Digital Risk Assessment
Template

This Digital Risk Assessment will help you to identify and assess the potential digital security threats associated with your story or assignment.

As you work through the assessment, you will find links to relevant sections of our Digital Security guide. These will give you further information on how you can mitigate different digital risks and reduce your exposure to potential threats.

Review the **DIGITAL SECURITY** resources to help you complete this assessment.

Please save a copy of this form locally for your own reference.

RORY PECK TRUST

WWW.RORYPECKTRUST.ORG

Date

1. Outline your assignment

Before you can properly identify the major risks to your digital security, it's a good idea to break down your assignment and consider its key elements. Try to identify all the major components: the story, interviewees, travel arrangements and any other actions that are vital to your plans. Once you've done this, it will be easier to identify all the areas you need to consider for your risk assessment.

List and give as much detail as possible on the following:

Story outline

Key interviewees

Travel plans

Accommodation

Key Actions

2. What digital threats are posed by covering this story?

Now think about your key risks, threats and adversaries.

Remember, you don't have to be covering a controversial or sensitive story to be digitally vulnerable. You should get into the habit of completing a risk assessment for all assignments or stories, as the process may reveal potential threats that you had not already thought about.

Consider the following:

a) Will you be contacting or interviewing vulnerable people?

If yes:

- How will you store and protect the data of people you are interviewing?
- How and where will you store your notes and materials?

See the section below on Communications for more questions about contacting people securely.

b) Are you covering a sensitive or controversial topic?

If yes:

- Does it involve information that needs to remain secret or confidential?
- Do you understand and know how to use secure research methods?
- When are you going to be at greatest risk?
- When will your sources be at the greatest risk of targeted surveillance: during research or production, when the story is finished or when it goes public?

See the section below on Research and Online Access for more questions about working more securely online.

c) What is the location of your assignment/story?

- What is known about government surveillance/censorship of the web and mobile communications in that area?
- What are the laws around the use of encryption, VPNs, or the right to free speech on social media?
- What has been published regarding the persecution or rights of journalists, whistleblowers or activists over their online activity?

d) Who are the adversaries likely to pose a threat to your digital security?

Think of your adversaries in two ways:

i) INTENTIONAL ADVERSARIES:

These could be governments, businesses, criminal organisations or individuals opposed to your work or to media exposure. Think of who may face some cost (legally, reputational, professionally, etc.) as a result of your assignment.

ii) UNINTENTIONAL ADVERSARIES:

This can include random hackers targeting a service used by thousands of people, including you. It could be someone hacking a wireless network or it could be the theft of your equipment.

Online guides for further reading:

ENCRYPTION →

MALWARE →

3. Your equipment

List each piece of communications equipment you will be bringing.

For each one, state:

- What kind of messages will you be sending and receiving with the device (e.g. SMS, email, instant message, phone calls)?
- Is there, or has there been, any sensitive information on this device that could put you at risk or that you need to protect?
- Will you always have your devices with you?
- Will you be leaving the device where someone may be able to access it?
- Do you have security checks (e.g. passwords, encryption, etc.) set up on your device to help prevent unauthorised access?
- Will you be using anyone else's communications equipment or public internet access during your assignment?
- What steps will you take to reduce the risk that using this equipment could pose to you?

Online guides for further reading:

MOBILE PHONES →

COMPUTERS →

4. Your materials

Consider what material(s) you'll be gathering or recording during your assignment.

For each one, list:

- What format is the material (e.g. film, text, audio, images, etc)?
- Is the content controversial? If it were accessed by hostile parties, would this put you or anyone else involved in the report under threat?
- Where/how is this material being stored? Have you taken any steps to protect this information?
- Will you need to send material?
- What steps are you taking to minimise the chance and severity that recording/transmitting the material will pose?
- How are you moving your material across borders?

Online guides for further reading:

SECURING YOUR MATERIALS →

BORDER CROSSINGS AND CHECKPOINTS →

5. Communications

List all of the people who you will need to contact while on assignment, such as interviewees, freelance colleagues, sources and editors.

For each contact, state:

- Who are they and who could be monitoring them (employer, government, etc.)?
- How will you be contacting them? Have you researched which method of contact is most secure?
- Will you need to send or receive any sensitive information from them?
- Will contacting them put you or anyone else at risk? What steps will you take to mitigate the chance and severity of this risk?
- Do you have a plan for backing up and deleting messages? Have you discussed this plan with your source?

Online guides for further reading:

EMAIL → | ENCRYPTION → | MOBILE PHONES →

6. Research and online access

Think about what sites, information and content you will need to access online and consider the potential risks of doing so.

If accessing online content could cause you problems, make a list to help you consider the dangers.

For each one, state:

- Have you researched the company that provides you with both your Internet and your mobile phone coverage? Do they have a close relationship with the government of the country you are living/working in?
- Have you researched the law to find out how long these companies are required to keep your data on file?
- Is that content blocked in the country/region you will be working from?
- If you need to access blocked content, how will you do this?
- What potential is there that your activity could be monitored?
- What steps will you take to mitigate these risks?

Online guides for further reading:

NAVIGATING THE INTERNET →

MALWARE →

7. Your digital profile

a) Have you reviewed your online profile for content that could put you or your contacts at risk?

- Have you researched yourself online to see what information is available about you and taken steps to remove data you do not want in the public domain?
- Have you published or commented on anything that criticises an adversary?
- If yes, what are you going to do to mitigate the severity of this risk?

b) Do you have one or more personal websites?

- Could the information stored on it put you or your contacts at risk?
- If yes, what are you going to do to mitigate the severity of this risk?

c) Are you planning on using social media during your assignment or story?

If yes:

- Have you created long, strong passwords for your accounts?
- How up-to-date are your privacy settings on social media sites?
- Have you actively engaged in (tweeted, shared, commented, liked, etc.) content that could put you at risk while on assignment?
- Do you have separate personal and work social media accounts?
- What other steps are you taking to mitigate the chance and severity that your social media activity could pose to you?
- Have you considered the possible psychological impact of social media on you, your team or your contributors?

Online guides for further reading:

SOCIAL MEDIA →

Remember!

Digital Security is only one part of an assignment or project safety plan and should be considered as just one part of your safety preparations. The Trust's Safety and Security Resources can help you with other areas of your safety preparation.

RORY PECK TRUST