

Privacy Online Guide



Privacy Online Guide

This toolkit is supported by JANIC / NED Grant to ADA

Written by **Derek Caelin & Bejoy Joseph George**

[Asia Development Alliance](#)

[Japan NGO Center for International Cooperation \(JANIC\)](#)

Info@ada2030.org



Table of Contents

ABOUT THE PRIVACY ONLINE TOOLKIT	5
1. INTRODUCTION	7
1.1. CIVIL SOCIETY IN THE DIGITAL AGE.....	7
2. THREAT MODELING	8
2.1. THREAT MODELING AND THE CIVIL SOCIETY ACTOR	9
2.2. WHAT CONSTITUTES RISK?.....	9
2.3. MODELING METHODOLOGIES	10
2.4. IDENTIFYING THREATS (OR THREAT INTELLIGENCE).....	11
2.5. THE 4-D THREAT MODELING PROCESS	12
2.5.1. WHAT ARE 'ASSETS'?	14
2.5.2. HOW DO YOU DECONSTRUCT?	14
2.5.3. THE IMPORTANCE OF DOCUMENTATION	14
2.5.4. DESIGN PROTECTION (RISK MITIGATION).....	15
2.6. THE HUMAN FACTOR	15
3. PRIVACY IN COMMUNICATION	17
3.1. MESSAGE'S JOURNEY	17
3.2. ENCRYPTION AND PRIVACY.....	19
3.2.1. SMS AND EMAIL	20
3.2.2. TYPES OF ENCRYPTION	21
3.2.2.1. ENCRYPTION IN TRANSIT AND AT REST	21
3.2.2.2. END-TO-END ENCRYPTION	21
3.2.3. METADATA	22
3.2.4. TRUSTING A SERVICE PROVIDER	23
3.3. APPS FOR COMMUNICATING SECURELY	23
3.3.1. ENCRYPTED EMAIL	24
3.3.2. SOCIAL MEDIA	24
4. PRIVACY IN BROWSING THE WEB	24

4.1.	ENCRYPTION ONLINE.....	25
4.2.	DNS AND PRIVACY	26
4.3.	COOKIES AND TRACKERS.....	27
4.4.	INCOGNITO OR “PRIVATE” MODE.....	27
4.5.	VPNS AND TOR	28
4.5.1.	VPNS	28
4.5.2.	TOR.....	30
4.6.	PLUGINS	31
4.6.1.	HTTPS EVERYWHERE	31
4.6.2.	PRIVACY BADGER	32
4.7.	BROWSERS	32
4.8.	OTHER TIPS FOR IMPROVING YOUR PRIVACY ON THE WEB	33
5.	PROTECTING YOUR ACCOUNTS	33
5.1.	ACCOUNT ATTACKS.....	34
5.1.1.	PHISHING	34
5.1.2.	WEBSITE BREACHES	36
5.1.3.	SURVEILLANCE AND MALWARE, AND OTHER ISSUES.....	36
5.2.	TWO-FACTOR AUTHENTICATION.....	36
5.2.1.	SMS	37
5.2.2.	APPS.....	37
5.2.3.	PHYSICAL TOKENS	38
5.3.	PASSWORD MANAGERS	38
6.	ADDITIONAL RESOURCES.....	40
6.1.	GUIDES.....	40
6.2.	TOOLS	40
6.2.1.	BROWSERS.....	40
6.2.2.	PASSWORD MANAGERS	40
6.2.3.	TWO-FACTOR AUTHENTICATION TOOLS	40
6.2.4.	VPNS	41
6.3.	INTERESTING LINKS	41
7.	CONCLUSION	41

About The Privacy Online Toolkit

This guide is for activists and members of civil society who are concerned about protecting their communications and browsing activity when using the Internet. This document will explain the basic process of determining who is threatening the reader and how, as well as the various things the reader can do to increase the privacy of their behavior online. Because everyone deserves to be able to use the Internet safely, no matter their level of technological skill, the authors have made a conscious effort to present the following information as simply and approachably as possible.

Note: Individuals and organizations who face security and privacy concerns should work with a digital security trainer to address challenges. This book will discuss some general best practices, but your own security and privacy strategy should be developed to meet your specific needs.

That being said, this guide will introduce you to a number of practices and tools you can take to protect your communications online. We'll start with Threat Modeling - a process by which the security threats are anticipated and the way you can structure a plan to address them. After that we'll discuss Privacy in Communication, and describe the way that a message travels through the Internet, the nature of encryption, and the various tools you might use to communicate securely. Next, we'll discuss Privacy in Browsing the Web: the value of encryption for websites and the various browsers and other tools you might use to protect yourself online. As an addendum, we'll also discuss a few elements of digital security that will help you to protect your accounts: two-factor authentication, phishing, and password managers. We hope this will be a useful introduction for users to practices that will help improve their safety in an increasingly digital world.

This guide is the result of Four weeks long training program organized by the [Asia Development Alliance](#) on Social Networking Site in September-October 2020, where a need of a guidebook for the CSOs were widely proseed by the participants from all across Asia and Pacific region.



Thanks to Mara Caelin, Steve Francis, Philip James, Seth Marbin, Rezy George and Arzak Khan for reviewing and editing this document.

Cover image by Vladyslav Cherkasenko on unsplash.com

1. Introduction

1.1. Civil Society in the Digital Age

Since the early days of the Internet, technologists have warned us that the Internet could be a highly regulated and surveilled space. In his 1996 book *Code*, Lawrence Lessig warned readers of the dangers in thinking the Internet was immune to censorship and surveillance:

"Whatever cyberspace was, there's no reason it has to stay this way. The 'nature' of the Internet is not God's will. Its nature is simply the product of its design. The design could be different. The Net could be designed to reveal who someone is, where they are, and what they're doing. And if it were so designed, the Net could become...the most regulable space that man has ever known."¹

Today, Internet users around the world must confront an increasingly regulated space. Governments, hackers, and private companies routinely monitor citizen behavior online, whether to monitor threats to the state, prevent the flow of information and ideas, or to develop a profile of users, in order to better control them (or to serve them targeted advertisements). Unlike more traditional forms of monitoring people, which required a relatively high investment of resources to track the communications and actions of individuals, modern surveillance uses machines to track user behavior at scale. Billions of users interact with online systems designed to log the websites they visit, their search histories, and their interactions with other users.

We exercise many of our civic freedoms – the right to assemble, organize, and speak – in online spaces: through social media, on news outlet websites, in conversations with friends and colleagues over communication apps. Some offline events exacerbate this trend towards the digital space. As we write this guide in the midst of a global pandemic, whole industries have moved online, and digital communications have replaced in-person speech for many.

Since so much of our civic lives takes place online, it is essential that citizens know how to seek information and interact online in privacy. As the techno-sociologist Zeynep Tufekci has said:

"Dissent requires the right to privacy: to be let alone in our vulnerabilities and the ability to form our thoughts and share them when we choose,"²

Now as much as ever, citizens need to be able to communicate safely. This guide seeks to help the reader learn to do just that.

¹ Lawrence Lesig. *Code Version 2.0*. Basic Books, 2006.

² Zeynep Tufekci. <https://zeynep.substack.com/p/ignoringblackmail>. Accessed 23 Dec. 2020.

2. Threat Modeling

Let us take our minds back some three million years ago to the stone age. A caveman steps outside his cave in the morning and sees this dead animal lying in front of his cave. The rotting flesh renders the animal inedible. Mr. Caveman starts walking away, then stops and turns. He surmises the smell may attract predatory animals to the area, animals which may end up attacking him. He therefore decides to dig a hole in the ground and bury the animal, thereby neutralising the threat.

There we have it - the first instance of threat modeling.

This may appear to be a rather simplistic example. The point is that we, as humankind, are programmed genetically to identify threats and take steps to neutralise them. This helped our ancestors survive and pass on their DNA to future generations. It is therefore a survival mechanism to identify threats to our wellbeing and take steps to avoid them.

Through millenia our ancestors foraged and thrived until mankind finally reached the information/digital age. A large proportion of people started using computers, local area networks, the internet and so forth.

A multitude of problems soon emerged.

IT administrators quickly found that networked computers were particularly susceptible to worms, viruses and trojans. Painful experience taught us a networked world could be a dangerous place. Software was compromised by malware. Email addresses were discovered to be easy to impersonate (or spoof). Users' personal information was being stolen. Identities were stolen. Users' computers were (and still are) being hijacked and held for ransom.

A new age of threats had dawned. In this context, it quickly became apparent that protection from potential threats could not be accomplished using an ad-hoc approach. Assessing the risk based on prior experience and a gut feeling - the system that worked so dependably for our ancestors, would not suffice in the complex world of technology today.

Our head honchos, the chiefs, engineers, generally-people-on-the-ball and suchlike realised that we need to develop a more structured system to identify threats and address weaknesses. And thus, was born threat modeling as a formal process in the technology industry.

Traditional threat modeling is a process through which IT professionals identify potential security threats and vulnerabilities (also referred to as risks), evaluate the seriousness of each risk, and devise techniques to mitigate attack and protect IT resources.

Threat modeling is therefore a *structured* security assessment and mitigation technique.

2.1. Threat modeling and the civil society actor

Since we all consume technology and use social media in today's interconnected world, there is a fairly high chance that a user's personal safety online may be compromised, often without his or her knowledge.

Many readers may have heard of "computer viruses" and "trojans." Collectively these are referred to as "malware". In addition to malware, civil society activists have the added risk of being actually targeted by vested interests who wish to hinder their work. This makes it critical that risk mitigation measures are taken when working on online devices.

Although not codified as such, the principles of threat modeling can be applied very successfully to a non-technology professional such as a civil society worker.

2.2. What constitutes risk?

In simple terms, risk is the possibility of something undesirable (or bad) happening. Risk mitigation is the process by which the effect of a particular risk is minimised or eliminated.

A question that arises are what are the risks that need to be mitigated? They need to be identified, of course. Here are some examples:

- The risk of one's identity being exposed when anonymity is desired (with sensitive information in an oppressive environment, as an example);
- The risk of sensitive or private information being stolen;
- The risk of exposing one's email credentials;
- The risk of unknowingly compromising a colleague by passing on malware;
- The risk of your technology assets (such as your computer and internet connection) being misused to launch a denial of service (DoS) attack on a web server, taking it offline;
- The risk of one's identity being hijacked to promote fake social media posts;
- The risk of using unlicensed software (often downloaded free) that may contain malware;
- The risk of a script on a website that keeps running even after you close the website, potentially exposing your browsing history or other sensitive information;
- The risk of buying a compromised laptop that contains malware and unknowingly using it;
- The risk of a compromised app on a mobile phone that steals data or collects private information;

- The risk of granting unnecessary permissions to a mobile app on a smartphone;
- The increasing risk of website and mobile app scripts that gather highly intrusive data of usage habits;
- The risk of apps such as Uber that continued to log a user's location long after the Uber ride was over, constituting a breach of privacy;
- The risk of being subject to attacks that track the users key presses or guess their password by trial and error;

A major portion of risk faced by an average non-IT user is on mobile devices due to the use of multiple apps that are installed without much thought or consideration towards security.

To address a risk, one has to anticipate the threat and take protective measures in advance. In other words, one has to apply a threat modeling process.

2.3. Modeling methodologies

Security teams in the IT departments and software companies use several different threat models to evaluate risks. There is a bewildering array of methodologies used by private companies in securing their technology assets and offering the same service to clients.

In the context of a civil society organisation (CSO) or a CSO practitioner, there is however no standard methodology that is currently being followed. In fact this is a fairly young science with respect to risk protection at this level.

Therefore, it falls upon the user to devise methods by which one can identify and address potential risk caused by using technology on a daily basis, including profuse use of various social media channels as is the norm today.

Unfortunately, there is no easy 'tried and tested' solution to implementing threat modeling. The risk profile changes quite drastically depending on the usage characteristics of any particular person or organisation. Furthermore, the activities of the civil society activist may incur malicious interest from vested interests that can vary wildly from government officials to private sector entities and various individuals, not to mention your garden variety hackers.

A complete risk mitigation solution that works under all circumstances does not exist. This is precisely why there is the need for modeling (or anticipating) potential threats.

One may misconstrue a good antivirus software to be the solution for avoiding infection by viruses (or malware). However, if the antivirus programme is not regularly updated, it will offer insufficient protection and may not detect the latest strains of malware. If it is misconfigured it may offer insufficient protection. In this case, the threat modeling exercise will help identify the risks of not updating the antivirus software regularly as well as if it is improperly configured.

While the user may have the best antivirus protection, if sufficient care is not taken towards keeping passwords private, their personal email access may be compromised and people with the wrong intentions (known typically as ‘threat agents’) may access their email accounts.

A modeling exercise therefore becomes necessary to gather threat intelligence. This modeling exercise may be in the form of creating a simple spreadsheet or a document template that may be reused within the organisation or in a particular context.

2.4. Identifying Threats (or threat intelligence)

Let us consider the case of Rita, a civil society worker. As a computer literate person who is active on media fairly extensively, Rita uses email in the course of her daily work and posts daily updates on her social media channels. Rita is however unaware of the concept of risk mitigation. She is therefore not careful when using her digital devices to avoid malware. She has no protection installed on her laptop nor does she follow best practices in safely using mobile apps. Asking Rita to do a threat model would be futile, for obvious reasons.

There is an educational component to threat modeling, as indicated by this example. One needs to be made aware of the various possible risks. A person who is not aware of the danger of malware will not worry about installing antivirus software.

Before identifying a threat, the user needs to be cognizant of it. This process of collecting data about possible threats (as applicable) is known as threat intelligence. Threat intelligence is the accumulation of knowledge with specific reference to various forms of threats that are constantly developing.

Threat intelligence are typically applied within the following areas:

1. Strategic
2. Tactical
3. Technical
4. Operational

Any of the above can be compromised due to threats which need to be identified by anticipating where breaches may occur during the course of daily work or otherwise. The gathering of such information constitutes what is called **threat intelligence**. Threat intelligence is gaining an understanding of existing and emerging threats to security (such as new data-mining techniques) with the aim of generating meaningful information for developing a threat model.

Frequently there is a trade-off between the severity of a risk and the possibility that it may actually happen or its frequency of occurrence. If the risk is not severe enough it may be allowed to happen more frequently in a threat model. This is because it is not practically feasible to neutralise every possible threat.

2.5. The 4-D threat modeling process

We have defined threat modeling as a proactive strategy for evaluating risks, analysing the severity of such risks and applying measures to mitigate these risks.

We have understood that the principles of threat modeling can be applied for personal safety and security online.

The question that arises is how we actually implement these principles?

There are various threat modeling methodologies developed by different software development companies that apply specifically to the software development lifecycle. Most are highly detailed and very specific to certain use cases.

Since these are all specific to software development and in some cases, local area networks, while it is possible to apply the same principles in the context of CSOs the terminology may be confusing and most, if not certain steps may be unnecessary.

We therefore lay out a highly simplified form of threat modeling called the 4-D process which constitutes of four overarching steps:

1. **Define** your assets that need protection;
2. **Deconstruct** the process by which they may be compromised;
3. **Document** this (ideally using a structured template);
4. **Design** a systematic and structured process for protection;



2.5.1. What are 'assets'?

An asset is something of value, which you do not wish to fall into the wrong hands. A very good example of this would be your email password. You do not wish for someone else to impersonate you. This is an asset that needs to be protected under all circumstances. The same goes for your social media access username and password combinations. Other assets would be your contacts' database or your list of donors.

The first step in threat modeling is therefore to list all of your assets. Depending on the situation these may also include your personal information, family member details, sensitive correspondence, work documents etc. The list of assets should be as comprehensive as possible.

2.5.2. How do you deconstruct?

Now that you have listed your assets, the next step is to deconstruct the technology pipe through which your assets flow. This is just a complicated way of saying that the combination of hardware and software used as well as the security of your device will affect your assets. Be aware of how each aspect impacts on the safety of assets.

Let us take the same example of your email password as an asset that needs protection. Many people have a browser account that allows them to store passwords securely (Chrome, Edge and Firefox are a few examples that allow this). If the password is stored in your browser by default, it may be at risk unless the browser password is sufficiently secure AND your device has a strong password or fingerprint mechanism to block unauthorised access. Furthermore the device needs to be protected against unauthorised remote access as well.

The deconstruction process would therefore include the browser, the actual email account username/password combination and the access restriction applicable on your computer or mobile device. Any of these may be a point of failure.

2.5.3. The importance of documentation

The whole concept behind threat modeling is that it is a structured process that is documented. A clear template should be developed for each use case. Taking the example of email security, the process of documentation would cover the potential points of compromise and what steps the user would take to secure the password. Again, a similar exercise could be undertaken with website administrative credentials.

The process of documentation assists with standardisation and helps promote best practices in security.

2.5.4. Design protection (risk mitigation)

After all of the work in identifying risks and documenting them properly in the previous steps, the final step would be to design or develop protection. This would be where a solution such as an antivirus software would be implemented.

It needs to be noted that designing protection is a combination of installing deterrents such as security software as well as following best practices such as regularly updating the software with the latest virus patterns.

Taking the email password as an example, a risk mitigation measure (or best practice) would be to use a sufficiently strong password that cannot be easily guessed. We can use whole sentences as passwords and add numerals and special characters to them. Furthermore another best practice would be that one does not enter the password without sufficient privacy (such as in full view of an overhead camera or people standing behind the user).

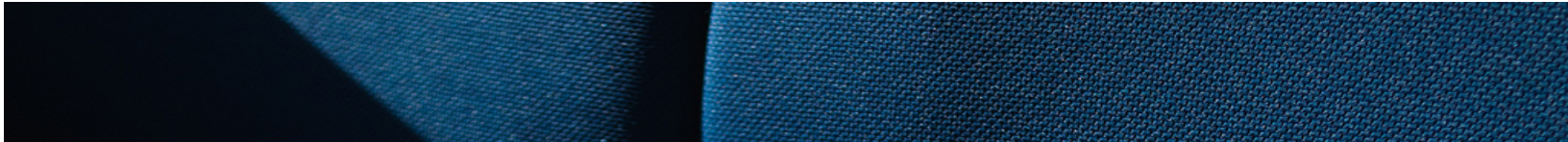


Photo by Glen Carrie on unsplash.com

2.6. The Human Factor

This is the age of social media. People are social creatures. People do silly things on social media. Look up the story of Hannah Sabata who robbed a local bank at gunpoint in 2012 and then decided to post a YouTube video bragging about this. She was arrested in quick order (We have linked to the article below in the [Links](#) section).

This is also the age of *social engineering*, a manipulation technique that exploits human error to gain private information or otherwise exploit the victim. People's greed and need for social



affirmation can be exploited to manipulate them into compromising security, as we'll discuss in the section below.

The point is that people are very often the most prone to failure in any system. The chances of a security breach caused by a staff person are higher compared to the inherent risks of hardware and software. Most threat modeling exercises place emphasis on actual end users as a critical source of failure. Some measures that need to be put in place to mitigate this risk would be the requisite staff training and an ongoing emphasis on security.

Perhaps one of the most critical aspects of risk mitigation is appropriate staff selection and training as well as the application of clear security protocols in organisational communication and social media channels. It is also imperative that your team understand how your important messages and information may be exposed and should be protected, as we will discuss in the next sections.

Keep in mind that digital security is both institutional and individual.

3. Privacy in Communication

Every day, many of us use the Internet to message a colleague, an acquaintance, a family member, or friend. In some environments we can send dozens, if not hundreds of messages a day, often through multiple services. Telecommunication is vital for coordinating action, planning activities, or simply getting through the day's tasks. The messages we send and receive do not simply disappear from our device and appear on another. In this section, we will review how a message travels from one place to another, and who can see it along the way.

3.1. Message's Journey

How does a message travel from one device to another? Our chats, texts, videos, and sound files are transmitted from a variety of different apps and through a number of different channels, but many of them behave the same way. Unfortunately, it is very rare to see a message travel as represented in the picture below: directly from one place to another. This *can happen* in some circumstances - for example, if you are using a special app designed to send messages through a phone's Bluetooth transmitter - but generally the process is more complicated.



A message can only jump directly from device to device with special apps, and users usually need to be very close together.

Instead, the message must pass through a number of different stages as it travels from one phone to another. It may be helpful to think of the journey in seven stages:



The message originates in the **Sender's Device** and all the apps and services on it...



...then, if the device is connected to wifi WiFi, it passes through the **Sender's Router** that connects a device to the Internet...



...the message then enters the **Communications Network** - the collection of devices that transmit messages from machine to machine until it reaches its destination...



... on to the **Service Provider** - the company, organization, or individual providing the communication service (for example, WhatsApp). After this, the message passes...



...back to the **Network**, again...

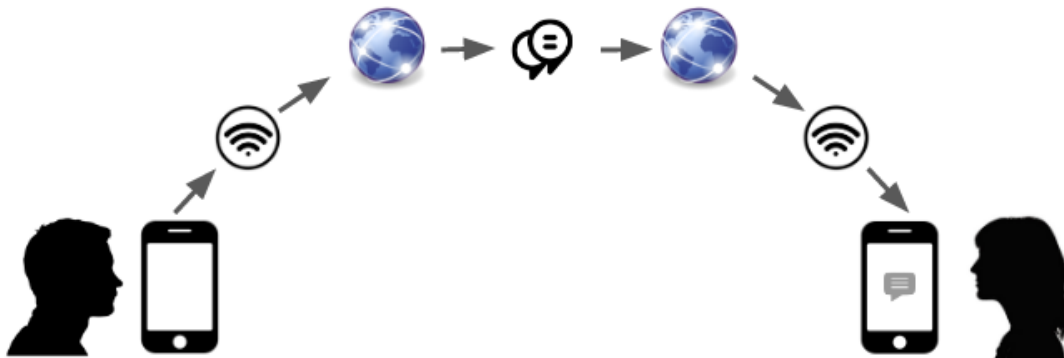


...Then it passes to the **Recipient's Router**, if she is connected to the Internet that way...



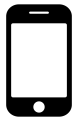
... finally, the message arrives at the **Recipient's Device**, and all the apps and services on it.

Put together, these stages look like this: a step-by-step process in which a message passes from point to point.



The important thing to remember is **that each stage of this journey represents a point where your message might be seen**. Our goal in this toolkit is to help you protect your message at each stage.

Let's say that you send a message to a colleague. How might an adversary view those messages?



On the **Sender's Device**, a message might be seen by the organization that makes your messaging app, or by attackers if a virus is monitoring your activity.



If the **Router** or WiFi network the user is connected to is compromised, someone with access could see the websites you are using and any unprotected messages.



The same risk is present when using a **Communications Network**. If your activity isn't secured, the sites you view and messages you send are visible to your phone company or Internet Service Provider (ISP).



The message **Service Provider** (for example, the app you're using to chat with your friends, or the website you're using). If your content isn't protected, that company can view it.



The **Network** is again a potential risk - as a message passes through the Internet or telecommunications infrastructure, it can be viewed by the machines and devices carrying it along its path.



The **Recipient's Router** may be monitored, just as the senders' may be.

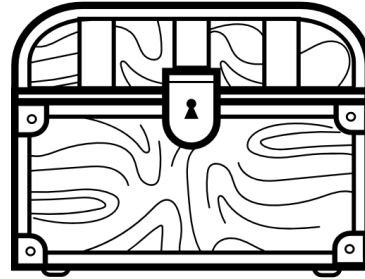


The **Recipient's Device** and all the apps and services on it

This means that **without any protection**, each stage represents a point where your messaging or browsing on the web might be viewed by bad actors. This is why it is important to use the right tools and follow the right practices to protect your messages and browsing history.

3.2. Encryption and Privacy

One useful safeguard throughout your message's journey is **encryption**. Encryption is the process of changing a message so that it cannot be read without knowing some secret method of interpretation.



It may be helpful to think of encryption as a chest with a lock on it. If you place your message in the box and lock it, the message can only be read by someone who has the right key. If you trust the strength of the lock, you can hand your chest to a delivery person and be reasonably confident that your message can only be viewed by people who have the key. If your message is encrypted well, it can safely pass through stages of the message's journey where there are untrustworthy actors. Encryption is a vital part of secure and private communication in the modern era.

3.2.1. SMS and Email

Today, many communication apps (and many websites) use some form of encryption. Notably, two common forms of communication - SMS messages and email - do not. Both SMS and email were designed decades ago, and have not changed much to meet the security challenges of the day. Sending a message through email or SMS is a little like sending a postcard; it can easily be read by anyone as it travels along its journey.

Illustrative Story

An investigative journalist has been writing a story about her country's leadership. She is about to break a story about the government's corrupt dealings. She sends the final draft of her story to her editor and waits to hear back. Hours later, she turns on the news to see a government official lambasting her media outlet. She's confused - he's quoting her story, which hasn't even been published yet. The only people who should have seen the draft are her and her editor. What has happened?

The journalist sent her story by email, which passes unencrypted through the Internet. Her company's internet service provider has a close relationship with the government, and has allowed the government to read all incoming and outgoing emails to the media outlet. To protect her messages, the journalist should have perhaps used a messaging service that used encryption.

If you have a sensitive message to send, you almost certainly should not be using either SMS or email to send it.

3.2.2. Types of Encryption

There are at least two categories for encryption: encryption **in-transit and at rest**, and **end to end** encryption.

3.2.2.1. Encryption In Transit and at Rest



If encrypting communication is like putting a chest in a box with the lock, sending a message through encryption in transit and at rest is like giving a key to the messenger carrying the box.

With this form of encryption, you *must trust the service provider* to protect your information.

Here are some services that provide this form of encryption as of autumn of 2020:

- Facebook messenger
- WeChat
- Skype
- Twitter DMs
- Slack

3.2.2.2. End-to-End Encryption



End-to-end (E2E) encryption only allows the recipients of the message to read it. Sending an end to end encrypted message is like handing a message box to a delivery person without providing a key. If a service truly uses end-to-end encryption, there is less risk that the service provider will abuse your information, because they lack the key to open it.

Services that employ end-to-end encryption are less vulnerable to government requests for information, because they are literally unable to access much of their user's content.

- WhatsApp
- Signal

- iMessage
- Telegram (in some cases)

Remember, even if a message is end-to-end encrypted, it is not necessarily invulnerable. If any device in a conversation is infected with a virus, or if the app in question has an unknown security flaw, or even if users are automatically backing up your messages in an unencrypted format, a message may be compromised. To reduce your risk, don't use software from unknown sources, and keep your phone and your apps up to date.

3.2.3. Metadata

Even if a message is encrypted, it is possible to discern quite a bit of information about a user by tracking *metadata*. Metadata is often described as "data about data". In the case of messages, metadata can include:

- **Who** is sending a message to whom
- **When** a message was sent, and how long messages were exchanged
- **Where** the messages were sent and received from,
- **What** devices were involved in the conversation.


Metadata can tell you a lot about what is being discussed, even if the content itself is encrypted.

Illustrative Story

A worker at a telecom company reviews the communication traffic of one of the company's customers. She finds that at 3pm on Wednesday, the customer received a phone call from a clinic that is known to provide testing services for sexually transmitted diseases. Immediately after receiving this call, the customer dialed the number of her spouse. Their conversation was short. Immediately after their call, the spouse contacted a number he previously only dialed late at night. The customer dialed a prominent divorce attorney. What can the worker guess about the content of these conversations?

Even without knowing the substance of any of these calls, the someone reviewing the metadata of a conversation may make reasonable inferences about the actors involved simply by knowing who was talking to whom, and in what sequence.

WhatsApp is a free messaging service with one of the largest user bases in the world. The app provides end-to-end encryption for all messages passed between users, meaning (presumably) WhatsApp can not view the content of messages sent. However, at the time of writing, WhatsApp retains metadata records of conversations, so it knows the communication networks of all its users. WhatsApp is owned by Facebook, a company whose business model relies on knowing as much as possible about its users, so many analysts believe that this information is somehow used by Facebook.



By contrast, the messaging app Signal keeps almost no metadata records about its users. The creators of Signal (a nonprofit) publicly boast that they are unable to respond to legal requests because they keep virtually no unencrypted data about their users.

3.2.4. Trusting a service provider

An important part of the choice to use an online tool is deciding how much to trust a service provider, and what you trust them to do.

Whenever selecting a service, ask yourself:

- Do I trust this service provider not to abuse my data?
- Do I trust this service provider to protect my data from others?

For example, Google offers an email service for free, but it scans the content of your emails in order to understand you better and deliver more relevant ads to you. If you are comfortable with this deal, you might place a lot of trust in Google, because it provides a number of security protections to defend its users. On the other hand, Google receives [hundreds of thousands of government requests for user information a year](#), and provides at least some user information for a majority of these requests. So, depending on your threat model, you might find yourself thinking carefully about what messages you send through Google, because Google may be compelled to provide information to authorities who use a legal request.

3.3. Apps for Communicating Securely

Below, we've listed a few of the most common apps for communication. Please note the following:

- These apps are constantly updating and this information may change. This guide was last updated in November, 2020.
- Be aware that not all apps listed below are allowed in all countries - know the laws in your state before adopting a tool.
- Remember, even messages that are encrypted can be read by an adversary under certain circumstances. These apps can help you communicate more securely, but you aren't invulnerable.

Name	1-on-1 End-to-End Encryption	Group Message End-To-End Encryption	Message Encryption at Rest	Message Encryption in Transit	Video End-To-End Encryption	Video Encryption in Transit
WhatsApp	Yes	Yes	Yes	Yes	Yes	Yes
Facebook	No	No	Yes	Yes	No	Yes
Skype	No	No	Yes	Yes	No	Yes
Telegram	Yes	No	Yes	Yes	No	No
Signal	Yes	Yes	Yes	Yes	Yes	Yes
Slack	No	No	Yes	Yes	No	Yes
Wire	Yes	Yes	Yes	Yes	Yes	Yes
WeChat	No	No	Yes	Yes	No	Yes

3.3.1. Encrypted Email

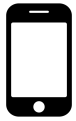
It is possible to send end-to-end encrypted emails. Some tools, like Mailvelope, Open PGP, or Protonmail allow the user to send end-to-end encrypted messages. Please note, even if the body of a message has been encrypted, the subject line and the attachments that accompany this message remain unencrypted.

3.3.2. Social Media

Unlike the methods listed above, social media tends to be a more public and less private form of communication. Many social media services offer “private” or “direct” messages, that might be treated as “encrypted in transit and at rest.” Depending on their threat model, users may be more or less comfortable with a private company being able to monitor the communications of their users. If privacy is desired, an end-to-end encrypted messaging app is probably a better solution.

4. Privacy in Browsing the Web

Browsing the Web anonymously can be very difficult to do. Most of us accept some level of visibility when going online - we accept, for example, that the website we log into knows who we are - but depending on our threat model we may decide that we need to take steps to prevent our traffic from being seen. As with sending a message, there are a number of stages where your activities on the Web can be observed.



On the **Browsing Device**, the websites a user visits and her actions on them may be viewed if the device has a virus or has given untrustworthy software too many permissions.



If the **Router** or WiFi network is accessed by another person, she could see the websites you are using, and even the content displayed by those websites, or the communication of sensitive information (such as passwords, or financial data).



The **telecom provider** or the **DNS provider** (the service that tells your computer where to go when you type in a url) knows what websites you are going to.



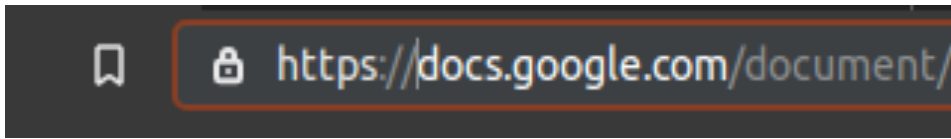
The **Website** you've visited knows what pages you're going to. If you've logged in, if you have identifying information stored in your browser that can be read by the website, or if the website simply recognizes the "fingerprint" of your computer's hardware and software, that behavior can be linked to a person.

Unless you have taken steps to hide it, most devices in this process will be aware of a user's IP address, and this can go a long way toward determining the location of the user itself. Using a VPN or TOR may hide your IP address from some actors, while revealing it to others. Your threat model can help you to determine what the right tools are for your situation.

4.1. Encryption Online

Many websites use encryption to provide privacy for their users. This encryption creates a "tunnel" through which the website and the user pass information. Say an ISP is monitoring the browsing behavior of a user -- if that user visits a website using encryption, the ISP will see the name of the website, but not the pages viewed or the information.

Users can tell if the website they visit uses encryption by looking in the URL bar of their browser. Most browsers will show an icon like the one below if the connection is secure, or say "not secure" if the website is unencrypted. Another way to check is by looking at the full URL of the website you visit. If the website begins with "https://", they are using encryption. If you only see "http://", the website is not encrypted. Never enter sensitive information into an unencrypted website - the information you send can be seen by all observers of your connection.



Browsers commonly communicate that a website is secure by putting a lock next to the URL.

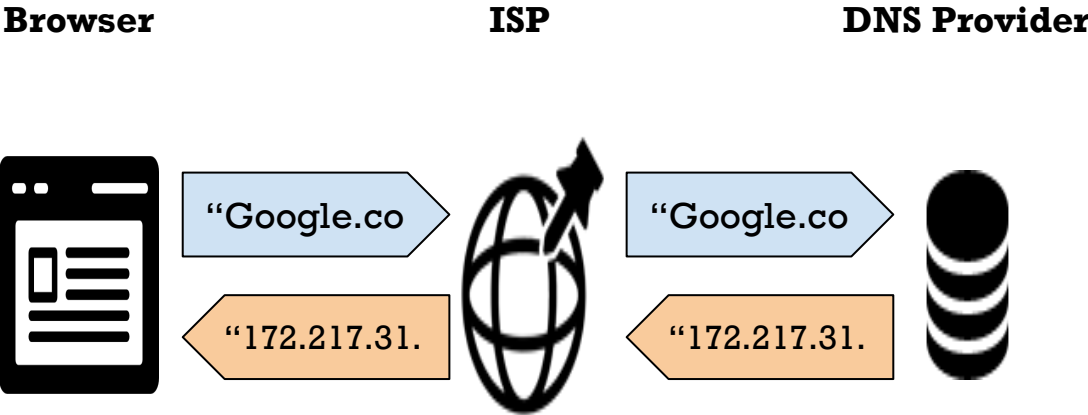
Websites usually obtain encryption “certificates” from other websites. These certificates expire after a certain amount of time, and unless they are immediately renewed, a visitor may receive a scary warning, like "There is a problem with this website's security certificate". If you see an error like this, don't proceed - it could be a sign that your connection is not secure.

Making sure that your browser is contacting a website securely is a challenge. Sometimes websites default to HTTP when they actually support HTTPS. The free browser extension [HTTPS Everywhere](#) helps to ensure that your browser insists on using HTTPS by default.

4.2. DNS and Privacy

Browsers navigate through lines of text called “IP addresses” that signify the identity and location of a machine on the Internet. While a computer is able to read address like “172.217.31.255” or “2c0f:fb50:4000:0:0:0:0” (both of them are occupied by Google services), humans have a hard time remembering these seemingly random collections of numbers and letters. That’s why “domain names” were invented; to give users a simple phrase like “google.com” to remember.

When a user types “google.com” into her browser, the browser goes to a Domain Name System, or a “DNS” provider, which keeps a record of website names and the IP addresses that are associated with them. A browser will ask for the IP address associated with a domain name, and will receive a string of letters and numbers it can use to find the correct website. With the IP address in hand, our browser can contact the machines running the website at “google.com” and show us the page.



What does this mean for user privacy? It means that for our browsers to find the websites we're looking for, at least two entities - the Internet Service Provider, and the Domain Name System provider, will know the websites we visit. (This may have implications for security, too - in some cases Internet companies may direct their customers to untrustworthy DNS providers, who in turn will send users to a fraudulent website.)

Tech savvy users can direct their routers to rely on a trusted DNS provider, but that might not be the easiest solution for most people. Instead, we'll talk about other tools everyone can use on their devices.

4.3. Cookies and Trackers

Whether it is Chrome, Firefox, Safari, or any number of popular browsers, the tool you use to browse the Web may store and share personal information in unexpected ways.

Often, this is for the convenience of the user. For example, once a user has selected their primary language for a website, they would like the website to remember that setting regardless of whether she is logged in to the service or not. To facilitate this, the browser stores a bit of information about the user - say, their language of preference - and recalls that information as a user is navigating around a given website.

Sometimes, however, browsers can remember information about us that we'd prefer not to be shared. Sometimes this information is shared across websites, and anyone with a broad enough view of the user's behavior - an advertiser, a person with access to user data from multiple websites, etc - will be able to learn about the user's browsing history or other sensitive details.

To address this, the user can often instruct the browser to actively delete information - sometimes called cookies - as she browses the web. Some free plugins and some browsers (shared later) can automatically perform this task or block known harmful cookies.


4.4. Incognito or "Private" Mode

Many browsers come with a "private" or "incognito" mode. What do they do?

Usually, these services mask user activity from *other users of the browser or computer*, **not** from people with access to the local network or actors at different stages of Internet browsing.

Here is how the Chrome browser describes its private mode:

"Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept. However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit."



Private modes are usually best for when you want your computer to forget your browsing history after you are finished using it, or when you want to log into your accounts from a trusted computer that you nevertheless want to forget your actions. Beyond this, private modes don't shield your online behavior from observers. To do that, you'll want to use other tools, like VPNs and Tor.

4.5. VPNs and Tor

Some services on the internet are designed to conceal the user's location and identity from the online website they are accessing and to circumvent blockages and restrictions on the Internet. These tools can be useful, but should also be used with caution, as they may reveal information about your online behavior to specific parties.

4.5.1. VPNs

Virtual Private Networks (VPNs) are machines that you ask to browse the web on your behalf.

Suppose I wanted to borrow a book from my local library but I was embarrassed by the topic or the genre. If I didn't want anyone in the library to know it was me that was borrowing the book, I might ask a trusted party to borrow the book and give it to me in the library parking lot. As far as the library knows it is in the possession of the person who walked in the door and checked it out, but in fact, the book is in my hands. The act of checking a book out through an intermediary is much like the process of using a VPN, and with similar advantages and risks.

When a user logs into a VPN, they are effectively asking another computer to visit websites and share the content of those pages with them. As far as the website being visited is concerned, the visitor who comes to their website is the machine in the VPN, not the user (as long as the user does not give themselves away by logging in to the website.) This can be very useful. If a country blocks all of its citizens from accessing a certain website, this restriction can be circumvented using a VPN. Moreover, connections with VPNs are usually encrypted, so that even observers of a person browsing the Internet using a VPN can only see that she is connected to the VPN service.

A few caveats:

- A VPN may mask your traffic from observers, but you won't be invisible. Observers will be able to tell you're using a VPN, and this may draw attention to you in unexpected ways.
- A VPN won't protect your machine if it is infected with a virus. If the device is compromised, a VPN won't prevent the device from tracking the user's behavior.
- Depending on your location, use of a VPN may or may not be legally permitted.
- As with borrowing a book through a third party, it is essential that you trust your VPN to protect your web activity.

This last point is critical. After all, by using a VPN, you are trusting a machine (and whomever has access to that machine) with your information. The same rules of caution about other services on the Internet apply with VPNs -- if you aren't paying for it, you likely are the product, and the service could be tracking and selling your information in some way. In particularly bad scenarios, VPNs can even be malicious. In 2020, one activist in Iraq reported that a free VPN was being shared by groups of Iraqis that was likely built by the government itself to monitor its citizens.



Source: hackread.com

VPNs may advertise themselves as “not tracking user logs,” but upon being audited (or hacked) some of these have been revealed to have been keeping detailed records of their users' behavior.

A good rule of thumb is to be extremely cautious with free VPNs developed by for-profit companies. You are better off using a VPN provided by a nonprofit or social enterprise, or use -- if possible -- a well-reviewed paid VPN.

Two options for Android devices are:



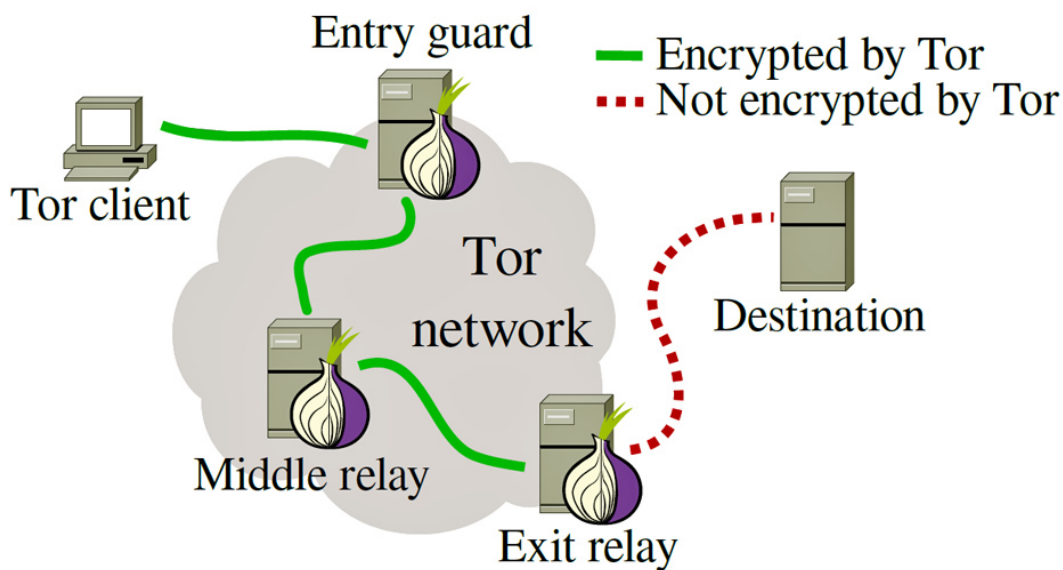
Orbot routes your phone's data connection through the Tor Network (described in more detail below).



Psiphon is a censorship circumvention tool run by a nonprofit that behaves like a VPN. It keeps logs about what users as a whole are doing with the service, but not individual data.

4.5.2. Tor

Tor is a free and open source method of accessing the Internet. It behaves similarly to a VPN in that the user connects to a machine online and their activities are routed through other machines. The difference between Tor and a standard VPN is that the user's traffic is bounced between *multiple* machines in a method designed to obscure the user's traffic. No single machine in the Tor network knows all the information about the user's behavior.



Source: fossbytes.com

Because the Tor network relies on passing information through a variety of machines, the speed of Tor is often much slower than an ordinary Internet connection. But for sending messages or accessing blocked websites, Tor can be a free and effective way to use the Internet safely. Over the years, Tor has become easier to access and use. The Tor Browser is available for free online and on mobile devices. It is even possible to use Tor inside some standard browsers; the Brave browser (which is described further below), for example, allows the user to open a private window with Tor.

Bear in mind:

- As with a VPN, someone monitoring your Internet connection may not be able to see the sites you visit, but they will see that you are using Tor. Depending on your environment, this may draw attention to you.
- Tor helps the user anonymize their behavior on the web. No solution is perfect, however - continue to use best security practices while browsing the web.

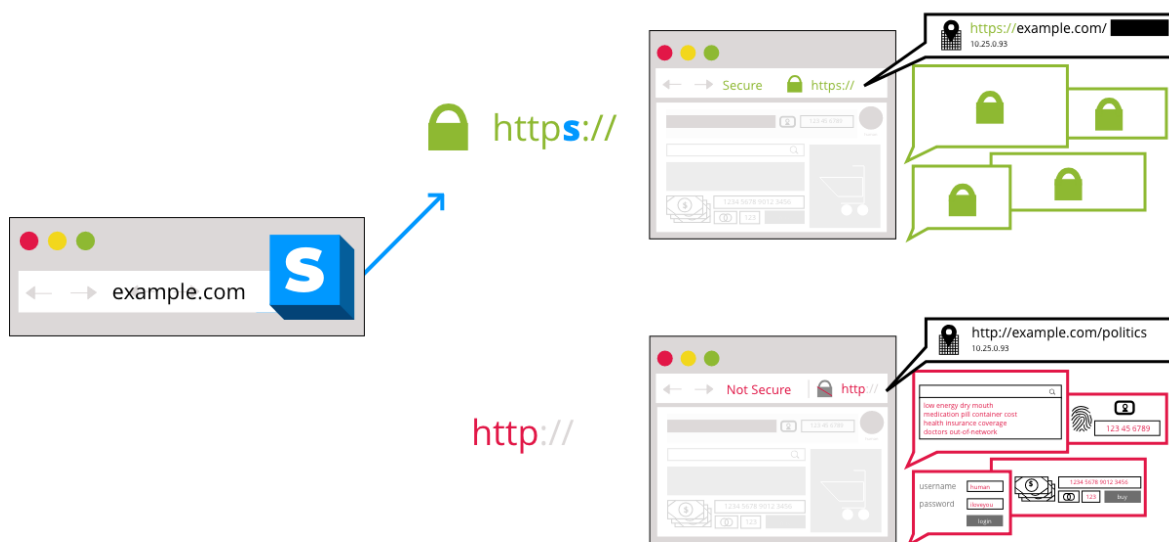
4.6. Plugins

Plugins are little applications that change the behavior of your web browser. Some browser plugins have been designed to help improve user privacy on the Internet. They won't protect your computer from viruses, but they may limit the amount of trackers observing behavior and ensure that your browser is encrypting your traffic.

The Electronic Frontier Foundation (EFF) is a nonprofit organization dedicated to Internet privacy, among other issues. To address the concerns listed above, here are two plugins developed by the EFF.

4.6.1. HTTPS Everywhere

It is now very common for websites to employ encryption to protect their users, especially if sensitive information is exchanged between the service and the browser. Some websites, however, offer only limited support for encryption, and either default to unencrypted pages or they link to encrypted versions of pages. HTTPS Everywhere improves privacy by making the browser ask for the most secure version of a site. The result of this is that someone monitoring your browser traffic can only see the domain of the website you visit, not the content the website is providing you.



Source: Electronic Frontier Foundation

At time of writing, HTTPS Everywhere is a plugin for Chrome, Firefox, Edge, and Opera. It is built into Brave and the Tor Browser.

4.6.2. Privacy Badger

Most websites online will load content from a number of different sources - a picture will load from one site, ads will load from another, and so on. Sometimes the content that is delivered from another source has trackers in it, as discussed previously. As the EFF describes below, the plugin helps protect you from sites that appear to be tracking you.



“If as you browse the web, the same source seems to be tracking your browser across different websites, then Privacy Badger springs into action, telling your browser not to load any more content from that source. And when your browser stops loading content from a source, that source can no longer track you. Voila!”

Privacy badger provides you with some privacy from the websites you visit, too - for example, Google and Facebook are normally able to track which links you click on when you visit their site. Privacy Badger replaces the links on these websites with links that go directly to the content, so Google and Facebook have less insight to what you click.

Privacy Badger runs on Chrome, Brave, Firefox, Edge, and Opera.

4.7. Browsers

Most mainstream browsers are “secure” in the sense that they are actively developed by people who resolve known security issues with the software. That being said, differences between browsers have some implications for user privacy. It is important to remember that browsers are just a part of a user’s suite of security tools, and security and privacy require that a user be cautious and careful when using the web. For the most part, browsers can’t stop you from downloading dangerous software, or exposing your information online in a social media post.



By far, the most popular browser at time of writing is Google’s **Chrome**. Not only is Chrome frequently installed on its own, but the open source version of Chrome forms the basis of Microsoft’s Edge and Brave. Chrome is fast and comes with many helpful extensions, including the two recommended by this document.

However, Chrome is a Google product, and by default, it collects a lot of information about the user’s online behavior so as to build a profile for ad delivery. You can disable much of Google’s data collection by changing the settings of your Google account, but the default setting of the browser is to collect as much information as possible. Also, Chrome does not block third-party and social trackers by default.



As mentioned above, **Brave** is built off the open source version of Chrome, but it makes some very different decisions about user data. Brave does not collect information about users, and by default it blocks third party trackers and ads. Brave has built in “HTTPS Everywhere”, and the user can use Tor in a private window. For users who want a private experience similar to Chrome, Brave can be an attractive option.



Firefox is an open source browser created by the nonprofit Mozilla. Like Brave, Firefox blocks third-party trackers by default, and the extensions recommended in this document can also be installed.



The **Tor** browser is built upon Firefox, with additional privacy protections by default, as well as an automatic connection to the Tor network for anonymous browsing. Among the browsers listed here, it provides the most protections for user privacy, at the cost of convenience. By its nature, Tor is a slow experience, and does not allow for as many customizations.

If you're worried about someone monitoring your activity, and you lack access to a good VPN, you may want to use Tor to access sensitive information. However, you should be careful about over-using a system built for extra security. One reason for this is that simply using Tor may cause a user to stand out in a crowd, causing him or her to be singled out or questioned. A second is that people have a tendency to scale back inconvenient security settings over the long term - installing extensions or signing into accounts for convenience that end up reducing user privacy. As with all tools, be aware of *why* you are using your browser and what the risks are for any given behavior.

4.8. Other Tips for Improving your Privacy On the Web

- Keep your device healthy with up-to-date software and anti-virus software. Always install updates for your device and software as quickly as possible.
- Don't install software from unverified sources - a free VPN or browser apk from outside the official store may be more than it appears.

5. Protecting Your Accounts

Although not directly a part of privacy online, making sure that you keep control of your online accounts is critical to protecting your communications and your information. This section will be about the threats your accounts may face online and the ways you might safeguard against them.

5.1. Account Attacks

Using services on the Internet means keeping track of a bewildering number of usernames and passwords. The following are several ways your accounts might be attacked.

5.1.1. Phishing

One of the most common ways an account might be attacked is through email, or other trusted communication apps. When a user receives a message seeking to trick them into exposing sensitive information (like a password) or downloading a dangerous malware program, it is called “phishing.”


Many phishing messages play on common human weaknesses in order to get the user to click or provide information. These weaknesses include:

- **Greed:** a foreign dignitary wants you to be the one to host his fortune until he can flee the country. Just send your bank account information, and you’ll be rich!
- **Fear:** your taxes returns were filed wrong! Click on a link to correct your information before the government comes to fine/arrest you!
- **Panic:** Your account has been detected doing something wrong and will be locked unless you act now!
- **Respect of Authority:** Your boss wants a sensitive file emailed quickly - don’t make her wait!

Even the most cautious digital security trainer can fall for these attacks. Unless we train ourselves otherwise, humans are likely to make quick (and mistaken) decisions when we find ourselves in the above scenarios. Learn to recognize when you’re feeling anxious or jumping into action quickly. Take a breath, and inspect the message closer. A second look might prevent you making a dangerous mistake.

Depending on the sophistication of the attack, the message can appear to come from a genuine source, or direct you to an apparently authentic page. Messages can have poor grammar and punctuation, or be perfectly composed. Messages can originate from an unfamiliar source, or appear to come from an address that looks like your boss. In short: any message you receive can be a phishing attack, so always be cautious.





[Having trouble logging in?](#)

*A fraudulent site that appears to be a perfect replica of a Paypal website - except for the web address.
Source: Ragtag "Preventing Phishing" Training*

Phishing attacks don't have to come from email - you can also receive fraudulent messages over SMS or by a trusted messenger. Just remember to check all your communications carefully, especially if they are asking you to:

- Provide an username/password/account
- Reply with valuable information
- Click on a link
- Open an attachment (Word, PDF, etc.) with malware

If you suspect a message is a phishing attack, do the following:

- Don't open the file, respond, or otherwise interact with the message more than you have to.
- If it's directing you to go to a website, navigate to the site on your own (don't trust the link they're sending you) to check to see if the message is authentic.
- If you know the supposed sender, send a message through a trusted second channel (a separate email, a WhatsApp message, etc) to confirm that they did send the first message.
- If you're receiving the message through a work account, forward it to your I.T. services.

If you work at an organization with a lot of internal communication, consider adopting a service other than email to send messages. Plenty of alternative tools like Slack, Teams, Skype, Wire, Mattermost, or other chat-based communication tools are harder to turn into a

vehicle for phishing attacks, because all the messages sent are coordinated by a single service.

5.1.2. Website Breaches

Scarcely a week goes by without a news story that some popular website has been attacked. Hackers will employ a variety of techniques to break into a website and extract sensitive information, which may include collections of usernames and passwords. These collections of usernames and passwords eventually leak onto the Internet, where they can be purchased and traded by all sorts of dangerous actors. Eventually this may mean that your user name and password can get into the hands of bad people through no fault of your own.

Breaches can be especially dangerous if the user affected repeats his or her username and password across the Internet. If that happens, an attacker who gets access to one username/password combination can gain access to any websites where that combo has been used.

Of course, once you know your password has been stolen, you should change your password on the website in question right away (most responsible websites will prompt you to do this once they are aware that you've been compromised). But what about your other accounts? The best defense against losing passwords through breaches is creating long, unique, random passwords for each one of your services. The best way to do this is to use a password manager, which we will discuss further on, but even a physical list of passwords (if you can secure it!) is a reasonable way to accomplish this. Remember, if every account you have on the internet uses a different password, the damage caused by a breach can be contained.

5.1.3. Surveillance and Malware, and other Issues

Finally, your account can be compromised through hostile software running on your machine, someone monitoring your internet traffic (or even looking over your shoulder as you type your password) or any number of other issues you may face as you navigate the Internet. Practicing common sense as you navigate links, installing only trusted software and visiting secure websites, using antivirus software and generally staying vigilant to danger is the best way you can protect your accounts as you use the Internet.

5.2. Two-Factor Authentication

But what happens if your password *does* get into the wrong hands? What if you accidentally log in to a fraudulent website or someone watching you watches as you log into your account? Is your account automatically lost?

Many online services -- particularly the ones that hold on to sensitive information, like banking, emails, and other communication services -- allow you to secure your account through a process called "Two-Factor Authentication" (2FA). 2FA requires a user logging in from an unfamiliar browser or device to go through a second check to help confirm the

identity of the user, usually asking them to use a personal device or a physical token that would be on their person. The process is like a last line of defense for your account. If you want to see a growing list of services that support two factor authentication, take a look at <https://twofactorauth.org/>.

Two-factor authentication comes in a variety of forms. In general, all forms of 2FA are a good extra layer of security for your account, but some are better than others.

5.2.1. SMS



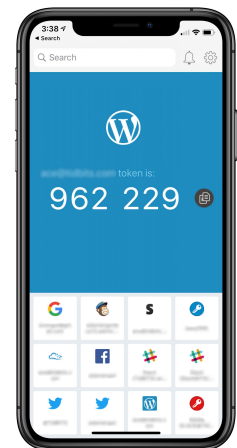
The first - and possibly most prevalent - form of 2FA is via SMS messages. With this method, the user registers a phone number to be contacted during log in. The SMS will contain a string of numbers that will be entered into the browser, and off you go!

While SMS-based 2FA is good, it is vulnerable to a sufficiently advanced attacker. For one thing, if the user is logging in to a very convincing fraudulent website, they may inadvertently share their 2FA code. (This is another reason to pay attention to the domain of the site you're visiting.) This method is also vulnerable to an attack called "SIM hacking", in which attackers convince the telecom company that you've switched numbers. Finally, SMS-based authentication isn't useful if you need to travel outside the country to a place where your number doesn't operate. So, while SMS is good, it isn't the best option available.

5.2.2. Apps

Authentication apps are another form of 2FA. To use app-based 2FA, the user downloads an app like Authy, or Duo, from the app store. The user links her app to an online service at the point of activating 2FA. Thereafter, whenever she must pass a 2FA check, she opens the app and looks for the numbers tied to the service. These numbers usually change every 30 seconds, so the user must be quick to enter them. (Image source: tidbits.com)

Unlike SMS, App-based 2FA doesn't rely on a communications network to send the user an authentication number, so the method is less vulnerable to being intercepted. On the other hand, it's still possible to phish a user who wields app-based 2FA, so the user still needs to be vigilant.



5.2.3. Physical Tokens

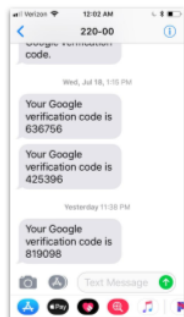


A third and very effective method of 2FA is token-based authentication. This method forgoes using the phone as an authentication method and instead uses a little electronic “key”, typically no larger than a USB thumbstick (most can even fit on a keychain). Instead of entering a code, the user inserts the token into their device where it is read by the browser.

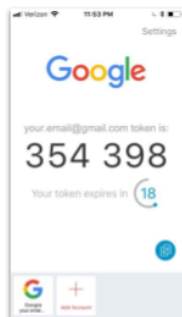
(Image source: Yubico.com)

Unlike SMS and app-based verification, a physical token is very resistant to phishing. Where possible, a physical token is the current preferred 2FA method.

Which method to choose? As the visual below describes, a physical token is the most preferred 2FA option, followed by a 2FA app, and then SMS. It is likely, however, that a user will need to employ all three options across the Internet. Some services only support one form of 2FA; others will allow a user to employ multiple methods. Use the most secure option available.



SMS/Text



2FA App



Security Key



Source: Ragtag’s “Setting up 2FA Social Media”

5.3. Password Managers

For better or for worse, the primary way we safeguard our accounts online is through a password. The best passwords are:

- Long (12+ characters in length)

- Random (do not follow a predictable pattern and are not made up of obvious words)
- Unique (not repeated in multiple services.)

Unfortunately, the human brain is usually not too good at remembering long strings of random letters and numbers. Many of us rely on dozens of services around the net, and sometimes find ourselves repeating the same password over and over. This can lead to vulnerabilities if a password is discovered.

One solution to this problem is a password manager. In its simplest form, a password manager is a program that remembers username and password combinations for websites. Most modern browsers now offer to remember login details for the user. Companies have also created more complex tools, which help to generate the random passwords, tag and group them for use, and share them securely with trusted contacts.

Password managers are part of a good defense against phishing, too. Unlike a human, a password manager is not easily fooled by a fraudulent website if it is found at the wrong web address. This means that most managers will not offer to fill in the password manager. If a password manager refuses to provide the login details for a site, consider it a signal to be cautious.

There are plenty of free and cheap password managers. Most browsers serve the job fine. If more benefits are needed, such as the option to use the password manager as an app, the user can try a free tool such as 1Password or LastPass.

6. Additional Resources

6.1. Guides

For more guidance on processes and ways to keep safe online, look at these options.

- **Tactical Tech:**
<https://tacticaltech.org/projects>
- a number of important guides about data and digital security
- **Privacy International:**
<https://www.privacyinternational.org/learn>
features a collection of articles about the various ways citizens may be surveilled in the modern world
- **Ragatag:**
<https://helpdesk.ragtag.org/hc/en-us/categories/360000940571-Digital-Security>
- a number of tutorials focusing on two-factor authentication and phishing.
- **Internews:**
<https://safetag.org/>
- a guide for conducting a security audit of your organization (use this with a professional.)

6.2. Tools

Please review the relevant sections of this guide before using these tools.

6.2.1. Browsers

The following are browsers with features designed to enhance privacy.

- Brave Browser: <https://brave.com/download/>
- Tor Browser: <https://www.torproject.org/download/>

6.2.2. Password Managers

Password managers generate and remember long, random, and unique passwords so you don't have to.

- 1Password: <https://1password.com/>
- LastPass: <https://www.lastpass.com/>

6.2.3. Two-Factor Authentication Tools

2FA tools provide a second layer of verification for your accounts.

- Authy: <https://authy.com/>
- Duo: <https://duo.com/>
- Yubico: <https://www.yubico.com/>

6.2.4. VPNs

VPNs encrypt your device's data connections and help circumvent censorship. (The tools listed here are open source and provided by a nonprofit.)

- Orbot: <https://guardianproject.info/apps/org.torproject.android/>
- Psiphon: <https://www.psiphon3.com/en/index.html>

6.3. Interesting Links

Digital Civil Society Lab (Stanford university)

<https://pacscenter.stanford.edu/research/digital-civil-society-lab/>

What is social engineering? <https://www.imperva.com/learn/application-security/social-engineering-attack/>

Threat intelligence in cybersecurity

<https://www.eccouncil.org/cyber-threat-intelligence/>

Threat modeling explained: A process for anticipating cyber attacks

<https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html>

Threat Modeling Cheat Sheet

<https://cheatsheetseries.owasp.org/cheatsheets/Threat Modeling Cheat Sheet.html>

Building resilient systems to keep civil society safe online

<https://digiresilience.org/>

Hannah Sabata, dumbest criminal by far:

<https://qr.ae/pNSMna>

7. Conclusion

Security threats are constantly evolving.

We hope the information contained in this guide will help users keep their communication and browsing activity on the Internet private and secure. We've covered some general tools and practices, but to find guidance for your specific context we urge you to speak with a digital security trainer who knows your situation and can guide you through the complicated elements of digital privacy and security.