LIBRARIES FOR PRIVACY

a digital security and privacy toolkit

Protecting library staff and users in the age of Big Data

A Scottish PEN Publication

THIS TOOLKIT HAS BEEN BROUGHT TO YOU BY

Scottish PEN is the Scottish Centre of PEN International and was founded in 1927 as a not-for-profit organisation that champions freedom of speech and literature across borders. Scottish PEN campaigns on behalf of the rights of writers both at home and abroad, ensuring they can express themselves fully free from the threats of violence, censorship, intimidation and interference. We have been vocal opponents to the silencing of writers across the world and have campaigned on behalf of writers including Raif Badawi, Anna Politkovskaya, Liu Xiaobo, Ragip Zarakolu and Lydia Cacho, as well as leading campaigns in Scotland to reform defamation law, oppose pervasive surveillance and champion Scottish writing in all its languages.

Scottish PEN is a registered Scottish Charity with the charity number SC008772. Scottish PEN is a SCIO (Scottish Charitable Incorporated Organisation).

IN COLLABORATION WITH:

LIBRARY FREEDOM PROJECT

CILIPS Scotland's library and information professionals

SLiC Scottish Library & Information Council

This has been made possible through the generous funding of the Joseph Rowntree Charitable Trust

CONTENTS

TIEVIN WIR METADATA

This poem in Shetlandic was kindly donated to Scottish PEN for this toolkit by the 2014-2017 Edinburgh Makar, Christine De Luca.

Tievin wir metadata	Stealing
Hit's göd ta hae a place padlockit fae pryin: fae social networkin, bloggin, tweetin, textin an aa dis gödless googlin; fae uncan waelin	unfamiliar; selecting
trowe wir metadata, sturknin somewye.	Through; congealing
Dey mizzer your life bi virtual fitprints, bi your clood status; can tell whan last	They measure
you spack wi dis een or dat. We tink	spoke; this one or that; think
at we can sheeks ahint firewaas an	blether behind
passwirds, but der nae holy o holies.	there's
Foo fine ta hae a hert-hol, hiddlt	How; very centre; hidden
awa i da wippit recesses o da brain, da crevices o consciousness, whaar	tangled
only you can hack inta your ain mind; fin dat you can still surprise yoursel.	

-- Christine De Luca
Dat Trickster Sun, Mariscat Press, Edinburgh, 2014

ACKNOWLEDGEMENTS

This toolkit is the result of collaboration between a range of different people and organisations that have selflessly weathered a vast number of different versions and email correspondence to help us arrive at this final version.

Scottish PEN is an organisation that represents writers and while we have worked with libraries and library staff across Scotland, we are not library staff members and as a result cannot speak for the sector in terms of what guidance and insight would best support these institutions. So we would like to thank everyone from the library community who took the time to guide us through the working realities of library staff and volunteers to ensure this toolkit offers guidance that reflects the needs and concerns of libraries.

The strength of this toolkit is down to the work, patience, expertise and diligence of everyone who helped us produce it.

This toolkit is the result of a partnership between Scottish PEN, the Library Freedom Project, the Chartered Institute of Library and Information Professionals in Scotland (CILIPS) & the Scottish Library and Information Council (SLIC). We would especially like to thank:

- Alison Macrina the Founder and Director of Library Freedom Project
- Catherine Kearney (Director) and Sean McNamara (Policy & Digital Officer) of CILIPS
- Pamela Tulloch the CEO of SLIC

Scottish PEN would also like to thank:

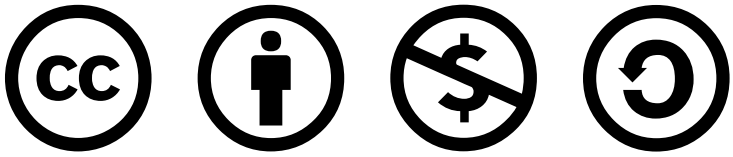
- Aude Charillon – Library & Information Officer, Newcastle Libraries
- Ian Clark
- Douglas Greenshields – Web Developer, Markup
- Wendy Kirk – Librarian at Glasgow Women's Library and all staff members
- Micah Lee – Security Engineer, The Intercept
- Rebecca Oliva – Head Librarian, Scottish Poetry Library
- The Radical Librarian Collective
- Kevin Sanders – Research Support Manager, University of West London
- Dr Lauren Smith – Knowledge Manager, Iriss
- Alana Ward – Libraries, Museums and Archives Manager, Inverclyde Council

We would also like to thank Christine De Luca for donating her poem **'Tievin wir Metadata'** to this toolkit and for her consistent, enduring and resilient support of our work.

This document was made possible by the generous funding of the Joseph Rowntree Charitable Trust.

Can I share or duplicate this work?

This work is licensed under the **Creative Commons Attribution-Non-Commercial-ShareAlike 4.0** International License. To view a copy of this license, visit www.creativecommons.org/licenses/by-nc-sa/4.0/



INTRODUCTION

If you have nothing to hide, do you have nothing to fear? This question has come to define digital surveillance, following the Snowden revelations in 2013 that forced into daylight the sheer scale and capability of intelligence agencies around the world to collect and analyse data in the name of national security.

But in the age of digital surveillance powers that seek to collect data on all to find the few, there is a distinct need to look to how we can protect the privacy of library staff and users across Scotland.

This issue is not monopolised by state surveillance as undertaken as part of law enforcement or terrorism prevention. The digital economy is based on a foundation of data collection, sharing and analysis. The process by which Internet services and platforms collect personal and usage data to deliver services and make a profit has shaped how we interact and engage with the Internet. With surveillance sitting at the heart of the digital eco-system we contribute to, an increased awareness of the seen and unseen transmission and sharing of our data, and steps we can take to take control our data is a growing concern for everyone online.

Libraries are a shared common good, enabling everyone, regardless of income, background, gender, sexual orientation, ethnicity or faith to receive and source information, communicate with others, apply for jobs or benefits and contribute to discussions with people across the globe. Libraries are many things to their local communities, but Scottish PEN believes they should not become spaces where personal data can be scooped up indiscriminately without due protections; our privacy is too high a cost to pay.

With increased obligations being passed on to libraries to collect and share the private data of its users, looking at how libraries can protect

the privacy and security of both their institutions and their users is a vital task when exploring the role of libraries in the digital age.

Developed in collaboration with the Charted Institute of Library and Information Professionals in Scotland (CILIPS), the Scottish Library and Information Council (SLIC) and the Library Freedom Project, as well as the involvement of library staff and volunteers we hope this toolkit will offer clear and practical guidance, as well as facilitating broad, open and inclusive debate on the vital issues facing the realisation and understanding of our fundamental freedoms in digital spaces, within the context of Scottish libraries.

In the national strategy for libraries entitled *Ambition & Opportunity: A Strategy for Public Libraries in Scotland 2015-2020*, developed by SLIC and the Carnegie UK Trust, the responsibility of libraries to protect the privacy of their staff and users was outlined as a clear priority for libraries across Scotland:

> Librarians have the understanding and expertise to champion and promote openness and the public's right to information; oppose censorship and efforts to inhibit access to information; select and make available information; guide and support the public to seek, obtain and navigate available information; support the public to utilise and share this information; facilitate intellectual and cultural creativity; **and safeguard the privacy of the public through ensuring data collation and surveillance are necessary, proportionate and lawful.** [emphasis added]

We hope this toolkit will offer practical steps towards realising this goal and catalysing debate about how libraries can continue to function as the vanguard for fundamental freedoms in Scotland and beyond. This toolkit is only the start of a conversation on what tools and practices are available to ensure libraries can continue to protect the digital security and privacy of their institution, staff members and users. We cannot, in this medium, offer an exhaustive guide as to guarantee total security or privacy (if, in fact, they exist in the first place). It is also important to note that the tools and practices suggested in this toolkit are sourced from a range of trusted sources authored by a range of established ex-

perts in the fields of computer security, journalism, activism and digital rights, but is by no means beyond interrogation or scrutiny. They also demonstrate, in the opinion of the toolkit's author, the most secure options available at the date of publication. There may be other similar tools available, which we do not intend to ignore or criticise. They also represent the most secure options at the time of writing and we cannot guarantee that vulnerabilities or more secure options will not be available after the publication of this resource.

There are also a number of powerful tools available to users that we have decided to omit from this toolkit, which includes (but is not limited to) PGP Encryption and more secure or decentralised operating systems such as Qubes and Tails. This is not a comment on their efficacy or suitability for protecting both online privacy and security, but is, instead, an editorial decision based on the desire that this toolkit is understandable to library staff and users from a range of tech literacy backgrounds. When evaluating the services provided in libraries we took the decision that these platforms would be harder to provide in the library setting, while also requiring bespoke technical support that went beyond the scope of this document. We would recommend that any library staff member interested in these tools should look at the resources in the link list at the end of this document or seek other independent advice.

All we can recommend is that you use this resource as a guiding hand when looking to improve your operational security and processes by which staff members, volunteers and users can take steps to secure their online privacy. Please interrogate each and every suggestion, research the field to see whether there are tools that better suit your needs, and reach out to others to learn all you can about what works best for you.

Nik Williams, Project Manager, Scottish PEN

CHECKLIST

There are many things we can do to ensure our data is protected and our systems, networks and devices are secure. Before we explore the many different tools or behaviours we can deploy to protect both our digital security and privacy here are a few tips:

1. **Keep your systems, devices and networks updated –** Ensuring you update your digital infrastructure regularly means that you are better protected against new and evolving threats. Updates respond to newly discovered vulnerabilities and so regular updates ensure you and your users are protected. Also avoid installing older pieces of software that are not currently supported – this means that newer threats may not be addressed, rendering your system vulnerable. Auto-Update features can help you ensure your systems are up-to-date without you having to manually monitor the status of each device.

2. **Do your research –** This toolkit is a start, but before looking to update your digital infrastructure or install new programmes be sure to research each tool or programme to understand its privacy and data usage policy, compliance with all industry standards and how often it is bug-tested and updated.

3. **Do not get blinded by the spin –** Sometimes the best tools are not the ones with the biggest marketing budget. Just because you see a certain tool advertised more regularly than others, does not mean it will offer you the best protection. Do your research, read reviews, reach out to experts or other users and analyse transparency reports to identify the best tools for you.

4. **Involve as many people as possible into the decision-making process –** Using Privacy-Enhancing Technologies (PET) may result in you using platforms, tools or software in your library that your staff

members and users do not recognise. Involve all stakeholders in your decision-making process to ensure that you have addressed all concerns. Flyers announcing why you have used certain tools, open meetings and announcements on the library website will enable all stakeholders to get involved and learn more. This can also act as a spur for your users to encourage them to follow your lead.

5. **Avoid dogma or polarisation –** Every library staff member or user does not need to be Ed Snowden, or hold a computer sciences PhD to protect their private data. Do not encourage an all-or-nothing approach to digital security. It will seldom be the case that every library or user will embrace or need to embrace every piece of advice contained within this toolkit. The best way for people to protect their private data is to encourage an open and inclusive process that enables individuals to choose what tools best suit their situation, technical literacy and comfort level. What is important is ensuring everyone, including library staff and volunteers, alongside library users, can make an informed decision.

✂ CUT OUT & TAPE NEAR YOUR SCREEN

Security News Consumer's Handbook

1. Wait for independent experts to weigh in.
2. If a story reveals security holes, ask who is most likely to be affected.
3. Beware language that ignores the likelihood of an attack.
    - Absolute language (e.g., "unbreakable encryption")
    - "Can," "could," "able to," or "it's possible to…" (e.g., "if they want to get in, a burglar *can* ram a Toyota through your front door")
4. Don't lean on one opinion. Look for the consensus of experts within and across stories.
5. Ask how expensive the threat really is (time, effort, financial, legal, technical resources).
6. Beware marketing terms (e.g., "NSA-proof," "military grade cryptography").
7. Know who to trust. Understand the political leanings and motivations of software creators.
8. Lend trust to open source software, especially when tested under security audits.
9. Don't judge software developers on the existence of vulnerabilities—judge them on how they respond.

OpenNews

A helpful guide created by OpenNews on things to look for when exploring different tools

USING THIS TOOLKIT

This toolkit has a number of distinct focus groups and areas, which are connected together by the library as an institution. But in spite of this connection, there are distinct differences between each group that will require a very different approach when we look to evaluate and address our digital security and privacy concerns.

In broad terms we have broken down the groups as:

- **The library –** The institution's digital infrastructure and procedures
- **Library staff and volunteers –** Delivering on the institution's procedures, while undertaking specific work that requires awareness of digital security & privacy issues, such as handling borrower data
- **Library users and broader community –** People who use the library for a range of services. The advice outlined in this toolkit will support library users both within the library and outside it

These are by no means discrete or disconnected groups – there are a number of overlaps between the groups i.e. library staff are responsible for library procedures but also, as individuals, they have their own specific requirements and needs, as well as potentially being users of libraries themselves.

SECURITY OR PRIVACY

It is important to distinguish between digital security and privacy. Many tools such as Google are secure (in that they protect against malicious attacks and malware) but do very little to protect your privacy from Google's own processes that capture user data. Tor is excellent in terms of protecting your privacy but is not as secure as Google in many respects. It is important to look at these properties as aspects that may overlap at times but remain separate and thus in need of being addressed specifically and separately.

TECH LITERACY

This toolkit is designed as an entry into the debate on digital security & privacy and is targeted at library staff members, volunteers and users with very basic tech literacy skills. When there are aspects that may require increased levels of expertise it will be identified in the designated chapter.

HYPERLINKS IN THIS TOOLKIT

Throughout the toolkit there are links for you to either download new tools discussed in the chapter or to find out more information about them. To ensure the toolkit remains readable, we have removed some longer URLs from the body text, instead hyperlinking relevant lines of text, which are accessible on the online version, but not the print version. All URLs can be found on the linklist on page 62.

For plugins for browsers and apps downloaded from app stores, we have hyperlinked the text where appropriate. If you are unable to click on these (i.e. viewing the printed version of this toolkit) it is recommended that you search for the app name in the relevant application store your device users.

To download the digital copy of this Toolkit: www.bit.ly/libraries-for-privacy-toolkit

This version of the toolkit was created on:

18th May 2018

Why is this here?
Threats against online privacy and security change as new technologies and capabilities evolve. As a result, we cannot guarantee that this toolkit will remain up-to-date or accurate in the face of changing circumstances. If you are using this toolkit a substantial time after this date, it is recommended that you seek out the latest information related to the tools and practices contained in this document.

INVESTIGATORY POWERS ACT

The Investigatory Powers Act (IP Act) was announced by the then-Home Secretary Theresa May in November 2015 to modernise and consolidate surveillance legislation in the UK. It passed through both Houses of Parliament at the end of 2016.

You can read the full act here

The government's summary of the bill when announced is as follows:

> A Bill to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

POWERS

The audacious piece of legislation is unlike any other seen in a western democracy, outlining broad powers that include:

- **Internet Connection Records (ICRs) –** the retention of ICRs of every British citizen for 12 months by Internet Service Providers that can be accessed by a range of public authorities. ICRs are a record of every website we visit and every smart phone app we access – they contain the main domain of every site visited i.e. Scottishpen.org not scottishpen.org**/about**.

- **Equipment Interference (EI) –** Government hacking that enables the intelligence services to access a device, system or network to obtain encrypted files, passwords and data; remotely control devices; gain access to further networks & devices; and potentially destroy devices.
- **National Security and Technical Capability Notices –** The method by which the Government will impose 'requirements' and obligations on tech companies, to ensure that they can carry out equipment interference, interception and mass data retention on the Government's behalf. This may include circumventing encryption and the installation of 'backdoors' into communications networks so the government can access data shared in real time.
- **Bulk Powers –** The targeting of the many to find the few. Bulk powers contained within the Act include Bulk Interception (intercepting data in transmission), Bulk Acquisition (acquiring and storing data), Bulk Equipment Interference (hacking) and Bulk Personal Datasets.
- **Bulk Personal Datasets –** These are databases and registers that contain information on a large group of people. These will be accessed, held and used by the intelligence agencies to make connections about who we are, what we do and who we know. These may include the electoral roll, HMRC tax returns and sporting events ticket lists.

For more information: Big Brother Watch

OVERSIGHT

The oversight mechanism in the IP Act is an improvement to the surveillance laws already in place across the UK (many of which were only avowed in recent years), but falls short of international norms.

Announced as "world-leading" by Theresa May when she announced the bill to Parliament, many of the powers within the bill will be subject to a 'double-lock' procedure. When seeking powers contained within the act, an intelligence agency or other authorised body will submit a warrant to the Secretary of State, who then scrutinises and approves (if appropriate) the warrant. This is then passed on to a Judicial Commissioner – a newly created role for senior judges – who will then review the Secretary of State's decision, before the warrant is approved.

This process establishes both political and legal oversight but lacks clarity as to the level of detail and scrutiny the Judicial Commissioners will have. A concern remains that this power is framed along the lines of a judicial review that is limited to scrutinising the process undertaken by the Secretary of State, not the content of the warrant.

WHAT THE IP ACT MEANS FOR LIBRARIES

Libraries offer a great deal of services to their users that involves the Internet. This includes public Wi-Fi, public access terminals and the retention of both user and staff data on the library systems, many of which may be dependent on 3rd party storage, software or hardware.

The Investigatory Powers Act's definition of telecommunication operator is incredibly broad:

> A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system, which is (wholly or in part) in or controlled from the UK.

Source: Investigatory Powers Act, National Security Notices Draft Code of Practice

This broadness and refusal to grant exceptions to public bodies or operators with a small user base means that libraries that offer online services as outlined above cannot be exempted from powers and obligations contained within the IP Act. Depending on the organisation and management of different libraries, the obligations contained within the bill may fall on:

- **Individual libraries**
- **Local councils**
- **Educational institutions i.e. schools and universities**
- **3rd parties who provide the online services to the libraries and/or councils including the providers of the public Wi-Fi networks.**
- **Private institutions i.e. law firms governing law libraries**

This is the basis for this document; without guidance and support, libraries may be unaware of the increased obligations passed onto them by this piece of legislation, alongside the tools and practices that could help themselves and their users protect their personal data.

A NOTE ON THE IP ACT AND ENCRYPTION

End-to-end encryption ensures that when you send a message no one except the intended recipient can access and read what you have written. If the data is intercepted by an unknown 3rd party they will not be able to read the message as it will appear to them in a scrambled and illegible format. As well as unknown 3rd parties, this also includes the service provider, including WhatsApp, Signal or Facebook. However, following attacks in London and Manchester the then-Home Secretary, Amber Rudd and Prime Minister, Theresa May have called for the capability to undermine the provision of end-to-end encryption due to the fact that intelligence agencies cannot access and decrypt messages being sent.

While there is little detail as to how this will be deployed or implemented, technical capability notices as set out in the IP Act, are the aspect of the act that may be used to justify this sweeping political manipulation of a process that ensures a high level of privacy and security.

THREAT MODELLING

Category: Security / Privacy

This chapter is an amended version of the guide created by the Electronic Frontier Foundation as part of the Surveillance Self-Defense resource.

There is no single solution for keeping yourself safe online. Digital security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats. To become more secure, you must determine what you need to protect, and whom you need to protect it from. Threats can change depending on where you're located, what you're doing, and whom you're working with. Therefore, in order to determine what solutions will be best for you, you should conduct a threat modelling assessment.

When conducting an assessment, there are five main questions you should ask yourself:

1. **What do you want to protect?**
2. **Who do you want to protect it from?**
3. **How likely is it that you will need to protect it?**
4. **How bad are the consequences if you fail?**
5. **How much trouble are you willing to go through in order to try to prevent those?**

When we talk about the first question, we often refer to assets, or the things that you are trying to protect. When we are talking about digital security, the assets in question are usually information and data. For example, your emails, borrowing details, contact lists, instant messages, and files are all assets. Your devices such as computers, tablets or mobile phones are also assets.

The identification of assets in the context of libraries is of added importance due to the fact that libraries will hold personal data of both users and staff members on their systems. In this manner, ensuring libraries take steps to ensure they store this data securely is a central responsibility that cannot be ignored.

Activity One: Write down a list of assets (data & devices) that you keep, where they are kept, who has access to them, and what stops others from accessing them.

In order to answer the second question, "Who do you want to protect it from," it's important to understand who might want to target you or your information, or who is your adversary. An adversary is any person or entity that poses a threat against an asset or assets. Examples of potential adversaries are your boss, your government, or a hacker on a public network.

Activity Two: Make a list of who might want to get hold of your data or communications. It might be an individual, a government agency, or a corporation.

There are numerous ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data. An adversary could also disable your access to your own data.

The motives of adversaries differ widely, as do their attacks. A government trying to prevent the spread of a video showing police violence may be content to simply delete or reduce the availability of that video, whereas a political opponent may wish to gain access to secret content and publish it without you knowing.

Activity Three: Write down what your adversary might want to do with your private data.

The capability of your attacker is also an important thing to think about. For example, your mobile phone provider has access to all of your phone records and therefore has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted

communications. Your government might have stronger capabilities.

CONSIDERING RISK

A final thing to consider is risk. Risk is the likelihood that a particular threat against a particular asset will actually occur, and goes hand-in-hand with capability. While your mobile phone provider has the capability to access all of your data, the risk of them posting your private data online to harm your reputation is low.

It's important to distinguish between threats and risks. While a threat is a bad thing that could happen, risk is the likelihood that the threat will occur. For instance, there's a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in UK (where they are not).

Being Specific and Realistic

The importance of a threat model lies in its ability for you to identify issues specific to your unique situation. This can mean your professional role in your library or activities undertaken in your personal life. In this manner it encourages you to be both specific and realistic in creating your threat model.

Being Specific – Breaking down your assets as much as possible enables you to identify practical steps to address individual vulnerabilities and potentially different adversaries. For example, breaking down borrower details (address, payment details, lending history) may reveal different adversaries who may seek access and different ways each piece of information can be secured.

Being Realistic – Threat modelling enables us to look for adversaries who can be realistically expected to seek access to our assets. While it may be impossible to accurately predict everyone who may seek access, this approach allows us to model our response to genuine threats and risks, while avoiding the worries of modelling a response based on a powerful, though unlikely adversary, which may lead you to utilise

tools you and your users may not need.

Conducting a risk analysis is a personal and unique process; not everyone has the same priorities or views threats in the same way. Many people find certain threats unacceptable no matter what the risk, because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view them as a problem.

Throughout this toolkit, this assessment will help you decide what changes you may want to make to your usage and deployment of online systems and services. It is very likely that you will not need to implement everything suggested in this document – this assessment will hopefully help make that choice more straightforward.

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes for library users
- Users to develop unique assessment to identify which tools and approaches best suit their threat model
- Develop bespoke training for local businesses with a focus on cybersecurity and protecting data against 3rd parties
- Encourage and support library staff and volunteers to develop a threat model based on their specific role within the library

A TEMPLATE THREAT MODEL

See below for an example portion of a Threat Model to guide you through creating your own. Thank you to Rebecca Oliva, head librarian at the Scottish Poetry Library for developing this example model.

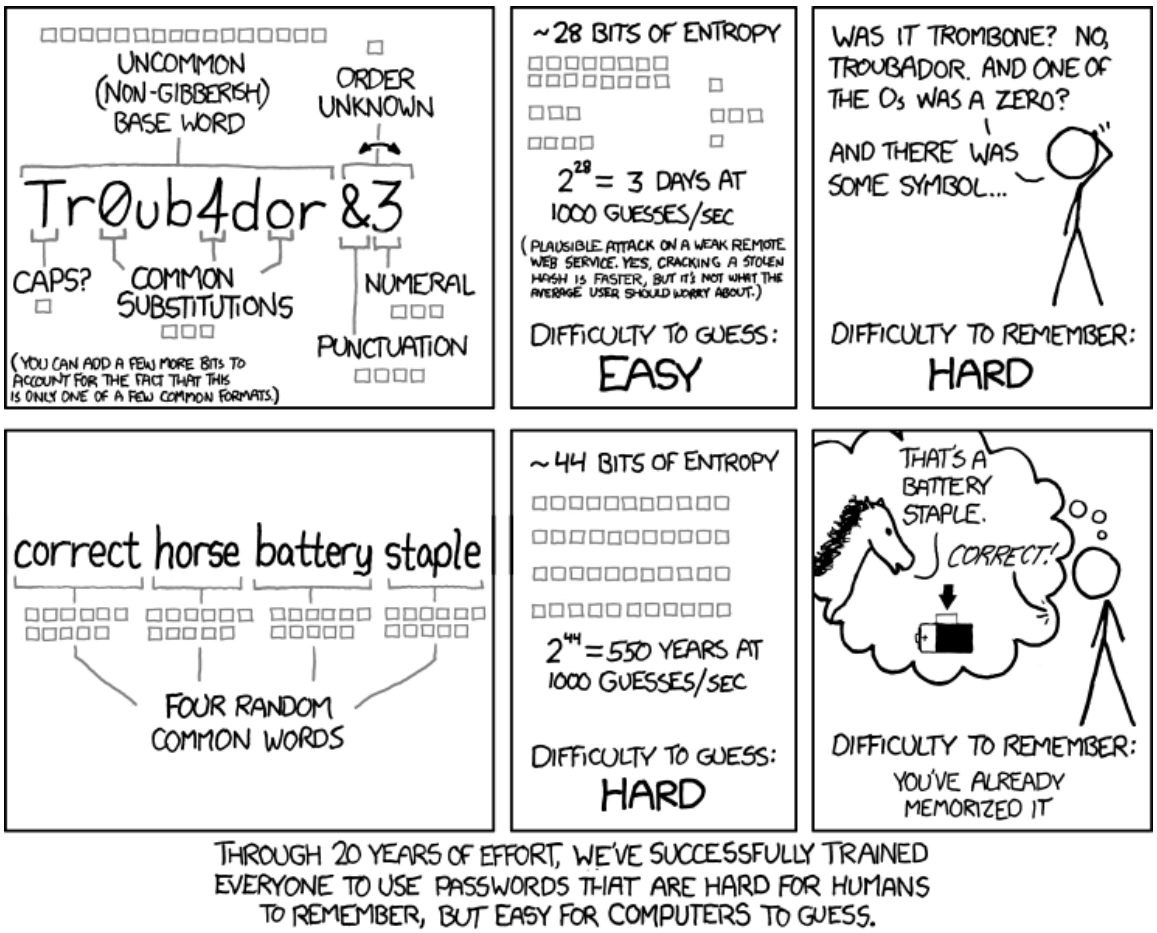
Note: It is not recommended that you take this example as your own. Threat models enable us to give shape to our own specific situation, and any vulnerabilities contained within. As a result, the steps contained below are only relevant to a very specific situation. Nor is this example an exhaustive example of a threat model, other threats and potential remedies may exist for these identified vulnerabilities that have been omitted for space as opposed to their relevance or significance.

What do you want to protect?	Who do you want to protect it from?	How likely is it that you will need to protect it?	How bad are the consequences if you fail?	How much trouble are you willing to go through in order to try to prevent those?	Recommended Practices
Web browsing data from public Wi-Fi	• Private companies • Government agencies • Other users & staff members	• Very likely chance of corporate tracking, malicious 3rd parties and other users. • Government agencies are less likely	• Trust in institution may be damaged especially with vulnerable users • High costs in relation to data protection responsibilities	• In-depth debate with Wi-Fi providers are necessary • Expertise regarding technical support i.e. VPNs	• Allow users to connect via VPNs • Allow users to search the web via Tor • Utilise WPA2 security on Wi-Fi network
Catalogue searches on public devices	• Other borrowers & staff members • Government agencies • Private companies	• Very likely due to potential value of data generated from searches.	• Vulnerable groups avoid using public devices to search catalogue	• Offer alternate ways to search catalogue but will depend on user awareness and comfort.	• Allow catalogue searches via either Tor Browser or private browsing modes
Borrower loan history	• Government agencies including police forces • Corporations • Malicious 3rd parties such as hackers or cyber-fraudsters	• Government agencies may seek in relation to serious crime or terror investigations or part of Prevent strategy. • Protect it from corporate surveillance and 3rd parties	• Borrowers are likely to trust the library less and avoid using resources we have to offer • Vulnerable groups may avoid using the library if browsing history can be accessed by 3rd parties	• The trouble may be considerable if we are required to change LMS or limit functionality for users who want to browse their own history.	• Borrower loan history can be automatically deleted; but this must be balanced with the likelihood that borrowers may want to browse their history. • LMS can allow borrowers to delete their own loan history
Cloud Storage	• Cloud storage providers • Unknown 3rd parties including hackers & corporate partners • Government agencies	• Very likely due to dependence of 3rd party tools and potential value of data shared and stored	• As well as potential data protection breaches, you risk losing the trust of borrowers by asking them to trust a third party.	• We would need to ensure any cloud services we choose retain baseline functionality to ensure this does not adversely affect other library services.	• Use cloud services that are encrypted and protect data during transfer • Use services that are zero-knowledge • Use strong passphrases to access cloud services

~~PASSWORDS~~ PASSPHRASES

Category: Security

Weak passwords are the equivalent of giving away the keys to the kingdom. While it is common for people to reuse passwords across platforms and devices, a password may be only as secure as the least secure service where it's been used. So if a password is cracked, it may give the 3rd party access to more than one platform alone. Weak passwords also undermine the security built in to digital platforms. If you use a more secure online tool, but still use weak passwords (or passwords used for other devices) the added security of the tool would amount to nothing as the weak password would be relatively easy to break by 3rd parties.



xkcd cartoon on password strength

Password Top Tips:

1. **Think of passphrases as opposed to passwords**
2. **NEVER reuse passwords across different accounts, platforms or devices**
3. **Uses random words in your passphrase that have no connection to you personally**

There are a number of ways that passphrases can be strengthened:

PASSPHRASES

It is best to think of a passphrase as opposed to a password as they are longer in length & harder to crack through brute force attacks (a trial and error method to decode encrypted data such as passwords).

Key things to remember when creating your passphrase:

- **Known only to you**
- **Long enough to be secure**
- **Hard to guess, even by someone who knows you well**
- **Easy for you to remember**
- **Easy for you to type accurately**

source: The Diceware Passphrase

DICEWARE

This is an easy way to create a strong yet easy to remember passphrase. Diceware™ is a method for picking passphrases that uses dice to select words at random from a special list of random words of varying lengths.

Each word in the list is preceded by five-digit number. All the digits are between one and six, allowing you to use the outcomes of your dice rolls to select a word from the list.

How to:

1. **Download the complete word list**
2. **Choose how long you want your passphrase - 6 words is recommended**
3. **Roll the dice five times per word (i.e. 6-word passphrase requires 30 rolls)**
4. **Write down the result and group in 5s i.e. 12321 46655 51653 65624 43122 36454**
5. **Use the word list to assign each code to the random word assigned to it: 12321 46655 51653 65624 43122 36454 becomes armadillo refining retrace virus oval maimed**
6. **This is your random but memorable passphrase**

Please note: Some platforms require you to add numbers and/or punctuation marks. These can be added to the passphrase generated by the Diceware method.

PASSWORD MANAGERS

Password managers are encrypted software applications that enable the safe and secure storage of a large number of passphrases. Stored in this manner, users can depend on strong passphrases, without necessarily having to remember them all (although that is not a bad thing). All you need to remember is one strong master passphrase to access the manager.

Password Managers can either store data on encrypted parts of your web browser, on web apps (for mobile devices) or locally on your device.

Recommended managers:

- **LastPass:** www.lastpass.com
- **1Password:** www.1password.com
- **KeePassX:** www.keepassx.org

STORING PASSPHRASES

If we are using different passphrases for different platforms or tools, we will end up with a large number of passphrases we need to remember. This is necessary but complex. Password Managers, as outlined above, limit the number you need to remember – only the master passphrase for the manager would need to be remembered – but what can we do to store and remember passwords beyond that?

Should we write down passphrases? This is a highly-contested issue but again relates to your threat model. Looking at the assets you hold and any potential adversary you have identified, is it likely they would try to access your home or steal your wallet? If the answer is no to these questions, it could be safe for your write down passphrases.

Technologist, Bruce Schneier stated on his blog: "We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet."

Things to think about:

- Store all passwords securely but not in the same place
- Do not have passphrases on display, especially if you have a lot of visitors or are interviewed on film from home – this is an example of what not to do
- If possible, when writing down your passphrases do not identify which platform or service they relate to.
- You can buy 'password notebooks' but this puts all passphrases in one easily identifiable place, and so should be avoided.

TWO-FACTOR AUTHENTICATION (2FA)

2FA strengthens the security of encrypted systems by requiring unique login credentials to be generated by another device besides the one you are looking to login in from, including either a smart phone or tablet. As well as asking for your passphrase, the system will then send an SMS or voice call to a registered device or through an authorisation app, which will generate a unique code you will be required to input to access your account.

The benefit of this is that even if a 3rd party gets access to your pass-phrase they would require to have access to the registered device to access the unique code.

A number of platforms use 2FA including Gmail, Facebook, Microsoft and Twitter. A number of these platforms will frame it as an optional extra. Look at the privacy or security settings to see whether it is an option for you to use. It is sometimes called **Login Approvals**.

Note: If you believe your secondary device (phone or tablet) may be insecure, you may want to look at using authorisation apps or Yubikeys (below). If you device has been accessed, SMS messages containing your unique code could be intercepted.

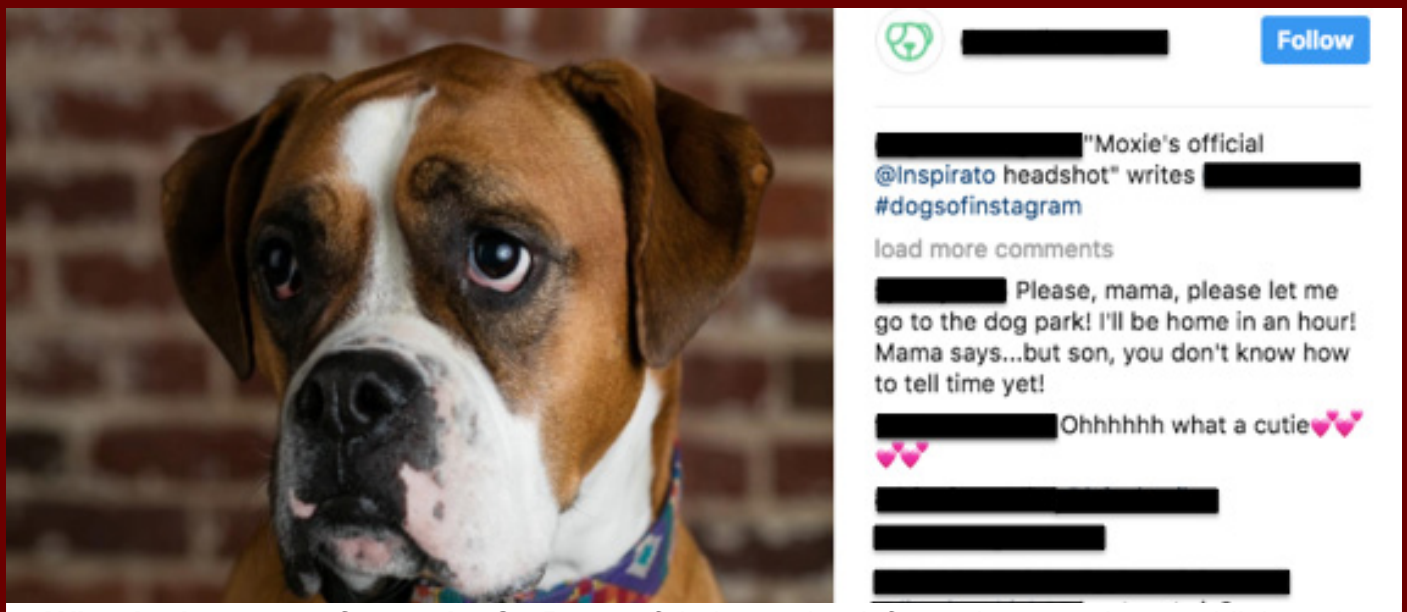
YUBIKEYS

Yubikeys are pieces of hardware that you plug into your device's USB port that offers two-factor authentication. Once it is plugged in, when you log in to a service or platform that supports Yubikey authentication you press the button on the key and it will generate and share with the device a one-time code that will enable you to access your account or service.

For more information: www.yubico.com

THINGS TO REMEMBER

Security questions are a simple way for people to gain access to accounts if they have forgotten their log-in details. However, they are easily bypassed when a third party can obtain the answers. For example, if your security question is what was the name of your first pet? and you post photographs on your Instagram account with the caption 'remembering Fido on the 10 year anniversary of his passing', it is not difficult for a 3rd party to bluff the system.



What is the name of your dog? *- Be careful about what information you share publicly as it may be used to uncover your password or answers to your security questions*

It is recommended to create fake answers to these questions that cannot be unearthed by a simple web search. Or alternatively, use the answer to security questions as an excuse to create another strong passphrase – remember your answer to these questions do not need to be true!

PASSPHRASES FOR LIBRARY SERVICES

A number of library services require users to set up an online account. Libraries should support users to create and use strong passphrases:

- Library systems should not place an upper end threshold on the number of characters in a passphrase – the longer a passphrase, the more secure it is
- Require users to change their passphrases when first given access to library services
- If using pin codes as opposed to passphrases these should also not be limited to a specific number of digits and not connected to personally identifiable information i.e. birthdays or postcodes

SECURING PASSPHRASES IN LIBRARIES

Encouraging users to use strong passphrases would be meaningless if they are stored on the library's database in plain text, meaning that an adversary can bypass the users and access the database and capture all of the passphrases stored on the system. Ensuring the passphrases

are stored securely is vital and at the centre of the library's responsibilities to their users. There are a number of ways the library can ensure they store passphrases securely. These issues will be important when you look at which Library Management System to deploy throughout your service.

Hashing - This scrambles the passphrase into an illegible collection of characters using a key known only to the system itself.

Salting & Peppering - These add a unique, random string of characters before the passphrase (salt) & after it (pepper) before it is hashed. Some sites use the same 'salt' for each passphrase, but unique salts can be used to strengthen this process.

Algorithms - The hash value is derived from the combination of both the passphrase and the key, using a set algorithm. Secure Hash Algorithm 2 (SHA-2) "is a family of hash functions that produce longer hash values." While there are newer algorithms available, SHA-2 remains the basic standard that should be used to protect the security of passphrases held on the library system.

Source: The Guardian

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users:
  - Training on developing strong passphrases
  - Installation of Password Managers
  - Training on 2-Factor Authorisation
- Ensure passphrases are held securely on your library system
- Develop bespoke training for local businesses with a focus on cyber-security and protecting data against hackers
- Install Password Managers on all staff computers and offer training to ensure staff members can deploy them effectively
- Encourage users, when opening accounts for library services, social media, email or other online services, in libraries to use strong passphrases
- Have a Diceware set (dice, word list and note paper) in your library that users can use to create strong passphrases

CORPORATE SURVEILLANCE & ADBLOCKERS

Category: Security / Privacy

The digital economy is built on the collection, storage and sale of personal data through our interaction with different websites. Monitoring our online behaviour enables sites to be tailored to our needs and search history, while giving them an intimate insight into our private transactions and preferences.

With expanded state surveillance these datasets may also be co-opted by the state, without our knowledge, to develop in-depth profiles and supplement further surveillance powers. As demonstrated by the TalkTalk hack, the security of the data held by private sector organisations cannot be guaranteed. When this data contains sensitive information, it is vital that users are able to choose what they share and trust known 3rd parties to hold their data securely.

TARGETING OUR DATA

Using advanced data analytics, the US superstore, Target is able to predict when customers were pregnant by the items they bought including unscented lotions and vitamin supplements. This was demonstrated in Minneapolis where a father demanded to know why his high-school aged daughter was receiving coupons for baby clothes and nappies, only to find out later that she was in fact pregnant. Target was able to figure out she was pregnant before she had told her father solely from the data her purchases generated.

ADBLOCKERS

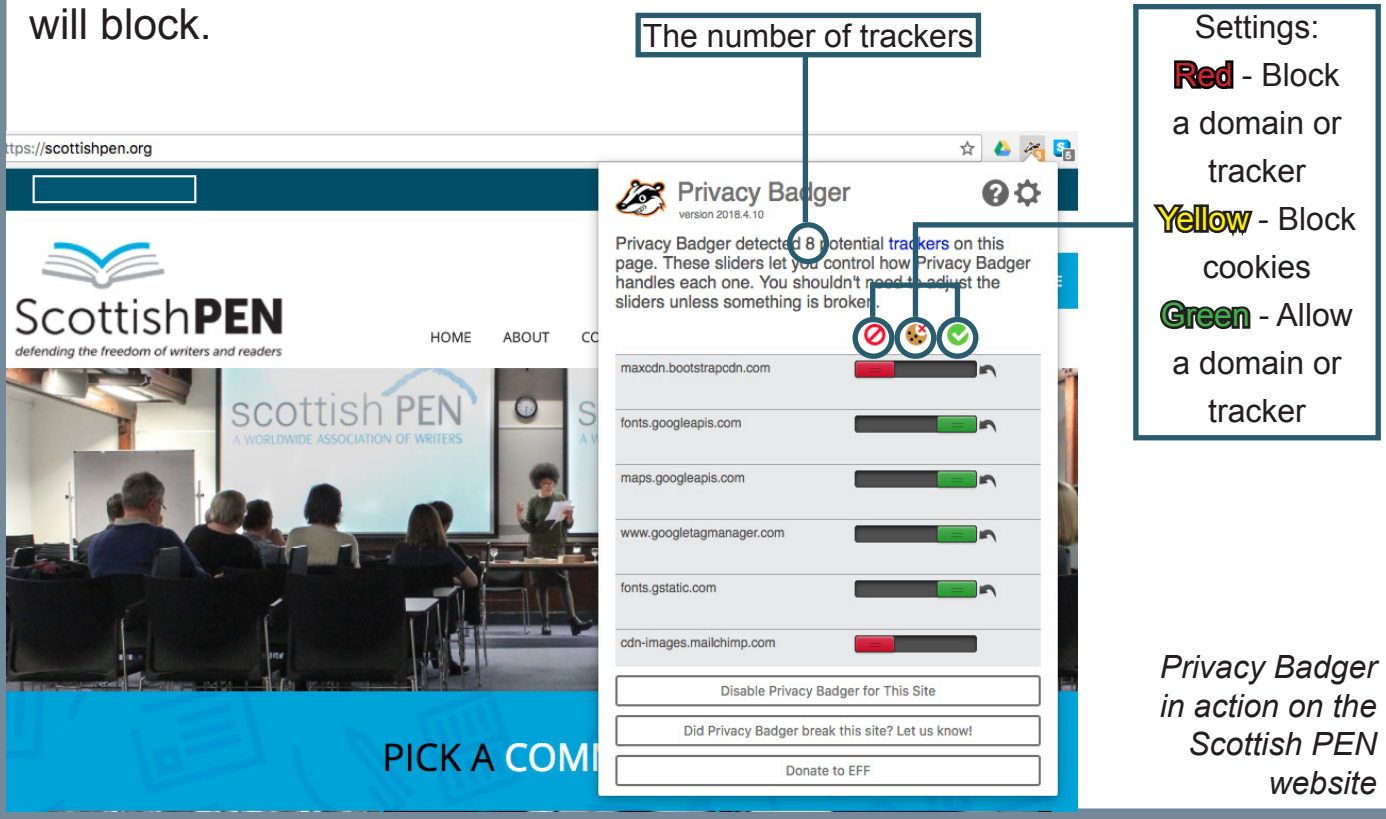
These add-ons for web browsers will block trackers and adverts, which monitor your usage and can harvest information about you.

Recommended AdBlockers are:

- **Privacy Badger:** www.eff.org/privacybadger
- **UBlock Origin:** Chrome | FireFox

Many blockers, including Privacy Badger are able to give you an itemised breakdown of which trackers are monitoring you at any given time, allowing you to choose which would you like to disable and which, according to your threat model, you are happy to leave running. As many media players track usage, the deployment of a blocker may result in players not functioning correctly. Accessing the adblocker in your web browser, you can manually turn these on to enable the media player to function properly, while still blocking others.

Please note: It is important to remember that a number of websites are able to monitor whether you are utilising an adblocker and can restrict access to their content as a result. As many sites use advertisements as a source of income, it is up to you to decide which sites you are willing to allow to track you as part of their business model and which you will block.



Privacy Badger in action on the Scottish PEN website

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users
  - Installation of adblockers
  - Training on corporate surveillance & trackers
- Develop bespoke training for local businesses with a focus on cyber-security and protecting data against 3rd parties
- Encourage businesses to utilise a considered approach to deploying ads and trackers on their online services and platforms
- Work with the IT department and management to undertake an internal audit to ensure all trackers and ads used on online library services are necessary for service provision, transparently deployed and keep data collection to a minimum
- Install Privacy Badger or UBlock Origin on all library computer systems (staff and user terminals)

WEB BROWSING SAFETY

Category: Security / Privacy

Alongside adblockers, there are a number of steps you can take to protect your web browsing that will secure both your private data and your system or device.

SEARCH ENGINE CHOICE

Search Leakage - Browsers collect and share users' data and search terms with the sites searched. There are a number of steps that can be taken to disrupt this.

DuckDuckGo is a search engine that does not collect data or track users, which means it cannot share information with 3rd parties. DuckDuckGo does not log or store your IP address or user agent (details of the technical data about the device and software you use to access the Internet) and the default setting is to not store cookies (personally identifiable data that are retained for sites to 'remember' aspects of users' behaviour).

To set DuckDuckGo as your default Search Engine:
www.duckduckgo.com/install

DuckDuckGo Privacy Essentials (browser plug-in): Chrome | FireFox | Opera | Safari

DuckDuckGo Mobile App: Android | iPhone

Qwant is a French search engine, which like DuckDuckGo doesn't collect data, use cookies or track users. By disassociating users with their IP Address, search queries on Qwant are anonymised. As well as promoting private web searches, Qwant seeks to be transparent as to how

it uses the data it does hold (i.e. through creating a Qwant account) by establishing the role of Data Protection Officer who keeps a register of all processes undertaken with collected data that can be shared to any user upon request.

Access Qwant here: www.qwant.com
Qwant Mobile: Android | iPhone

ADD-ONS & SCRIPTS

Browser plug-ins and add-ons such as Flash, RealPlayer, Quicktime, and others can be manipulated into revealing your IP address and it is highly recommended that you remove plug-ins to ensure your personal data is protected.

One way to control the scripts that are running on your browser is to install the **NoScript** FireFox extension which provides extra protection for FireFox, Seamonkey and other Mozilla-based browsers: this free, open source add-on allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice (e.g. your online bank).

Download: www.noscript.net

BROWSERS

Each web browser collects and shares personal data differently to provide its own specific service. The most private is Tor Browser, which accesses the Internet through the Tor network (see later chapter), but Google Chrome is one of the most secure, due to its protections against malware. Of course the trade-off is consenting to Google's collection of personal data – depending on your threat model, this trade-off may or may not be acceptable.

Browsing Modes – Many web browsers have a mode of browsing that is far more private and can be invaluable within a library context, where many different users use the same device. Google Chrome's Incognito mode or Mozilla FireFox's Private Browsing mode both allow users to

browse the web without their browsing history being stored on the device. It also ensures that when you close the window all cookies are deleted, which would prevent other users potentially accessing data or information generated by users before them who have forgotten to log out. These browsing modes may not stop information being collected by the websites visited or by the Internet Service Providers.

In FireFox you can change the settings so the default behaviour on the browser is similar to that of the Private Browsing mode, meaning that the browser will not remember or track your behaviour online

To do this:

1. **Click Preferences in the browser menu**
2. **Click the Privacy tab**
3. **Under the History section change the setting to FireFox will never remember history**
4. **You will be asked to restart the browser**

Note: In the same Privacy tab, you can manage your **Do Not Track** Settings under the tracking section.

BRAVE

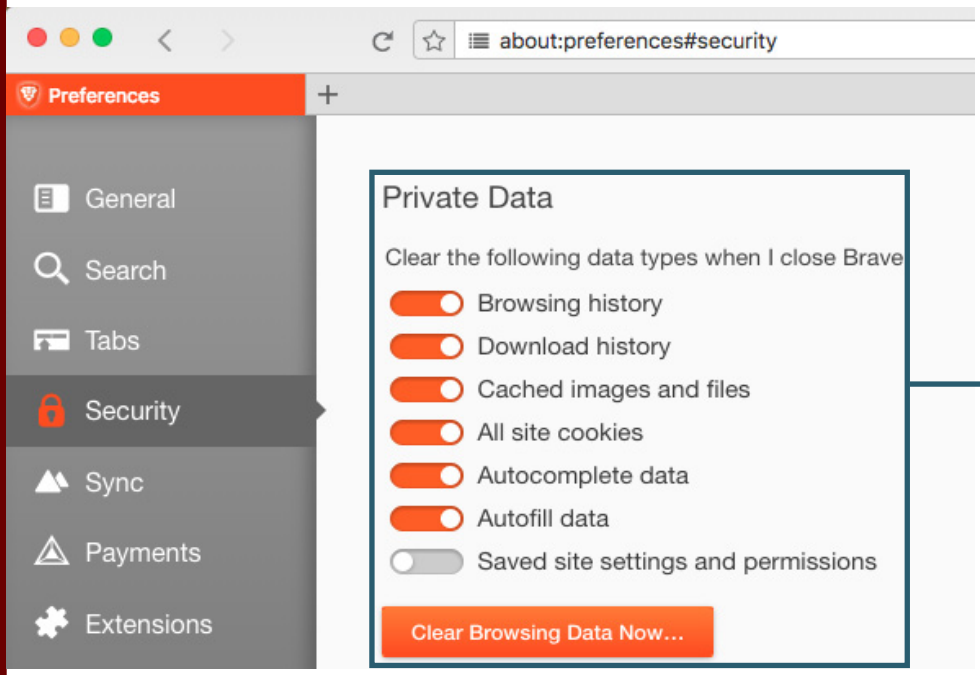
This is a new open-source web browser based on Google Chrome that blocks ads and trackers, including cookies, by default and also has HTTPS Everywhere pre-installed to ensure that where possible your communication with websites is encrypted (see later chapter for more information). You can also turn on pre-installed password managers including LastPass (see earlier chapter).

Download: www.brave.com/download

You can configure the browser to delete specific types of private data including browsing and download history when you close the browser.

To do this:

1. **Open Brave**
2. **Click on the three vertical dots on the right hand side of the browser**
3. **Select preferences or settings**
4. **On the left, select the Security tab**
5. **Under the heading Private Data, you can toggle different data types to be cleared when you close Brave**



Brave's settings that allow you to control what data Brave will clear when the browser is closed

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users
  - Installation of secure web browser, search engine and tools to limit access to scripts and plug-ins
- Develop bespoke training for local businesses with a focus on cyber-security and protecting data against 3rd parties
- Install where possible:
  - DuckDuckGo as the default search engine
  - NoScript (if using Mozilla FireFox)
- If you offer Mozilla FireFox as a browser your staff or patrons can use on terminals within the library, it is recommended to change the browser's default behaviour to that of the Private Browsing mode.
- Develop guides or posters demonstrating the differences between different web browsers and search engines to ensure users can make a choice as to which service to use

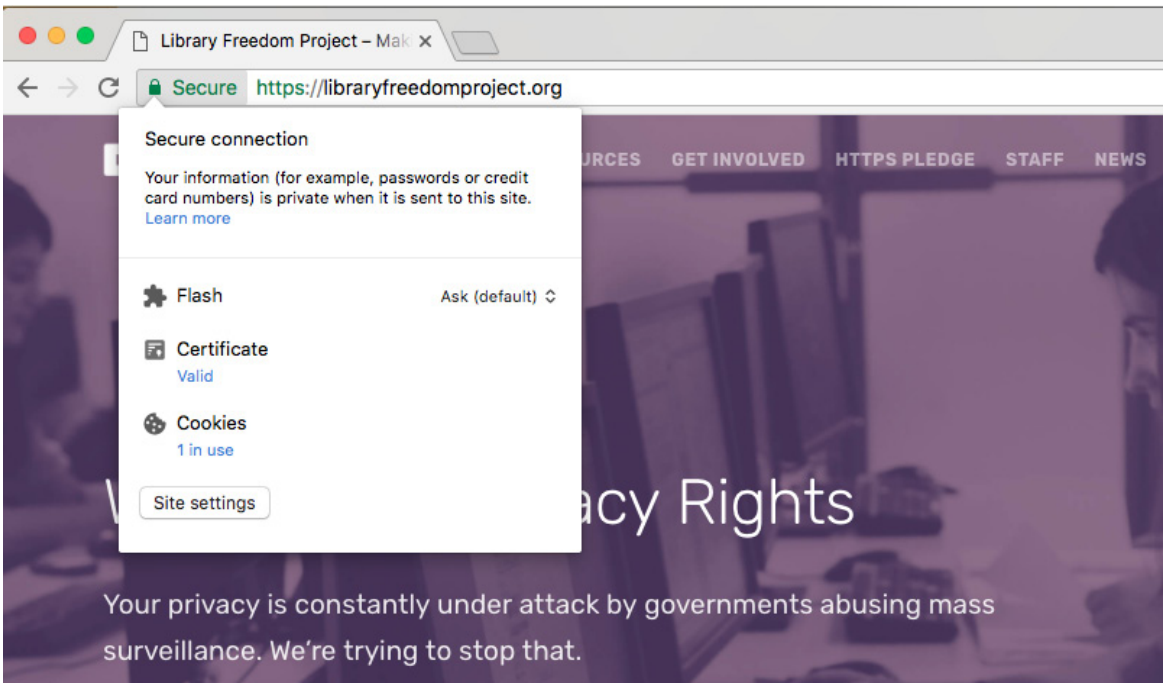
HTTPS

Category: Security / Privacy

Hypertext Transfer Protocol (HTTP) is an application protocol that is the foundation of data communication for the World Wide Web. It defines how messages are formatted and transmitted.

In the words of the Electronic Frontier Foundation (EFF) “As revealed by the Snowden NSA surveillance documents, HTTP traffic can also be collected and searched by government agencies without notice to users or webmasters.”

HTTPS add secure to the protocol, ensuring all communications between your browser and the web are encrypted.



Using Google Chrome the green padlock and ‘secure’ will be visible in the search URL in your browser when visiting a site that supports HTTPS

HTTPS EVERYWHERE

Created by the EFF and The Tor Project, HTTPS Everywhere is a Fire-Fox, Chrome and Opera extension that encrypts your communications with a number of major websites, making your browsing more secure. While many websites depend on the unencrypted HTTP protocol, this add-on rewrites requests to websites to ensure they use the encrypted HTTPS if they support it. So in other words, with HTTPS Everywhere installed, when a website has enabled HTTPS, this add-on will make sure your communications with the website is undertaken via the encrypted channel as default.

Using HTTPS Everywhere will also allow you to block all unencrypted requests to ensure that you are only able to access sites that utilise HTTPS encryption.

Click here to read an EFF blog about how HTTPS can support and protect libraries and their users.

Compatible Platforms: Chrome | FireFox | FireFox (Android) | Opera
Download: www.eff.org/https-everywhere

SECURING WEBSITES & SERVICES

For those hosting websites it is recommended that you deploy websites using at least TLS (Transport Layer Security) 1.1 so data shared by the site and the Internet is encrypted. There are a number of online services to support you in this request, which will walk you through the installation process, as well as providing you with the digital certificates necessary to enable HTTPS (SSL/TLS) for websites.

Let's Encrypt is a Certificate Authority that issues certificates free of charge and **CertBot** is a tool developed by the EFF to facilitate the provision of Let's Encrypt certificates.

To get started: www.letsencrypt.org

HTTPS & GOOGLE RANKING

For added incentive for sites to adopt HTTPS encryption, Google will prioritise search results based on whether the site uses encryption or not, and beginning in July 2018 with the release of Chrome 68, Google Chrome will mark all HTTP sites as “not secure”.

MAKING THE MOVE

The Digital Public Library of America has been working to move everything over to HTTPS and the White House Office of Management and Budget (OMB) issued a directive calling for all “publicly accessible Federal websites and web services only provide service through a secure HTTPS connection.” If we can migrate library websites to HTTPS, we can ensure that the information shared by both library staff and users is done so in a secure manner that protects personal data.

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users
  - Training on importance of HTTPS & encryption
  - Installation of HTTPS Everywhere plug-in
- Develop bespoke training for local businesses to migrate their online services to using HTTPS
  - Focus both on web browsing and web servers
- Install HTTPS Everywhere on all staff & user terminals
- Migrate all library websites to HTTPS - This will require a higher level of technical literacy but your website hosts or developers in your area should be able to support you

VPNs

Category: Security / Privacy

VPNs or **Virtual Private Networks** enable you to create a secure and private network within a public or shared network. There are many reasons why users may choose to use a VPN – employers can use a VPN to set up an intranet and a VPN can help users in different parts of the world access online content that uses IP Addresses to restrict access based on geographic locations – but VPNs can offer users the ability to secure their browsing history and Internet usage from 3rd parties and their Internet Service Provider.

A large number of VPNs have proliferated, each with their own benefits or weaknesses. Due to the sheer number of VPNs on offer we will not suggest one in this toolkit, but here are a few guidelines and issues that may relate to your work in libraries or in your personal life.

Here is a good guide to different VPNs on the market.

Free VPNs are available on the market alongside paid services that give you the opportunity to pay for a yearly service or via monthly payments. But free VPNs may sell your data they collect through their service to monetise the service.

If you are looking for a VPN to avoid pervasive surveillance or data collection, we would recommend avoiding:

- Services that are based in jurisdictions with overly restrictive surveillance and data collection legislation with disproportionate powers and limited protections, such as the UK following the passage of the Investigatory Powers Act;
- Services that maintain and store logs of all activity that is undertaken when using the VPN – this log could give 3rd parties access to your

online activities, undermining your online privacy.

VPNs that reduce your privacy

Because there are a large number of VPN providers available to both libraries and their patrons, your choice of service is important. If you choose a VPN that stores logs, monitors your usage or sells your browsing data to 3rd parties (most times without your consent or knowledge) this may, in fact, be more invasive than your Internet Service Provider, and as a result undermines your privacy further as you lose control over your data and how it is used by others.

Benefits of Using a VPN

With the Investigatory Powers Act being able to pass on obligations to telecommunications providers to store Internet Connection Records, as well as other 3rd parties being able to monitor, store and share your browsing history, a VPN is a powerful and easy-to-use tool to ensure users can maintain control over their browsing history.

VPNs can also help users protect their digital security. Using a VPN within a public Wi-Fi network can help protect against malicious 3rd parties from both within and outside the Wi-Fi network.

ARE WE WHAT WE BROWSE?

Jon Penney of the Oxford Internet Institute discovered in his 2016 study that, following the Snowden revelations, user traffic on Wikipedia to pages related to over 48 'terrorism-related terms' (as designated by the Department of Homeland Security) dropped by 20%. Alex Marthews and Catherine E. Tucker measured a similar drop in Google search terms in 41 countries related to terms that could get them in trouble with the US government.

Compatibility Issues in Libraries

Using VPNs in certain library Wi-Fi networks may be problematic as a number of networks may refuse the VPN to connect – effectively mak-

ing the VPN user unable to access the Internet until they disconnect from the VPN. As a result, users will not be able to make the choice to protect their online privacy through a VPN, which may result in the user either choosing to browse the web without the protection of a VPN or avoiding the library all together.

It is recommended that library staff work with their IT departments and local councils (if applicable) to address this issue to ensure the digital infrastructure can fully enable their users to make active choices to protect both their online privacy and security.

IDEAS FOR YOUR LIBRARY:

- Ensure public Wi-Fi network is configured to enable users to use a VPN on their electronic devices when using the network. This should include both laptops and mobile devices
- VPNs can be installed on the routers for public access computers in your library to increase the privacy of people using the Internet
- While it may be problematic for libraries to recommend specific VPN services, libraries could help users understand how a VPN works, identify the limitations and what questions they should ask of providers so they can make an informed choice if they wish to start using one

DEVICE ENCRYPTION

Category: Security / Privacy

Encrypting a device ensures the data held on the device is protected against a range of adversaries who have physical access to your device. As outlined by Micah Lee in The Intercept: **“disk encryption is only useful against attackers that have physical access to your computer. It doesn’t make your computer any harder to attack over a network”**.

As outlined in the later chapter on physical security, device encryption is vital to ensure devices can remain secure against physical attacks or interference.

Things to remember

- If you have a large number of files on your device, this process can take a long time (can be over 8 hours), so make sure your device is plugged in during the encryption process.
- It is recommended to back up all sensitive and important files before encrypting the device.
- Encryption is only as strong as the passcode or passphrase. Using device encryption will mean that the passcode you use to unlock your device will also decrypt your hard drive, so make sure you use a strong passphrase (see previous chapter).

Encryption processes depend on operating systems.

MAC OS

Apple computers have a built in process by which to encrypt the device. It is called **FileVault**.

To turn on FileVault:

1. **Open System Preferences**
2. **Click on Security & Privacy**
3. **Click on the 2nd tab at the top, FileVault**
4. **Ensure your device is plugged in, will all important files on your computer backed up**
5. **Click Turn on FileVault. This will encrypt the computer's hard drive**

Turning on FileVault will generate a recovery key – keep this code safe as it would be the only way to decrypt your device if you forget your passcode.

WINDOWS

Window's in-house encryption process is BitLocker, but is only available for the Ultimate and Enterprise editions of Windows Vista and Windows 7, and the Enterprise and Pro editions of Windows 8, 8.1 and 10, but not the Home editions. You can check whether you have BitLocker on your device by clicking on Windows Explorer and right-clicking on the C Drive. If you have BitLocker it will say 'turn on BitLocker' or 'Manage BitLocker' (this means that your device is already encrypted).

If you have BitLocker here is how you turn it on:

This step-by-step comes courtesy of Micah Lee's device encryption guide published on The Intercept.

1. Open Windows Explorer, right-click on the C Drive and select Turn on Bitlocker
2. You will be asked to back-up your recovery key – it is recommended to save it on another drive or print it out – if you save it to your Window Account, Windows could be compelled to hand over all data it holds (including your recovery key) to law enforcement agencies.
3. After a few more steps, your computer will reboot. After rebooting, your disk will start encrypting – you can continue working on your device while it encrypts in the background.

4. The next step is to set up a pin.
5. Click Start and type “gpedit.msc” and press enter to open the Local Group Policy Editor.
6. In the pane to the left, navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives.
7. In the pane to the right, double-click on Require additional authentication at startup. Change it from “Not Configured” to “Enabled,” and click OK.
8. Close the Local Group Policy Editor.
9. Open Windows Explorer again and right-click on C Drive. Click Manage BitLocker
10. In the BitLocker Drive Encryption page, click “Change how drive is unlocked at startup.” Now you can choose to either require a PIN while starting up, or requiring that you insert a USB flash drive - A PIN is probably better because you don’t need to remember a USB flash drive wherever you go and a passcode is easy to memorise.
11. The PIN will need to be between 4 and 20 characters long – the longer it is the more secure it is. As identified in the earlier chapter about passphrases, ensure the PIN is randomly generated, not related to your personally i.e. address, dates of birth. Click Set PIN
12. Reboot the computer again – you should be asked to type in your PIN.
13. If you device has a number of different user accounts, ensure all of them utilise strong passphrases.

Please Note: As one of the largest technology companies, Microsoft has publicly stated that it will comply with all lawful requests from law enforcement and intelligence agencies. The Snowden revelation in 2013 revealed that Microsoft had collaborated with the NSA to enable the interception of users’ data.

Other Available Services

TrueCrypt was a firm favourite of those who sought open-source and independent encryption services for devices or folders, but in 2014 the software stopped being updated, so it remains unclear whether the system remains secure against new threats that may have arisen following the end of development.

VeraCrypt is an expansion and evolution of TrueCrypt, which is being updated and audited on a regular basis.

For more information and to download - www.veracrypt.fr

MOBILE DEVICES

iPhones - Apple encrypts all mobile devices and tablets as default, so the user does not need to configure anything to ensure their device is protected.

Android - Android phones are increasingly becoming encrypted by default, but it is not uniform across the different devices. To check whether your phone is encrypted:

1. In **Settings** click on **Security**
2. Click on **Encrypt Phone** (as specified above this can take a long time so it is recommended to have your phone charging while you do this)

Alternatively, the option may be in the **Storage** section of your settings. If you do not have any of these options, it is likely the phone is encrypted by default.

For both Android and Apple phones it is vital that you use a strong passphrase or passcode to access the device. If these are easily guessed, it will undermine the protection of device encryption.

IDEAS FOR YOUR LIBRARY

- Ensure all devices in the library (used by both staff members and users) are encrypted
- Incorporate within digital literacy classes so users can encrypt their devices at home
- Support local businesses to encrypt their devices

TOR & ANONYMOUS BROWSING

Category: Privacy

Tor, or The Onion Router, is a volunteer-run service that provides both privacy and anonymity online by masking who you are and your location. The service also protects you from threats in the Tor network itself.

According to the Tor Challenge (run by EFF), "**When you use the Tor software, your IP address remains hidden and it appears that your connection is coming from the IP address of a Tor exit relay, which can be anywhere in the world.**" The security of the Tor network is as strong as the number of Tor relays available to users.

The Tor network ensures anonymity online and is used by journalists, human rights defenders, whistle-blowers and many more around the world to protect their privacy.

How does Tor work?

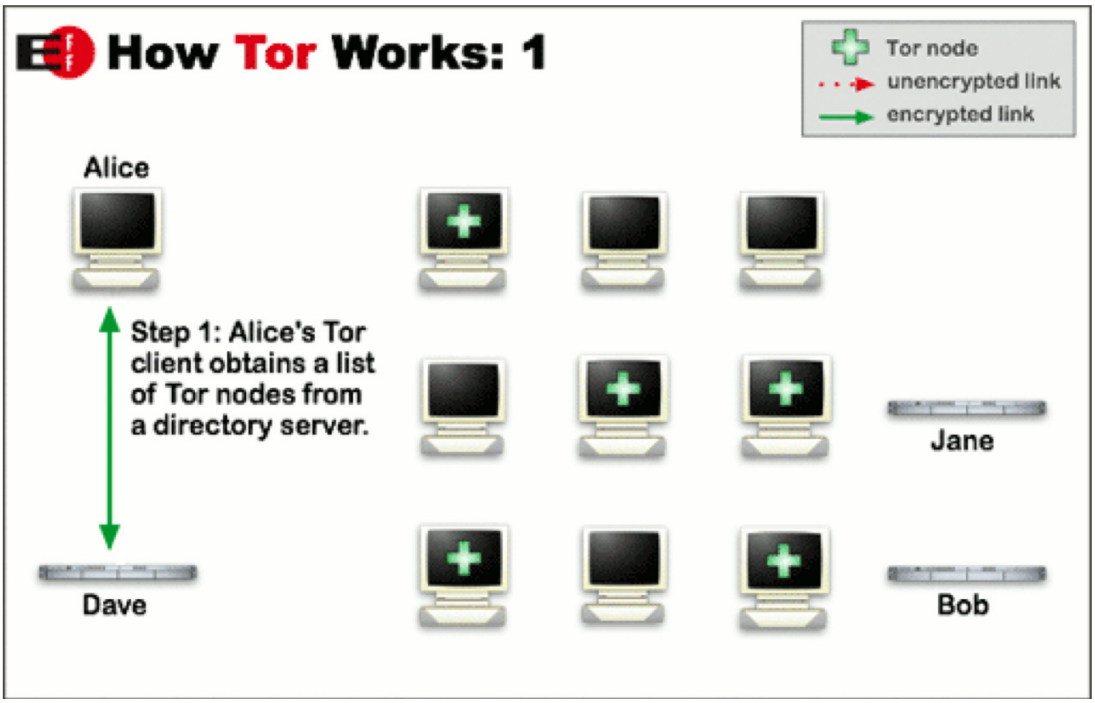
When you connect to the Tor network via Tor Browser, this is what happens:

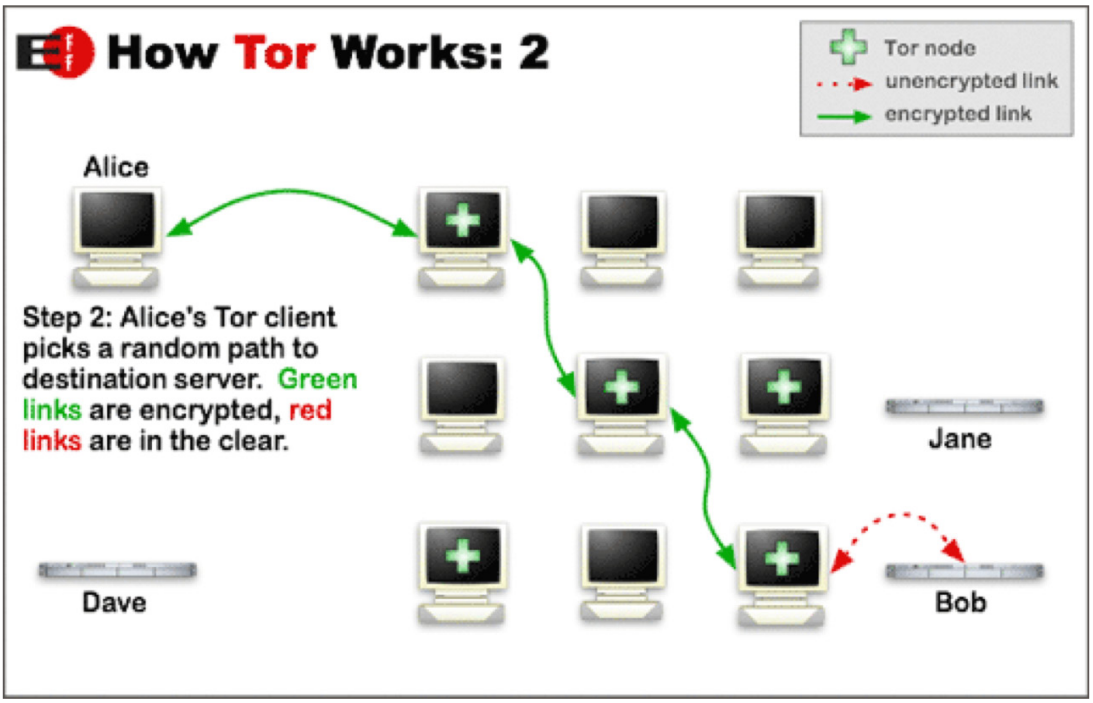
1. Using an encrypted channel, the user's Tor client obtains a list of Tor nodes from a directory server
2. Your client then plots a path through anonymous Tor nodes (servers), the path of which is randomly generated. The links between these nodes are encrypted.
3. When the user request reaches the Tor exit relay (the last node/server between the Tor network and the website the user is seeking to connect to) it is connected to the requested website server via an unencrypted link.

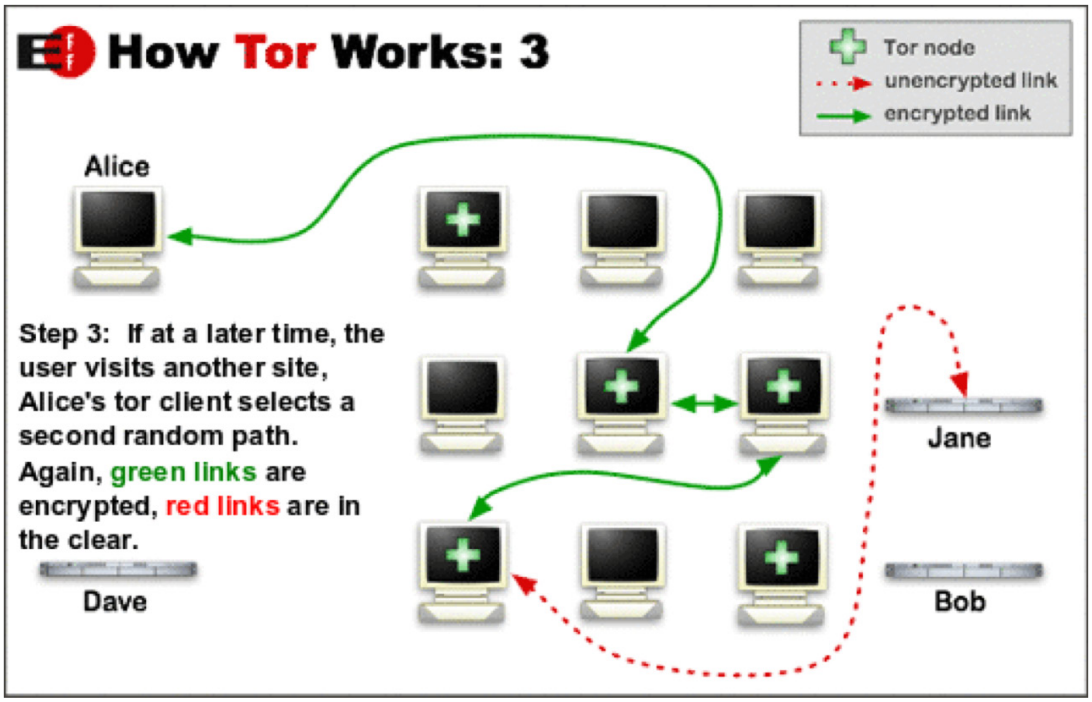
a. This is unencrypted because the personally identifiable information from the user has been replaced with the information of the last Tor node its request has passed through (the Tor exit relay)

4. Information from the website server is then passed through the existing pathway in the Tor network before displaying the website information to the user.
5. If you close your Tor Browser client it forgets both the data shared and the pathway established to share your request and when you open it again a new random pathway is generated through the network.

Here is a diagram developed by EFF outlining how Tor works







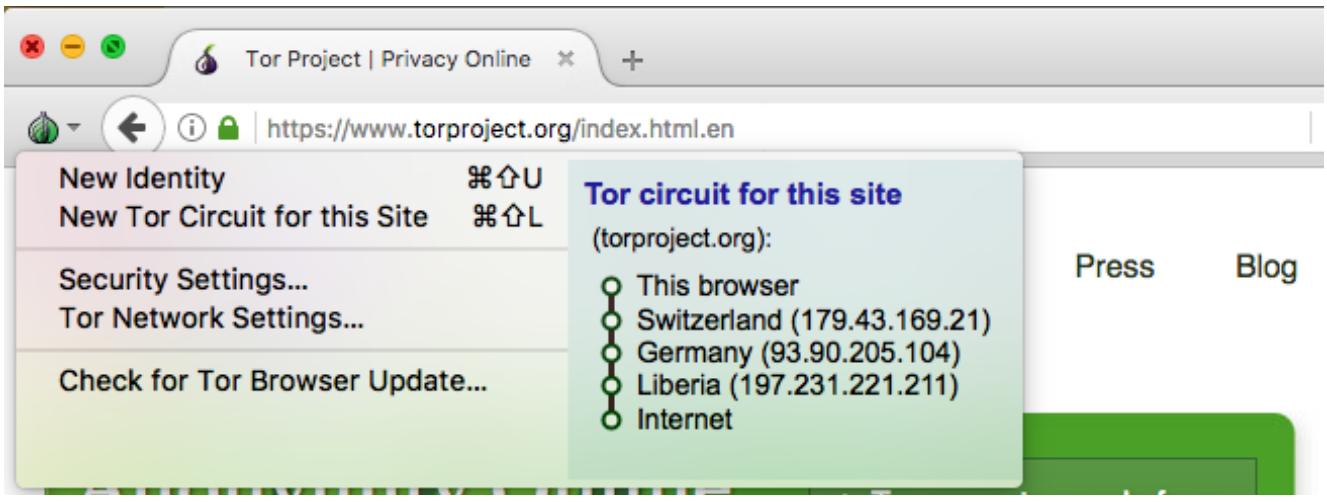
Tor:

- **Obscures your IP address**
- **Prevents cross-site correlation**
- **Blocks cookies and scripts**
- **Writes nothing to disk**

Library Freedom Project

To navigate the web via Tor, it is recommended to use Tor Browser. This browser is also bundled with a number of add-ons mentioned previously in this toolkit: NoScript & HTTPS Everywhere, as well as having DuckDuckGo as the default search engine.

To download Tor Browser: www.torproject.org/download/download-easy.html.en



Tor Browser shows the route your data travels through the relays that make up the Tor network

Things to Consider

When using Tor, to ensure your privacy is fully protected you may need to change your behaviour online.

Things to remember are:

- **Use Tor Browser to access Tor** – This will ensure you are using a platform that is pre-configured to protect your privacy and anonymity on the web. Almost any other web browser configuration is likely to be unsafe to use with Tor.
- **Don't torrent over Tor** - Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor.
- **Don't enable or install browser plugins** - The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others, as they can be manipulated into revealing your IP address.
- **Use HTTPS versions of websites** - Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website.
- **Don't open documents downloaded through Tor while online** - You should be very careful when downloading documents via Tor (especially DOC and PDF files, unless you use the PDF viewer that's built into Tor Browser) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address.

List courtesy of The Tor Project

Challenges for libraries

The very nature of Tor ensures anonymity (when properly utilised). However, it would be incorrect to suggest this does not offer problems for libraries seeking to utilise the network in their institutions.

Illicit Behaviour – Due to the nature of Tor, the network has been used for the promotion and sale in many illicit and illegal items and services. This includes illegal drugs and weaponry, alongside material related to images of sexual abuse of children and other criminal activities. This

content has defined in large part the public perception of the Tor network (earning it the moniker, the dark or deep web) but this should not define the network as a whole. The marketplaces for these materials are not easy to find, a very specific Tor URL is required and as they are not indexed, these sites cannot be found through conventional web searches, even within the Tor network.

Working with Authorities – The Tor network does not store information as to the pathways established or information shared by individual users, and because the information collected by the website pages accessed through the network only reveal details of the tor exit relay used, personal information cannot be shared with authorities, even upon receipt of a legal request. The principle of Tor is that you cannot share what you do not have in the first place.

THE MEDIUM OR THE MESSAGE

Illicit content shared on the Tor network represents the content of the message, not the definition of the medium. We need to be sure we approach this tool in a value-neutral manner that evaluates the tool's strengths for you and your requirements. Put another way, should we condemn paper, because of the publication of Mein Kampf?

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users
- Training on tor & anonymous browsing
- Install Tor Browser & mobile Tor tools
- Host open meetings & debate sessions on role of Tor in local communities
- Address concerns of user base i.e. parental control etc.
- Install Tor browsers on public terminals
    - Wholesale or via a singular terminal with Tor browser access
- Install Tor exit relay in local library

SECURE COMMUNICATIONS

Category: Privacy

There are a number of ways to communicate online including email, SMS (such as WhatsApp, Signal and Facebook Messenger) and VOIP (Voice Over Internet Protocol, such as Skype). Each have their own specific challenges related to both privacy and security.

EMAIL

Emails are neither secure nor private – once they are traveling between mailboxes they are similar to postcards, the contents visible to anyone looking.

For fully encrypted and secure email, the only system available is PGP Encryption, which requires a greater level of technical literacy and bespoke tools, as well as recipients who also utilise similar tools and practices.

Short of PGP Encryption, there are a number of steps that can be undertaken to ensure emails are sent and stored in the most secure manner possible.

Most email systems will use HTTPS to encrypt data travelling between websites and the Internet. Gmail, Yahoo, Tutanota & Protonmail offer HTTPS as default. If yours doesn't it would be worth downloading HTTPS Everywhere (see earlier chapter) to ensure your data is encrypted if it is available. This will ensure your communications cannot be read by other people on your network.

Please note: HTTPS will encrypt the information shared between you and your email service but not the contents of the emails you send or receive.

Recommended Providers

ProtonMail – This email provider is based in Switzerland and stores all data on their mail servers in an encrypted format. Data is also transmitted in an encrypted format between their servers and user devices. Messages between ProtonMail users are also transmitted in encrypted form within their secure server network. Protonmail has no access to the data held in personal email accounts and so cannot hand over information to the authorities even when asked.

To sign up to ProtonMail: www.protonmail.com

Tutanota – The email provider supports end-to-end encryption, so email stored on Tutanota's servers is encrypted and cannot be accessed or decrypted by staff members. Tutanota goes one step further than ProtonMail by encrypting subject lines, attachments and contact lists. Regular messages sent to non-Tutanota recipients are not encrypted in transit, but are stored encrypted on their servers.

To sign up to Tutanota: www.tutanota.com

Both Tutuanota and ProtonMail perform encryption via JavaScript so some vulnerabilities exist that could be used by a 3rd party to access the data shared via the email system.

Please note: Encryption will not obscure metadata or email subject lines (except in the case of Tutanota) and cannot protect against the monitoring of relationships between individuals. For example, if two people are communicating via email, the contents of their messages would be protected if they are using encryption, but this would not prevent a 3rd party identifying a relationship between the two people i.e. revealing that the two were communicating in the first place.

SMS & TEXT

Increasingly common, these tools enable individuals and groups to communicate across the Internet via text messaging, the sharing of videos and images and voice calls. Popular tools include WhatsApp, iMes-

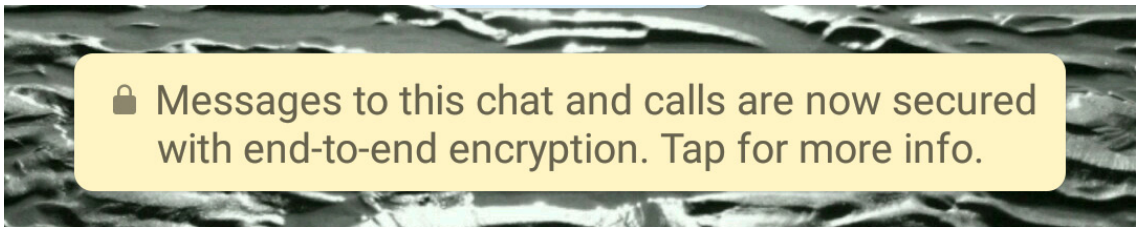
sage, Facebook Messenger and Signal.

Many are end-to-end encrypted which will frustrate attempts by 3rd parties to access communications data being shared, but as demonstrated with the controversy surrounding WhatsApp sending personal data to its parent company, Facebook, private data, such as metadata or usage statistics, can still be shared without the knowledge of users depending on the data sharing policies of the platform itself.

Signal – this open-source communications app, created by Open Whisper Systems allows for private messaging and calling over the Internet, both of which are end-to-end encrypted so nobody (even Open Whisper Systems) can access the content of the communication.

Compatible Platforms: Android | iPhone | Mac OS | Windows
Download: www.signal.org

WhatsApp - owned by Facebook, this uses the encryption protocol developed by Open Whisper Systems for Signal. As a result all WhatsApp communciations are end-to-end encrypted.



The message you will see on WhatsApp confirming the communications shared are encrypted

However, WhatsApp will share metadata and other usage reports and data with Facebook. Whether you choose to continue using WhatsApp is a choice to be made based on your Threat Model.

RETURNING TO YOUR THREAT MODEL

This toolkit can offer recommendations for certain tools and show why they may be more secure than others, but every choice you make in relation to yourself, your institution and your users must relate to your threat model to ensure the tools best reflect your needs. For more information check out this blog by EFF: https://www.eff.org/deeplinks/2018/03/why-we-cant-give-you-recommendation

Facebook Messenger - By default, Facebook Messenger is not encrypted, leaving the content open to the platform & other 3rd parties. However, through the online app you can use **Secret Conversations** that are end-to-end encrypted.

1. Open the app and a conversation with a contact
2. Click the 'i' symbol in the top right
3. Click on **Go to Secret Conversation**

VOIP (Voice over Internet Protocol)

Short of using Skype, which, according to the Snowden revelations, was co-opted by the NSA as part of the PRISM programme, other more secure platforms exist for video calls.

Both Signal and WhatsApp support video calls through their encrypted system (requiring both parties to be signed up to the platform), but **Wire** is a dedicated VOIP service that is end-to-end encrypted and does not sell usage date to 3rd parties. It also allows encrypted group video calls and file transfer services and because it is open source, its codebase can be scrutinised by independent individuals to verify and validate its security and address any newly discovered vulnerabilities.

Compatible Platforms: Android | Mac OS | iPhone | Windows
Download: www.wire.com/en/download

IDEAS FOR YOUR LIBRARY

- Incorporate within digital literacy classes to library users
  - Training on secure communications platforms
  - Installation of secure platforms
- Install or promote secure communications platforms on public terminals for both staff members and staff
- Produce easy-to-understand guides that can be used by users that can outline the different tools on offer and what can be done to ensure secure and private communication

SECURE FILE-SHARING & STORAGE

Category: Privacy

Storing and sharing files with others, or supporting the collaborative editing of documents, has redefined how people can communicate and work together in different locations and time zones, as well as backing up data on a range of devices. Depending on cloud computing, this approach gives you flexibility and access, but raises concerns as to the level of access given to 3rd parties.

MORE CONCRETE THAT IT SOUNDS

Cloud computing and storage sounds more abstract that it is in reality. When we use these services we are just depending on servers that are externally based and not controlled by the users. This enables documents contained within these servers to be accessed 24/7 on a range of devices as long as the device the user is using is connected to the Internet.

As the servers that enable cloud computing are managed by 3rd parties, the user has less control over the security processes undertaken to ensure the data is securely held.

The know-nothing defence

The **zero-knowledge** approach means that the provider, manager or developer of a platform or service is unable to access the data held by users of their service. This guarantees the integrity of the data and means that data cannot be shared by the platform – they cannot give what they do not have. This does have downsides – if you forget your

passwords to encrypted services (i.e. email or file storage) the service may not have access to this data and so cannot share it with you or help you select another password.

SANDSTORM

Sandstorm is an open-source digital environment that hosts a range of applications, which enables users to host documents and files and work with others with real-time chat rooms enabled to further support collaboration. The system also allows for backups to be saved to the cloud in an encrypted format.

For more information and to download: www.sandstorm.io

ONIONSHARE

Developed by Micah Lee of The Intercept and Freedom of the Press Foundation, OnionShare enables files to be shared anonymously via the Tor Network. Available for Windows, Mac OS X and Linux, Onion-Share sets up a web server on your device that shares the file via Tor. All the recipient needs is Tor Browser to download the file.

For more information: OnionShare Github

Compatible Platforms - Windows | Mac OS | Linux
Download: www.onionshare.org/#downloads

File-sharing over communications platforms

A number of end-to-end encrypted communication platforms allow for secure file-sharing, including Signal, Wire and WhatsApp (see earlier chapter).

How do the popular platforms fare?

GOOGLE DRIVE

Part of the Google digital eco-system, Google Drive allows for data storage and sharing, as well as collaborative work. Google Drive's

strengths depend on robust security processes that ensure malware or infected documents that are opened in Google Drive will be sandboxed – contained within the Google Drive system, without impacting the user's device. If you receive email attachments from an unknown contact, it is recommended that you download them (without opening) and upload them to Google Drive to open them.

However, in 2012 Google unified its terms and conditions to enable it to use files stored publicly on Google Drive as part of their promotional materials and potentially to help Google target ads to users. As outlined above in terms of Google Chrome, using Google Drive enables the corporation to collect and analyse your user data. This is a choice for the user based on their threat model.

A WOLF IN SHEEP'S CLOTHING

In 2016, an elaborate phishing campaign was undertaken using apparent Google Drive links shared from known contacts for 3rd parties to gain access to users' Google accounts. This was an incredibly sophisticated campaign that was able to mimic, with alarming accuracy, the appearance of Google Drive. This demonstrates the need for users to be aware of the programmes or platforms they use and to scrutinise every link they are sent.

DROPBOX

This is one of the most popular file-sharing platforms that has a number of security protections but fewer privacy protections. It does support 2-Factor Authorisation (see previous chapter) to add a layer of security for users accessing their accounts. However, it has been called 'hostile to privacy' by Ed Snowden, as Dropbox, like Google Drive, does not deploy a zero-knowledge approach, which means that Dropbox is able to access the files held by users if they receive a legal request to do so. Dropbox also stores information of users which includes IP Addresses and other information related to the device and browser used, profile information, behaviour on Dropbox and other personal data collated through usage.

iCLOUD

This is Apple's cloud storage system that operates as a back up for all Apple devices – in fact many Apple devices back up to iCloud as default, depending on the user to opt-out of the service manually. Like Dropbox and Google Drive, Apple does not deploy a zero-knowledge approach and while Apple has previously defended encryption on its devices (as documented in the well-known fight with the FBI regarding an iPhone captured from the San Bernardino attacks), there are weaker protections for iCloud as Apple is able to access the documents and data held in the cloud (remember it is a server they own, not a device you have), which can then be shared with law enforcement bodies and other 3rd parties.

IDEAS FOR YOUR LIBRARY

- Recommend file-sharing and storage tools to your users and staff that deploy a zero-knowledge approach and protects your private data from unknown 3rd parties

PHYSICAL SECURITY

Category: Security / Privacy

Alongside the steps outlined in this toolkit to strengthen digital security there are a number of steps that can be taken to improve our physical security. If a 3rd party cannot access our data or devices through the Internet, they may seek to access the information through physical access.

Here are a few steps you can take to improve your physical security:

1. **Never leave devices unattended –** If a laptop, tablet or mobile phone is left unattended this could be the window of opportunity for a 3rd party to access your device and potentially the data held within, which leads us to step two.

2. **Encrypt devices –** this step will ensure that physical access to a device does not necessarily mean a 3rd party can access the data contained within. If the devices are encrypted, in the worse case scenario were they to steal your device, encryption limits the possibility that they will be able to access any data, leaving them with a device they cannot access (for more details see earlier chapter).

3. **Be aware of your surroundings –** Without encouraging an all-encompassing sense of paranoia, an awareness of your surroundings and people in your proximity is recommended. If you are working in a public place and are sharing personal information – on a website i.e. setting up an account, paying for something or completing a contact form, or on the phone – make sure you take steps to avoid people eavesdropping your conversation, viewing your screen or keyboard. This is especially important when you are entering passwords

and other sensitive details.

4. **Never use a USB memory stick that you find –** If you find a USB memory stick, however intrigued you are, do not use it. You have no knowledge as to what is contained on the device and once it is plugged in you may be powerless to stop any malware that may be contained infecting your device.

5. **Connecting to Wi-Fi Networks –** Only connect to secure networks you know or are signposted to connect to by the venue you are present in. If you connect to insecure networks you may be vulnerable to attacks by others on the network – a VPN or the Tor network can help you avoid certain attacks but it is worthwhile only using secure networks where possible.

6. **Use digital devices when you need to, don't when you don't –** The best way to ensure you are not compromised online is not using online platforms, devices or networks when you don't need to. This is, of course, impossible as a lifestyle choice, but you can choose to not use digital devices or not have one on your person at the most sensitive times i.e. at protests or when communicating with others who require anonymity.

GLOSSARY OF TERMS

Brute Force Attacks - A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software can be used to generate a large number of consecutive guesses as to the value of the desired data. (techopedia).

Bulk Powers – Surveillance powers that collect data on the many to find the few. This includes bulk interception (intercepting communications data), bulk equipment interference (hacking) and bulk personal datasets (databases and registers that contain information on a large group of people, such as the electoral roll, HMRC tax returns and sporting events ticket lists).

Cookies - A small piece of data sent from a website and stored in the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember information such as items added in the shopping cart in an online store or to record the user's browsing activity.

Cross-Site Correlation – This enables activity on one system, device or browser to inform other systems, devices or browsers. This is something that Tor Browser has removed to ensure that no more data than necessary was captured and shared between different systems or browsers. This can also include correlation between different browser tabs.

Encryption – This is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible

again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption. (Mozilla)

HTTP / HTTPS - Hypertext Transfer Protocol (HTTP) is an application protocol that is the foundation of data communication for the World Wide Web. It defines how messages are formatted and transmitted. HTTPS is the encrypted version – the S stands for secure.

IP Address - A unique numerical code that identifies each computer using the Internet Protocol to communicate over a network.

Open-Source – A method of creating software that makes the original source code (the building blocks for the service or platform) available and accessible to the public via a license, who can inspect, modify, enhance and distribute the code. This enables the software to be tested and scrutinised by diverse and independent actors, increasing the chances of bugs, vulnerabilities or flaws to be identified and resolved.

PET (Privacy-Enhancing Technologies) – These are technologies that place the protection of their users' data at the forefront of the technology's design and deployment. It also is the approach that ensures full compliance with relevant data protection legislation.

Search Leakage – This refers to the sharing of user data between a search engine and the sites searched via the search engine.

Tor – The Onion Router, which obscures web browsing through the deployment of a network of anonymous servers. The IP address of the user is cloaked by the address of the Tor Exit Relay, which contains no personal or identifiable data of the individual user.

Tor Exit Relay – This relay is the last server/node in the chain of anonymous servers that cloak anonymous users browsing through the Tor network before reaching their destination.

User Agent – Like an IP address, the user agent contains details of the technical data about the device and software the user utilises to access

the Internet.

Zero-Knowledge – Due to protections such as encryption, this approach ensures data held on a platform, service or device cannot be accessed by others including the service, platform or device provider, only by the user or data owner. This practice ensures that service users do not have to depend on providers resisting demands for 3rd party access – providers cannot give what they do not have access to.

LINKLIST

EFF's Introduction to Threat Modeling: ssd.eff.org/en/module/assessing-your-risks

INVESTIGATORY POWERS ACT

- Full Act: www.legislation.gov.uk/ukpga/2016/25/contents/enacted
- Big Brother Watch factsheets: www.bigbrotherwatch.org.uk/all-campaigns/investigatory-powers-bill

TOR

- Download: www.torproject.org/download/download-easy.html.en
- Tor browser bundle: www.torproject.org/projects/torbrowser.html.en
- How to set up and run a Tor relay: trac.torproject.org/projects/tor/wiki/TorRelayGuide
- What to do when torproject.org is blocked: www.torproject.org/projects/gettor
- Bridges: more censorship circumvention for Tor: www.torproject.org/docs/bridges
- Getting help using Tor: www.torproject.org/about/contact.html.en

BEHAVIORAL ANALYTICS

- NoScript: www.noscript.net
- Privacy Badger: www.eff.org/privacybadger
- uBlock Origin FireFox: addons.mozilla.org/en-US/firefox/addon/ublock-origin
- uBlock Origin Chrome: chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm

HTTPS

- HTTPS Everywhere: www.eff.org/https-everywhere
- Test the TLS/SSL security of a website or browser and learn more about implementing TLS/SSL: www.ssllabs.com
- Let's Encrypt: wwww.letsencrypt.org
- Certbot: www.certbot.eff.org
- What Every Librarian Needs to Know About HTTPS: www.eff.org/deeplinks/2015/05/what-every-librarian-needs-know-about-https
- Tor and HTTPS: www.eff.org/pages/tor-and-https
- The Library HTTPS Pledge: www.libraryfreedomproject.org/https-pledge/

PASSWORDS

- LastPass: www.lastpass.com
- KeePassX: www.keepassx.org
- 1Password: www.1password.com
- Diceware: world.std.com/~reinhold/diceware.html
- Diceware word list: www.eff.org/deeplinks/2016/07/new-word-lists-random-passphrases
- Yubikey: www.yubico.com

MALWARE

- ClamAV: www.clamav.net
- Malwarebytes: www.malwarebytes.com
- OS X native malware protection: support.apple.com/en-us/HT202491 and support.apple.com/en-us/HT201940

FULL DISK ENCRYPTION

- Filevault (OS X): support.apple.com/en-us/HT204837
- Bitlocker (Windows): docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10
- Veracrypt: www.veracrypt.fr/en/Home.html
- Encrypting your laptop like you mean it: www.theintercept.com/2015/04/27/encrypting-laptop-like-mean

BROWSERS

- Brave: www.brave.com/download

MOBILE

- Library Freedom Project's Mobile Privacy Toolkit: www.libraryfreedomproject.org/mobileprivacytoolkit
- Replicant: www.replicant.us
- The Guardian Project: www.guardianproject.info
- Snoopsnitch: opensource.srlabs.de/projects/snoopsnitch

EMAIL

- Email Self-Defense from FSF: emailselfdefense.fsf.org/en
- ProtonMail: www.protonmail.com
- Tutanota: www.tutanota.com
- Check the security of your email server: www.starttls.info

VPNs

- A list of possibly good VPNs: www.torrentfreak.com/vpn-services-anonymous-review-2017-170304

SAFE SEARCHING

- DuckDuckGo: www.duckduckgo.com
- Qwant: www.qwant.com

COMMUNICATIONS

- Signal: www.signal.org
- Wire: www.wire.com/en/download

EXTRA CREDIT

- Surveillance self-defense from EFF: ssd.eff.org
- Security Education Companion from EFF: sec.eff.org
- Cryptoparty: www.cryptoparty.in

FILE SHARING

- Sandstorm: www.sandstorm.io
- OnionShare Github: www.github.com/micahflee/onionshare
- OnionShare: www.onionshare.org

TERMS OF SERVICE

- Terms of Service; Didn't Read: www.tosdr.org/index.html

OPERATING SYSTEMS

- Qubes: www.qubes-os.org
- Tails: tails.boum.org
- Subgraph: www.subgraph.com

If you have any questions or feedback on this toolkit please contact Nik Williams, Project Manager, Scottish PEN

Email: nik@scottishpen.org
Phone: 0131 226 5590
Website: www.scottishpen.org

Follow the conversation at: @ScottishPEN // @nikwilliams2

Want to join Scottish PEN?

Scottish PEN is a membership organisation of writers, readers and those who love literature and want to defend free expression. By becoming a member you can join our campaigns and defend writers.

Your membership dues will also help us continue our work both in Scotland and across the globe: www.scottishpen.org/join-us

www.scottishpen.org // @scottishpen // May 2018