ICT4D Collective

Using digital technologies safely, wisely and securely:

a short guide for small civil society organisations

Tim Unwin

On behalf of the ICT4D Collective
https://ict4d.org.uk

Version 4
August 2024

It is not a matter of "if", but "when" your organisation will suffer from a cyber-attack of some kind.

This could either be direct through your own digital environments, or you could be impacted by an attack on an organisation you work with. It is therefore essential to take all the precautions that you can to keep your staff and those you work with safe. Digital technologies can be used to bring many benefits to organisations, but it is essential to mitigate the harms so that the benefits can be realised.

Is it safe? Is it wise? Is it secure?

This short guide is designed to provide small civil society organisations (especially those with few resources) with basic advice on how to use digital tech safely, wisely and securely/privately. It is not intended to be all-inclusive or highly technical, but instead focuses on things that should be done by all civil society organisations, regardless of their technical or financial capacity. Basic cyber-security is essential, and with evolving technologies the threats are only going to get worse. Adopting these key practices will not necessarily prevent you from being attacked, but they should reduce the chances and impact of such attacks, and will help you to get back online as soon as possible.

How would you react to, or prevent, the following scenarios?

> You are the founder of a civil society organisation providing refuge to women who have been subject to violent domestic abuse. Your website showed pictures of some of the women at one of your shelters, and pictures from it were shared on social media. One day, a gang of youths including a man who had previously assaulted one of the women, attacked those at the shelter, and killed two of the women.

> You run a large organisation supporting children at risk of living and working on the streets, and keep a record on your computers of the contact details of all your staff, those you work with, and their families. You open the organisation's main computer on arriving at work one day and discover that you cannot access the data and there is a large image and text on your screen saying that your data will be shared openly on the web unless you pay a large ransom that would bankrupt your organisation and ruin your reputation.

The following guidance notes are kept as simple and clear as possible, with minimal use of technical language. Recommendations in red are deemed to be essential; those in blue are highly recommended.

What is of most importance to you? Plan to protect.

As the examples above suggest, you should begin by thinking about what data or information you need to protect most within your digital systems, and then create a plan to help achieve this. For some organisations working on sensitive issues with very vulnerable people, this might be ensuring that these people's identities are always kept as secure and inaccessible to others as possible. For others, it could be always being able to communicate with staff members in the field, and for yet others it could be ensuring that your historic archives are preserved for the future. You need to think about *what* information you have, *why* you have it, and *whether you really need it have it online* at all. If all you begin by doing is simply identifying your top five priorities, and start trying to ensure that they are protected, then you will already have made a significant step forward. However, never forget to have a non-digital back-up plan as well, so that you can continue to deliver your services and do your work without having to use your digital systems should the need arise.

Alongside this, build a culture of cyber security among all your staff and those with whom you work. This should involve them in decision making so that they can input their ideas, and own the resulting guidelines and practices. Your plan should also focus on collective support (helping others to adopt good cyber hygiene practices) rather than individual punitive measures (blaming someone for a security breach). To this end, it can be very helpful to have appropriate and relevant cyber security posters and slogans displayed prominently in your offices and public spaces (see Annex of examples and further resources). This helps to build an all important cyber security culture among your team, and can additionally also raise awareness of these issues among those who visit your offices.

Know the sorts of attack that you are likely to encounter.

There are numerous types of cyber attack and fraud that your organisation could encounter, but some of the most likely to affect civil society organisations are (in alphabetical order):

- *Deep fakes*: using AI-generated images, audio or video to damage reputations or influence public opinion.
- *Identity theft*: when an attacker accesses your identity/credentials and masquerades as you. This is difficult to detect because the attacker will mimic your normal behaviours and passwords.
- *Malware*: a generic term used to refer to any malicious program or code that is created with the intent to do harm to a computer, network or server.
- *Phishing*: an attack that uses email, SMS, phone, social media, or social engineering techniques to entice you to share sensitive information — such as passwords or account numbers.
- *Ransomware*: malware that encrypts your data and the attacker then demands a payment in order to restore your access to files and network. This is now one of the most frequent forms of attack and threatens many different types of organisation. A double-jeopardy ransomware attack is when the attacker also threatens to publish your data online.
- *Sextortion online*: extorting money or sexual favours from someone by threatening to reveal images or evidence of their sexual behaviour online.
- *Spoofing*: a technique through which an attacker disguises themselves as a known or trusted source (such as a friend or a bank). In so doing, they are able to engage with you and access your systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on a device.

These vary considerably in frequency, depending in part on the type of your organisation and the local context. However, the risk of fraud through spoofing is probably the most common that you are likely to encounter (often known as Business Email Compromise). This happens most often when a spoofed e-mail or message asks for money to be transferred, and the main protection is procedural rather than technical. You need to create a basic culture where unusual requests are always treated with suspicion, and ensure that correct payment authorisation processes are always in place.

Remember that new forms of fraud and attacks are always being developed. It is therefore very important to keep your organisation updated and regularly to update your guidance in response to any new types of threat.

Your staff: highest risk, and first line of defence

Most hacks to digital systems are caused by “human error” involving someone accidentally clicking on a link that takes them to a spurious site. It is becoming increasingly difficult to detect such scams, and staff should be encouraged to consider any unexpected incoming messages as being potentially hazardous.

- Appoint one trustworthy (and tech savvy) member of staff as being responsible for overall digital security whatever the size of your organisation, and ensure that they
    - Are appropriately trained (with regular updates).
    - Put in place an incident response and recovery plan that includes at a minimum
        - The systems that are critical and important to the organisation.
        - Who to contact or report the incident to for assistance.
    - Know details of the relevant national CSIRT (Computer Security Incident Response Team; or CERT Computer Emergency Response/Readiness Team) protocols. Although these are generally intended for larger organisations, they often have good advice and suggestions.
    - Share regular updates on the latest threats with all staff.
    - Encourage an atmosphere of open reporting rather than blame.
    - Report regularly on cybersecurity to the CEO/Board or equivalent.
- Ensure all staff use complex and unique usernames and passwords for all their different logins and apps.
    - All passwords should be at least 12 characters long, and preferably use numbers, lower case characters, upper case characters and symbols.
        - Whilst these may be difficult to remember, printing them on hard copy and keeping them in a secure place may be safer than keeping them in a folder on your device.
        - Passwords should be regularly updated, and immediately changed following the announcement of any data breech for which they might have a login.
    - An alternative approach to creating passwords is to use three random words, such as apple rift ocean and to create a single password “appleriftocean” out of them (again over 12 characters long). This combines being easy to remember with length, and to create diversity you could use the words in different order for different purposes, as in “oceanapplerift”.

- Require multiple authentications for all logins, both relating to the organisation and their personal lives (at least dual, 2FA, meaning two different systems or factors/categories, such as a mobile device and a laptop, or also using face recognition, for authenticating access to a device; MFA is multi-factor authentication; note that 2SV is two-step verification, which requires two steps but usually from the same verification category)
    - Various apps are available for enabling dual authentication, including
        - Duo Mobile (Cisco)
        - Microsoft Authenticator
        - Google Authenticator
- Provide annual training/updates for all staff on cybersecurity, and encourage them to take responsibility for their own safety and security online, both at work and in their personal lives.
- Do not allow use of work-related devices and apps for personal use by staff.
- Ensure that when staff or users leave your organisation their accounts are disabled or terminated, and personal data are removed from your systems.
- Volunteers and temporary staff can be a particular source of vulnerability, so make sure that they are fully trained and adopt your cyber-security policies before doing any work for you.

Data Security and Management

Data are the lifeblood of any organisation, and include information about staff, clients, partners, your networks, and the organisation's activities. Maintaining security and privacy with respect to these data should be a very high priority. To this end, the following good practices are recommended.

- Back up, back up and back up again. Keep secure multiple copies of your crucial data so that it is easier to start up again should you be hacked or subject to a ransomware attack.
    - Decide whether you wish to do this in the Cloud or on multiple secure hard disks in different locations (or even on paper).
        - Separate locations are important should there be a physical break-in, fire, or natural disaster
    - Consider having back ups on devices running different operating systems (one on Windows and another on macOS or Linux) in case one entire system is compromised.
- There are diverse opinions as to the pros and cons of each option, depending in large part on your priorities and expertise, but the important thing is to make sure you back up data.
- Know the legal position in your country with respect to your data management practices, and ensure that you comply.
    - The European GDPR (General Data Protection Regulation) is a useful model to follow if you do not already have a national policy
- At the very least, ensure that you have permission from individuals to hold any personal information/data about them.
    - And delete all such information should you no longer need to keep it.
        - Regularly check with those about whom you hold information that they are content for you to continue to hold it.

- Ensure that private information about people is always kept in password protected files in encrypted folders.
    - And make sure you keep a secure record of all the keys/passwords.
- Limit access of staff to private data about other staff and clients (text, images, audio, video) on a need-to-know basis.

Your Organisation's Digital Systems

An organisation's digital systems can usefully be considered as having three interconnected elements: devices, software and networks.

Devices

- Only purchase hardware from reliable sources.
- Factory reset all secondhand devices.
- Ensure that you update operating systems (most commonly Windows, macOS, or Linux) whenever a new version is issued.
- Ensure that all devices are physically secured.
    - Physical break-ins are a common source of data loss, and it is expensive to replace hardware.
    - If your mobile device is stolen, ensure that you erase all data from it remotely as soon as possible (using the Find My Device app for Android or Find May app for iPhones – remember to have these apps switched on before losing your device)
- Do not permit use of USB sticks to transfer data between devices.
- Consider using a circuit breaker to protect your electrical circuit from damage caused by a power surge.
- Limit your use of "smart" devices, they can generally all be used to track your usage and can be a source of vulnerabilities.

Software

- Use high quality antivirus software, and scan devices regularly.
    - Good antivirus software is freely available (good examples include Avast, AVG, Avira, Bitdefender, McAfee, Norton and Sophos – choice depends a bit on your Operating System).
    - Ensure that it has antivirus, web protection, ransomware and malicious traffic retention capabilities.
    - Remember to run full scans of all devices on a regular basis (preferably at least monthly).
    - Consider subscribing to a reliable source providing information about the latest scams and hacks (often free), such as
        - Experian https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/
        - Ofcom https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/top-tips-to-stay-safe-from-scammers/
        - Which https://www.which.co.uk/news/article/the-latest-scam-alerts-from-which-aBRLy2b02WkC
- Only purchase software from reliable sources or vendors.
    - Or use reliable Open Source software if you are familiar with how to install and use it.

    - Remember that there is much good free/low cost software available.
    - Never use pirated software
        - It may well contain malicious code.
        - It is likely to be out of date and not contain the latest security fixes.
- Ensure that most users within your organisation do not have “administrator status” or “access”, and try to limit use of software only to those who really need to use it.
    - Adopt the Principle of Least Privilege, whereby unnecessary high-impact permissions (such as admin access) to potentially damaging actions through a compromised account are limited.
    - Regularly monitor admin user accounts to ensure that they have not been compromised.
- Always update software as soon as new releases are available.
    - These usually contain security updates which help to protect your systems.
- As noted above, ensure that all users have complex passwords.
- Limit the apps and software available on organisation’s devices.
    - Do not allow individuals to upload their own software on organisation’s devices.

Networks

- Use a reliable Internet provider, cloud service provider, and managed service provider
    - Ensure they have clear Secure by Design practices.
    - This helps limit potential supply chain risks.
- Ensure that your routers and any IoT (Internet of Things) devices are password protected with complex passwords that are regularly changed.
- Create a guest network on your WiFi should you wish to provide access for guests.
    - This enables you to have your main network separate behind a firewall that helps to protect it from malicious attacks.
- Do not have passwords for your WiFi networks posted visibly on walls or notice boards where they could easily be photographed (if only by accident).
- Ensure all external access to your systems go through a VPN (Virtual Private Network).

Your Website

Your website is your window to the world. The following advice should help you to maintain a secure presence:

- Remember that everything on your website can be copied and used elsewhere on the web.
    - What don’t you want people to see?
- Ensure that you use a reliable and secure provider to host your website.
- Regularly back up the data on your website.
- Have a clear policy about what imagery you wish to show on your site, and ensure that it is complied with. Think especially about:
    - Whether you want to show people’s faces, or enable them to be identified.
        - This is especially important if you are working with potentially vulnerable adults and children.

- Where possible get a SSL (Secure Sockets Layer) certificate which enables you to use secure hypertext transfer protocols (https) rather than just http. In https, the browser and server establish a secure, encrypted connection before transferring data.
- Frequently test your website for potential security vulnerabilities.
- Keep the domain name/address (URL) as short, but meaningful, as possible.
- Generally avoid direct links to e-mail addresses to make it more difficult for automated programs to scrape it.
    - Use a contact page that directs messages to you.
        - Possibly also using a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
    - Or use an image of your email address.
    - Or, use the format a(dot)person(at)organisation(dot)org
- Some organisations prefer just to have a single external point of contact e-mail address such as info@organisation.org.
- Always update your add-ons and plugins.
- It is usually good practice only to allow a small number of people to author and upload material on your website.
    - Keep all access usernames and passwords confidentially secured.
    - Use different layers of security for different types of user, and only have one or two admin accounts.
- Follow any national guidelines or restrictions on websites.
    - Consider having policies on data use and cookies (files used by web servers to save information about users) to explain to users how you might be using their data and giving them options with respect to such usage.
- You do not need to spend a lot on expensive website design, but try to keep it simple and clear to provide the messages you want.
- Consider Vulnerability and Penetration Testing (VAPT) if you can afford it.

Social Media

Most civil society organisations will want to have a social media presence to publicise their work and connect with clients, but you should always be careful about the insecurities relating to using social media.

- Think carefully about which social media platforms you wish to use, remembering that they all profit in some way from the data they extract from you.
- Only permit a very small number of well-trained people who know your organisation well to upload material onto your social media accounts
- Use complex usernames and passwords everywhere (see similar comments above).
- Restrict membership of social media groups to trusted people.
    - On Facebook, for example, use group rules and ensure people agree to them before permitting them to join.
- Where possible use encrypted messaging apps such as Signal.
    - WhatsApp also uses Signal’s end-to-end encryption on all messages.
    - If you use Telegram always switch to “Secret Chat” mode, but end-to-end encryption even then is only supported for two participants.
- Do not let anyone (include staff, clients and visitors) post images of your activities or personnel without express permission being given.

E-mails

E-mails are the source of many vulnerabilities, and attacks to e-mail accounts are becoming ever more common.

- Have in place a system that regularly provides all staff with reminders about e-mail security, and notification about new types of threat or scams (see above) as soon as you are aware of them.
- Assume that any incoming e-mail that is not a reply to an outgoing e-mail from your organisation could be a threat.
- Never click on a link in an e-mail unless you are certain it is genuine and safe. Even then, think twice about it.
- Use SPAM filters set to a high level of protection (if possible).
- Use DMARC (Domain Message Authentication Reporting).
- Encourage all staff to contact the person responsible for digital security if they are at all suspicious of an e-mail, and definitely before they open it.
- Consider setting rules for incoming e-mails that only permit e-mails from trusted contacts to be accepted.
    - This can be very effective when used in conjunction with contact pages (see above).
- Always use bcc (blind copying) if sending an outgoing e-mail to many people.
    - So that they do not all receive each other's e-mail addresses.

Conclusions

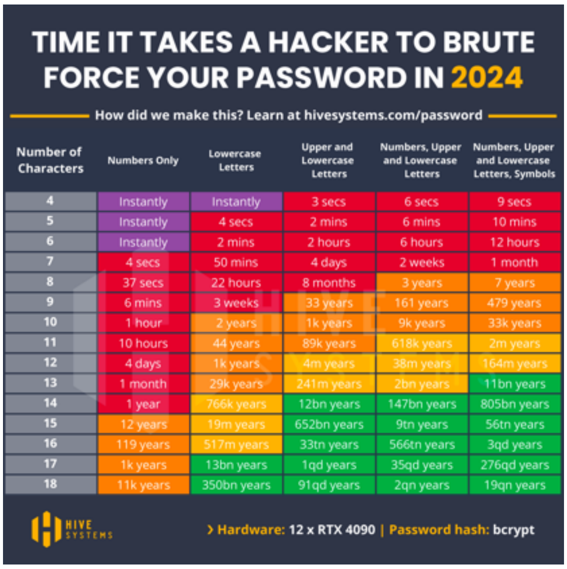
It is not possible ever to be 100% secure, but following the above advice will help you reduce the likelihood of your organisation being damaged through a cyber-security incident. Some final reminders:

- **Consider it likely that you will be affected at some time by a cyber-security incident.**
- **Have a plan in place to mitigate the impact of a cyber-attack.**
- **Appoint an appropriate person to have responsibility for digital security as part of their portfolio.**
- **Regularly train all your staff (including volunteers and temporary staff) in your cyber-security practices.**
- **Always use complex passwords and multi-factor authentication.**
- **Seek professional help as soon as possible should you be subject to a cyber attack.**

Is it safe? Is it wise? Is it secure?

Annex: Material that can readily be turned into posters or used as graphics in training courses

From Hive https://hivesystems.com/password
The time it takes a hacker to brute force your password in 2024. Brute force attacks use a trial-and-error approach systematically to identify login identities, credentials, and encryption keys. Combinations of usernames and passwords are used until the correct combination is found. Computers are able to do this very rapidly, and quantum computers will be able in the future to cut these times dramatically. It is essential to use multiple authentication methods to help reduce such threats.



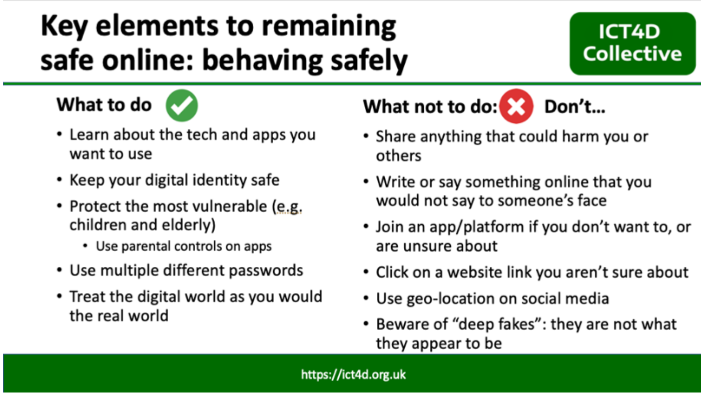
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS › Hardware: 12 x RTX 4090 | Password hash: bcrypt

From the ICT4D Collective
Three example of the diverse resources developed mainly during and following our work as part of the UKRI GCRF funded MIDEQ project (see our work on migration and digital tech). The slides can readily be printed off and posted on office walls as simple reminders. Full slide decks on different topics relating to the safe, wise and secure use of digital tech with graphics in multiple languages are available at https://ict4d.org.uk/sws/.



Key elements to remaining safe online: behaving safely

ICT4D Collective

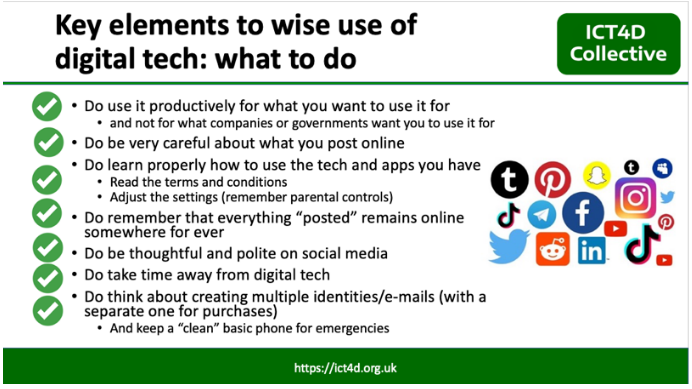
What to do ✓

- Learn about the tech and apps you want to use
- Keep your digital identity safe
- Protect the most vulnerable (e.g. children and elderly)
  - Use parental controls on apps
- Use multiple different passwords
- Treat the digital world as you would the real world

What not to do: ✗ **Don't…**

- Share anything that could harm you or others
- Write or say something online that you would not say to someone's face
- Join an app/platform if you don't want to, or are unsure about
- Click on a website link you aren't sure about
- Use geo-location on social media
- Beware of "deep fakes": they are not what they appear to be

https://ict4d.org.uk

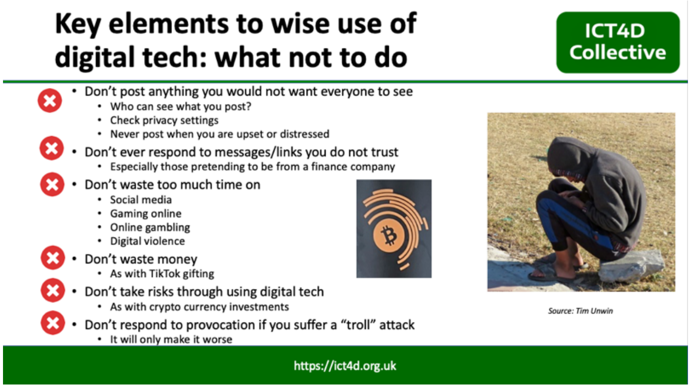


Key elements to wise use of digital tech: what to do

ICT4D Collective

- ✓ Do use it productively for what you want to use it for
  - and not for what companies or governments want you to use it for
- ✓ Do be very careful about what you post online
- ✓ Do learn properly how to use the tech and apps you have
  - Read the terms and conditions
  - Adjust the settings (remember parental controls)
- ✓ Do remember that everything "posted" remains online somewhere for ever
- ✓ Do be thoughtful and polite on social media
- ✓ Do take time away from digital tech
- ✓ Do think about creating multiple identities/e-mails (with a separate one for purchases)
  - And keep a "clean" basic phone for emergencies

https://ict4d.org.uk



Key elements to wise use of digital tech: what not to do

ICT4D Collective

- ☒ Don't post anything you would not want everyone to see
  - Who can see what you post?
  - Check privacy settings
  - Never post when you are upset or distressed
- ☒ Don't ever respond to messages/links you do not trust
  - Especially those pretending to be from a finance company
- ☒ Don't waste too much time on
  - Social media
  - Gaming online
  - Online gambling
  - Digital violence
- ☒ Don't waste money
  - As with TikTok gifting
- ☒ Don't take risks through using digital tech
  - As with crypto currency investments
- ☒ Don't respond to provocation if you suffer a "troll" attack
  - It will only make it worse

Source: Tim Unwin

https://ict4d.org.uk

Further resources

Most of these are reliable, short, clear, and easy to access simple guides to specific aspects of cyber-security; a few are longer guides with mode detail specifically relating to the needs of civil society organisations.

Canadian Centre for Cyber Security (2024) Mitigating cyber threats with limited resources: guidance for civil society, https://www.cyber.gc.ca/en/news-events/mitigating-cyber-threats-with-limited-resources-guidance-civil-society.

CISA (Cybersecurity and Infrastructure Security Agency, USA) (2024) *Mitigating cyber threats with limited resources: guidance for civil society*, https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf

Civicus (2022) Safety & cyber security: 8 tips for civil society digital defense, https://www.civicus.org/index.php/media-resources/news/blog/6118-safety-cyber-security-8-tips-for-civil-society-digital-defense .

Cloudflare (no date) How to secure a website, https://www.cloudflare.com/en-gb/learning/security/how-to-secure-a-website/.

Coulson, G. (Betterteam) (2024) Cyber security policy overview and sample template, https://www.betterteam.com/cyber-security-policy.

Crowdstrike (2024) 12 most common types of cyberattacks, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

GDPR.EU (2018) What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/.

Gov.UK (no date) The National Cyber Security Centre, https://www.ncsc.gov.uk/.

IT Force (no date) 5 cybersecurity policies every medium-sized business needs, https://www.itforce.ca/blog/cybersecurity-policies-every-business-needs.

National Democratic Institute (2022) *Cybersecurity Handbook for Civil Society Organizations*, https://www.ndi.org/publications/cybersecurity-handbook-civil-society-organizations.

Rubenking, N.J. (2024) The best free antivirus software for 2024, *PC Mag*, https://uk.pcmag.com/antivirus/120817/the-best-free-antivirus-protection.

Splunk (2023) Top 50 Cybersecurity Threats, https://www.splunk.com/en_us/form/top-50-security-threats.html.

Tom's Guide (2024) The best encrypted messaging apps in 2024, https://www.tomsguide.com/reference/best-encrypted-messaging-apps.

Workable (2024) Company cyber security policy template, https://resources.workable.com/cyber-security-policy.

Authorship and acknowledgements

Version 4: This draft was first prepared by Tim Unwin in June 2024 on behalf of the ICT4D Collective, and was subsequently revised in July 2024, with thanks particularly to comments from G. "Hari" Harindranath, Jamie Proctor, and Jamie Saunders. Further revisions were made in August 2024, with thanks to Danilo Pereira Sato.