July 2023 | Investigative Journalism in the Digital Age: An Online Safety Checklist

Public Media Alliance

CHECKLIST

This ten-point checklist highlights key tips for journalists undertaking digital approaches to investigative journalism. This checklist is not suitable guidance for working in war zones. Reporting in areas of armed conflict requires a different kind of specialist training, contacts, and vigilance.

1

Click wisely.

Do not click on links sent to you in email or on social media unnecessarily– particularly if the message has a sense of urgency. 'Phishing' attacks like these are the most common way a hacker can infiltrate you or your organisation.

2

Double up.

Two-factor or multi-factor authentication provides an additional level of security by protecting your account with something you know (normally a password) and something you have (an access card, or code from your phone.)

3

Be prepared.

If the online service has a method of setting up account recovery in the event of an attack or if you are locked out, ensure you set up those steps and keep a note of those details safe.

4

Don't be obvious.

Strong and long passwords are the key to online security. Your accounts can be hacked in random or targeted attacks. Loss of control over your email can also put your organisation, colleagues, and sources at risk.

5

Be original.

Do not repeat passwords in different accounts. Use a unique password for every site. Password managers such as KeePass might be helpful. You could also keep a written note of password hints to help you remember, but do not write your actual passwords down.

6

Keep it concealed.

Laptops and memory sticks are attractive to thieves and to those who might want to interfere with your work. These should be encrypted. Computers and phones should have encryption automatically, but check this is also true for all types of memory cards and sticks. You should always anticipate that you might lose data. Encrypted data is impossible to read without your passkey which protects your investigation and your sources.

7

Back it up.

Backup your data regularly. If you work for a large organisation do not assume your employer is doing this for you. Encrypt your backups. Online backup services may not use encryption so check if you need to do this before uploading. Veracrypt is a useful tool for this.

8

Reduce your exposure.

Much of the data sent over the internet is readable by others, particularly email over public WiFi. Operators of online services may also be able to read what you upload, or governments may be able to force them to. Options for email encryption include Protonmail, Flowcrypt and Mailvelope.

9

Keep it secure.

Your mobile phone may contain a lot of information about your sources and your investigation. If this were to be lost, stolen, or confiscated, your sources could be identified and targeted. Governments may be able to take your phone off of you during a search and copy its contents or compel you to unlock the device. Consider obfuscating important contacts and whistleblowers, using pseudonyms, or not holding those details electronically.

10

Assess the risks.

When planning digital investigative coverage, assess the risks in the same way your newsroom would for any reporting journey away from your newsroom. Consider resources, such as Rory Peck Trust's digital risk assessment template.

Developed in partnership with

BBC
Grace Wyndham Goldie (BBC) Trust Fund

Namibia University
of Science and Technology