Introduction

This guide is meant to accompany the Rory Peck Trust’s Digital Security Risk Assessment template for freelancers. Here you’ll find help for each of the assessment’s questions and topics to help you practice better digital security on your assignment. You can find out more about how to protect your digital security by taking a look at Rory Peck Trust’s Digital Security Resource.

1. Outline your assignment

Before you can properly identify the major risks to your digital security, it’s important to write down what your assignment will actually involve. Try to identify all the major components of your assignment: all the interviews, travel arrangements and actions that are vital to your plans. Write these out to help you complete your risk assessment.

2. Identify the risks

A. Are you covering a sensitive topic?

If you’re working on a controversial issue, knowing who you’ll be working with and how you’ll transfer these details is important to protecting yourself and your sources. Here are questions to help you begin:

When are you going to be at greatest risk? When will your sources be at the greatest risk of targeted surveillance? While researching and investigating the story? After submitting it? After the story goes public?

How are you preparing yourself for possible increased surveillance? How are you helping your sources prepare?

START YOUR RESEARCH:

- Improving your communication privacy with “How can I avoid being monitored online?” at rorypecktrust.org.

The Rory Peck Trust supports and assists freelance newsgatherers worldwide
Website: rorypecktrust.org Phone: +44 (0)20 3219 7860 Email: digitalsecurity@rorypecktrust.org
GPG Fingerprint: BB34 7051 F327 C9E8 0BD0 12D5 8C72 C1D4 E4A8 8995
Digital Security Risk Assessment guide

To be used with the ‘Digital Security Risk Assessment’ template

B. The location of your assignment:

What is known about government surveillance/censorship of the web and mobile communications in that area? What are the laws around free speech and right to privacy, if any? What’s been published persecution or rights of journalists, whistleblowers or activists over their online activity?

START YOUR RESEARCH:

- Freedom House’s “Freedom on the Net” report
- Reporters Without Borders’ “Enemies of the Internet” report

C. Who are the adversaries likely to pose a threat to your digital security?

An adversary could be anyone trying to stop your work or who poses a threat as a result of it. What do you know about the people or organisations that could be potential digital adversaries? Think of them in two ways:

- **INTENTIONAL ADVERSARIES**: These could be government, businesses, criminal organisations or individuals opposed to your work or to media exposure. Think of who may face some cost (legally, reputationally, professionally, etc.) as a result of your assignment.
- **UNINTENTIONAL ADVERSARIES**: This can include random hackers targeting a service used by thousands of people including you. It could include someone hacking a wireless network you happen to be using at the time. It could also be the theft of your equipment.

This way will help you decide on password protecting your equipment or encrypting hard drives. You may want to install firewall protection and consider whether you should be using some online services that could put you at greater risk, or be more cautious about what you click on or download.

START YOUR RESEARCH:

- Reporters Without Borders’ “Enemies of the Internet” map
- The SecureList threat report map by Kaspersky
D. What ways will these threats be manifested?

- **Unencrypted communication**: In this situation, anyone monitoring your online or mobile traffic can access all the information you’re sending and receiving.
- **Metadata**: Many tools and services keep logs about who you’re communicating with, the date and time and subject lines. Files you create, edit or share can also contain metadata about you and your work.
- **Geo-tracking**: Your mobile phone is (and your computer could be) revealing your location so long as it’s turned on. Removing the battery (if possible) and letting any reserve power die out is one way to ensure your phone powers down completely.
- **Malicious software**: Your phone or computer may contain software you don’t know about that’s giving other parties access to it and anything stored on it.
- **Theft or confiscation of your equipment**: When it’s out of your sight, someone else could be accessing your device’s contents, making copies of it, or loading malicious software to remotely access it later.
- **Hacking attempts**: Network spoofing, man-in-the-middle attacks and other methods could be used to capture or redirect your internet activity and record what you’re doing.
- **Mass surveillance**: Many governments and companies monitor and record online activity. Some will trade this information among allies and partners.
- **Targeted surveillance**: If you’re working on a sensitive topic over a long enough time, you’ll end up on an adversary’s radar, and they may start trying to intercept your specific communications and find out who you’re working with.
- **Your other online activity**: It may sound obvious, but using social networks whilst working on something discreet can be a bad idea. You may be unwittingly linking your work with your personal life, revealing more about yourself to potential adversaries than you should be.
- **Your contact’s digital trail**: All the above items refer to areas where you can reveal your own digital trail. Even if you’re practicing good digital security, your contacts may not be. Be careful how much personal information you share with them. Assess how you’ll encourage them to be safer.

**START YOUR RESEARCH:**

- Rory Peck Trust’s [Online Resource on Digital Security](mailto:digitalsecurity@rorypecktrust.org)
Digital Security Risk Assessment guide
To be used with the ‘Digital Security Risk Assessment’ template

- Security in a Box and Me and My Shadow by Tactical Technology Collective

The risks you may face

Look at the possible digital threats from the perspective of what you’re trying to protect. This should fall under two main headings:

- **Identity**: This could be your own, or the identities of people you’ll be on contact with. Is it important that the content you’re working with isn’t traceable to someone’s real identity? Write down the various identities of all involved and what could happen if an adversary knew they were assisting you. If you think that this could put you under threat, then you should focus on behaviours, tactics or services that offer more anonymous methods to communicate.

- **Data**: This could be text, images, video, spreadsheets or anything transmitted electronically. Could someone use this content to harm you or others, or stop your assignment before you’re finished? Write down all the ways this data could be used. If you think that it could be used against you, you should prioritise strong encryption for all your data at risk.

START YOUR RESEARCH
- Check out “What’s Digital Security About” rorypecktrust.org.
- Visit “Me and My Shadow” to learn more about your digital profile.

3. Understand your equipment

In the section above, we identified your digital equipment as a potential threat. Here’s where you’ll dig deeper into what poses a problem and how to deal with it.

A. What kinds of messages will you be sending or receiving?
Is your communication encrypted? Are your service providers sharing your information, making data visible? How do you know?
START YOUR RESEARCH:

- How can I avoid being monitored online?
- How can I send a file privately or anonymously?
- How can I keep a file from revealing my personal details?
- How can I use my mobile phone more securely?
- How can I manage my phone's data footprint?

B. Is there, or has there ever been, any sensitive information on this device that you need to protect?

If the topic you are covering is sensitive, it’s likely that it will involve information that was intended to remain secret or confidential. How are you making sure this information is protected? Do you have strong encryption set up on the device where the information is stored?

One way to determine if you should encrypt an electronic file is to think about it as if it were a physical thing: If it was a paper document, would you shred it before throwing it out? If someone found it, would the contents potentially pose a risk to yourself or anyone else? If the answer to either is yes, then you should encrypt that file.

C. Will you always have the device on you? (Hint: The answer is likely ‘no’)

Think of all the possibilities: theft, confiscation, accidental loss, a mix up at the airport, leaving your computer or mobile in another room, taking it to the repair shop, storing it in a hotel while you’re out... these are just some of the reasons you may not have a piece of technology with you at one time or another.

What information is on your mobile, laptop or other devices? What would happen if it were to end up where it shouldn’t? Do you have any security checks (e.g. passwords, encrypted hard drive and/or files, etc.) set up on your device to prevent unauthorised access? Could you securely erase or hide files so they wouldn’t be discovered?

Don’t leave any assignment-critical device alone in your hotel room or elsewhere. Invest in a comfortable backpack or other method of carrying bag that you won’t mind...
carrying for long periods of time, and avoid bringing technology that you don’t really need.

START YOUR RESEARCH:
- How can I keep my content safe if my computer is taken?
- How can I permanently remove a file from my computer?

D. Will you be using anyone else’s communications equipment or public internet access during your assignment?
There’s added risk whenever you use someone else’s technology, or access the internet through public networks. How are you avoiding a data trail that could expose confidential information? How are you making sure your connection is private? Be realistic about where you’ll be working and how much you’ll be relying on internet cafes, borrowed equipment, public wi-fi and so forth.

START YOUR RESEARCH:
- How can I safely use public networks or shared computers?
- How can I avoid malware?

4. What material will you be recording/transmitting?

A. How will you be securing the material you will be recording?
If you are recording material digitally, you should be encrypting it. The different tools for encrypting all have their advantages, drawbacks and strange quirks. For strong end-to-end encryption to work, your recipients will also need to be using the same encryption system to access your files. Agreeing with one another how you’ll do this, and testing it in advance is crucial.

B. Is the content controversial? Could it put you or anyone else involved under threat?
Could your source material identify confidential sources or anything you don’t intend to publish? Will you use any techniques or technology to hide someone’s identity in
the field, or will this happen during editing? What could happen if the source material was leaked before you took these precautions? **There are a number of apps and software that can help.**

C. Where/how is this material is being stored?

Are you storing your material in the cloud, or on a hard drive, usb stick or other device? It sounds straight-forward, but the better choice depends on which threat you’re trying to deal with. What do you know about potential adversaries and how they’ve obtained files from other journalists in the past?

**Option 1: Storing it online.** This is what people mean when they say, “in the cloud.” If your content is stored online, you can erase it from your hard drive. This could be helpful when attacks are directed at the physical machines themselves. It’s not without its issues, though. How secure is the online storage service? Where is it physically located and what are the various laws protecting privacy there?

**Option 2: Storing it locally.** Ensure your equipment is password-protected. Use encrypted hard drives. Secure local storage keeps you in direct control. It’s useful when internet connections are slow, absent, monitored or censored. The downside is that you’re carrying all your source material with you. A thorough search could reveal that second USB stick hidden somewhere. Enough interrogation can compel anyone to reveal their passphrases.

D. Will you need to send the material?

If you are planning on transmitting the material during assignment, explore the ways you can add security to the process.

1) **Content:** Would the content you’re sending put you or others at risk if revealed to an adversary?

- **Reduce risk:** The best method is strong-end-to-end encryption, but find what works best for your assignment. Set it up and test it with your content’s recipients in advance. Develop methods (a secret question, for example) to
Digital Security Risk Assessment guide
To be used with the ‘Digital Security Risk Assessment’ template

test on one another to ensure you’re both who you say you are online before trading sensitive information.

- **Limit what the files say about you:** You may have encrypted your content and created generic online accounts to send it, but metadata can reveal things you didn’t intend. If you’re using widely monitored or public networks, this could be a concern.

2) **Identity:** Would you or the recipient be at risk simply for being in contact?

- **Mitigate identity risk:** If you can’t be seen to be sending or receiving information from certain contacts, then come up with alternate methods to communicate with one another, preferably in person to start. Perhaps you’ve set up mutual generic email addresses or file sharing services that aren’t related to your actual identities. Be sure only to access these through secure networks and proxy services (such as Tor) or a strong VPN. Try not to leave traces of your activity on your computer.

START YOUR RESEARCH

- How can I send a file privately or anonymously?
- How can I keep my content safe if my computer is taken?
- How can I keep a file from revealing my personal details?

5. **Who will you be contacting and/or working with?**

When you’re sharing what you determine to be confidential information with someone, you’re putting trust in that person’s ability to keep the information safe.

A. **Who are they and who could be monitoring them (employer, government, etc.).**

List either specific sources, or source types and classify them in a way that makes sense for your assignment: On the record, off the record, deep background, and so forth. You could also be organising them another way: military, government agency, police, corporate employee, activist/partisan, civilian, whistle blower, etc.
For each of these, write down: Who they are; What’s their role is in your assignment; and who or what stands to be damaged by their involvement. This section’s information could likely overlap with your overall communication plan and safety risk assessment.

B. How you will be contacting them?
What are you going to be talking about? Who could be trying to stop you and/or them? What methods might an adversary use to monitor or interfere? Knowing all this information, what steps could you take? Some examples: In-person meetings, generic, anonymous email addresses, encrypted emails or chat services, intermediaries that can pass information.

C. Will need to send or receive any sensitive information from them?
How will you obtain it from the contact? (email, file sharing, a USB stick, on paper)? How will you be storing it and accessing it? Will you be contacting others to verify the information?

Information is like water: It leaks. It’s part of your job to keep it from putting yourself and your contacts at risk. The best way to strategize safer communication (whenever possible) is in person. You can test different methods, make agreements, set up security questions, or verify keys if you use GPG encrypted emails.

D. Will contacting them will put you or your contact at risk?
Write down the various kinds of risks (personal and professional) that could arise in contacting people and categorise them.

Now that you’ve identified which kinds of contacts or sources pose which kinds of risks, you can start to strategize different ways to work with them. There are no 100% secure methods, but there are practices that increase the likelihood of safer communication.

START YOUR RESEARCH:
- Protecting journalist sources: Lessons in communicating securely by Sarah Marshall
- How can I send a file privately or anonymously? at rorypecktrust.org
Digital Security Risk Assessment guide
To be used with the ‘Digital Security Risk Assessment’ template

- How can I use encryption with contacts? at rorypecktrust.org

6. What will you be trying to access online?

Think about all the websites you use. Include any online, mobile services or systems you may need to access on assignment. Write down all of the ones that could cause you problems. Does the government block them? Could they be subject to increased monitoring? How easily could they be hacked?

When answering the questions in this section of your digital security risk assessment, take notes on these questions: What do you know about the government’s censorship abilities? What do you know about the government’s ability to monitor individual internet and phone use? Who are other actors (criminal organisations, militants, private companies, political groups, etc.) that may have an interest in monitoring your online behavior?

START YOUR RESEARCH:
- How can I avoid being monitored online?
- How can I access blocked content?
- How can I safely use public networks or shared computers?
- How can I use my mobile phone more securely?
- How can I manage my phone’s data footprint?

7. Manage your digital footprint

Online presence
Do you have a personal blog, portfolio or website on your own domain name? It’s useful for getting work and showing your talent, but it can also cause problems. An adversary could look up your previous work and decide to target you. They could use your online activity to find out more personal information than you’d want them to know.
Start by searching for yourself using Google, Bing, DuckDuckGo or any number of other search engines. List which (if any) of search results could put you at risk on your upcoming assignment. How many of these items are on sites that you control? How many are on sites that others control? How much social activity by others regarding this content can you find?

Don’t try to disappear from the internet. It’s impossible to do, and you’re better off having an online presence that roughly matches how you’re presenting yourself. Some corroborating search results and a few web pages can be a good alibi.

A. Do you have one or more personal websites? List each one.
   If it’s a website you personally control, decide whether you need to remove some of the content, or if the whole site should be unavailable. After you remove the content, see if there’s been any recent social activity around it that could be public.

   Submit your site to be re-indexed by search engines (Here’s how to do it on Google). If you’ve unpublished or deleted just a few pages offline, submit those URLs to be removed from search engines (Here’s Google’s request form). Remember, though, doing so can take some time. Usually if nothing controversial appears in a short search, people won’t continue to look unless they have a reason to think there’s something to find.

B. Is your work featured anywhere online?
   List the articles or other mentions of you online that could pose a threat on your assignment. Contact the site owner and talk to them about it. You may want to request that they remove the content, or simply unpublish it until further notice. Or you may want to ask them to simply remove your byline for the time being. Remember, though, less is in your control here and the site owners can always cite their own terms and conditions if you’ve submitted content for them to publish. Being polite and honest about the situation often helps. Also, if these pages show up from searching your name, remember that they’ll still continue to appear until search engines get around to re-indexing those pages. Doing this just before leaving on an assignment will offer little security, and you will need to leave enough time to do this properly.
Watch out for trolls! It may be that your work has been negatively reviewed or profiled by someone who’s decided they have something against you. They may refuse to remove content or even make a bigger deal out of it if you contact them. This is one situation where it’s good to have other more popular, relevant content published that shows up more highly in search results. You should also have ready some way of explaining it or discrediting it should someone try to use it against you.

Social media

A. How up-to-date are you privacy settings on social media sites?  
Most all social network sites have different privacy settings, but these change, so make sure you know how yours are set before starting your assignment. Decide whether you should make your social profiles temporarily un-accessible or if you should delete them.

B. Have you actively engaged (tweeted, shared, commented, liked etc.) in social media content that could put you at risk whilst on assignment?  
Search the feeds and timelines on your various social profiles for words and phrases that may be related to your assignment, the region you’ll be working or other hot-button words that may cause problems. Consider hiding or deleting these if they’ll be a problem. Remember, if others have shared your social content, it could remain available elsewhere.

C. Do you have separate personal and professional social media accounts?  
If you answered no, then you could be putting your family and friends at risk. You’re also meeting people on assignment who you may not trust enough to be within one click of your personal life. Increase the privacy settings on personal accounts. Make them non-searchable, or possibly disable them while on assignment. Create a profile that you’d want contacts to find, or steer them toward a work-related email address.

D. What steps are you taking to mitigate the chance and severity that your social media activity could pose to you?  
Write down what you can control and what you can’t control. Are you taking
some of the measures suggested above? Ask yourself how you’ll explain this content should someone try to use it against you.

START YOUR RESEARCH:

- **How can I use social networks safely?** by Rory Peck Trust
- **Me & My Shadow** by Tactical Tech

Digital security is only one part of your safety preparation

Thinking about the potential risks that your digital communications can cause is a good place to start, but it's one of many concerns that you need to plan for when beginning a project where the topic or location may attract threats.

Take a look at our [Safety and Security resource](#) for more information about the risks you can face whilst on assignment, and the things you can do to help minimise them. Or alternatively, click on the links below to find out about Risk Assessments, Communications Plans and Proof of Life documents.

- **Get the Documents and Get Started**
- **Creating your Communications Plan**
- **Putting Together a Proof of Life Document**