ви плануєте робити для зменшення серйозності цього ризику?

b) У вас є один або більше власних вебсайтів?

- Чи може інформація, яка зберігається на них, наразити на небезпеку вас або ваші контакти?
- Якщо так, що ви плануєте робити для зменшення серйозності цього ризику?

c) Чи плануєте ви користуватися соціальними мережами під час виконання вашого завдання/історії?

Якщо так:

- Ви створили довгі надійні паролі для своїх облікових записів?
- Наскільки актуальні ваші налаштування конфіденційності на сайтах соціальних мереж?
- Чи ви активно долучались (твітили, поширювали, коментували, ставили лайки тощо) до контенту, який може наразии на ризик під час завдання?
- Чи є у вас окремі особисті та робочі облікові записи в соціальних мережах?
- Які ще заходи ви плануєти вжити для зменшення ймовірності та серйозності загроз, які може викликати ваша діяльність в соціальних мережах?
- Чи міркували ви над можливим психологічним впливом соціальних мереж на вас, вашу команду чи інших учасників?

Онлайн-інструкція для подальшого читання:

СОЦІАЛЬНІ МЕРЕЖІ →

Пам'ятайте!

Цифрова безпека — це лише одна частина плану забезпеченнябезпечності завдання або проекту, і її варто розглядати лише як частину вашої підготовки до забезпеченя безпеки. "Ресурси з питань безпеки та захисту" Rory Peck Trust можуть допомогти вам у інших сферах підготовки до безпеки.

Цей переклад було здійснено EU4IndependentMedia, що фінансується ЄС; ця публікація жодним чином не відображає позицій Європейського Союзу.