ENCRYPTION, PRIVACY, AND ONLINE SECURITY
Terra Ventures – 2023
v1.1

Introduction

As Terra Ventures extends its global reach, a growing number of our team members are embracing opportunities to live and work in remote regions worldwide. These voluntary assignments enable them to serve local communities, deepen their cultural understanding, and enrich our collective knowledge. However, these unique circumstances also necessitate the secure management of sensitive personal and corporate information across international borders.

With the advent of the digital age, tasks such as online banking, completing government forms, managing official employment matters, and other personal transactions have become increasingly streamlined yet, they also open avenues for potential security breaches. Moreover, the responsibility of handling Terra Ventures' intellectual property adds another layer to the importance of safeguarding data.

This guide aims to equip our international volunteers with the essential knowledge and tools to identify potential digital threats, understand the role of encryption in ensuring privacy, use advanced techniques to secure communications, and make informed decisions about applications and services that prioritize online security. With these resources, our global team members can confidently and securely conduct their online activities, ensuring the integrity of both their personal transactions and Terra Ventures' intellectual property.

This guide is split into five parts:

Part I: Understanding Privacy and Security Threats
Part II: The Role of Encryption in Ensuring Privacy
Part III: Virtual Private Networks (VPN) - Enhancing Online Security and Privacy
Part IV: More-Secure Security Techniques
Part V: Recommended Applications and Services

Part I: Understanding Privacy and Security Threats

Cyber Threats and Online Intrusions

Every day, individuals and corporations fall victim to cyber threats. These threats include phishing, malware, ransomware, and man-in-the-middle attacks, among others. Such attacks often aim to access sensitive personal information, financial data, or corporate secrets. Cybercriminals might use this data for their personal gain, to damage reputations, or to gain unauthorized access to systems.

Data Harvesting and Tracking

Even if you are not the direct target of a cyber attack, your personal data might still be at risk. Numerous online platforms and services collect a wealth of information about their users, often without explicit consent. This data can include browsing habits, location data, purchase history, and even the content of personal communications.

Part II: The Role of Encryption in Ensuring Privacy

Encryption transforms readable data (plaintext) into a coded form (ciphertext) that can only be read or processed after it has been decrypted. Encryption plays a crucial role in maintaining data privacy in various contexts, from internet browsing to mobile communications.

When we say plaintext, we mean readable; this applies to any digital content including documents, music, photos, etc. Our goal is to protect all our sensitive information from any unauthorized access.

Encrypted data can only be read by decrypting it first, this requires the encryption/decryption **keys**. What those keys look like – and more importantly, who holds those keys – are very important concepts that we hope you get an intuitive understanding of. For now, we'll just think of a *key* as synonymous with *password*.

When discussing encryption, we will focus on understanding the distinction between symmetric and asymmetric cryptography:

Symmetric Key Cryptography

Imagine you have a box that you want to send to a friend. You lock this box using a key, and your friend needs the exact same key to open it. This is the basic idea behind symmetric key cryptography.

In the digital world, this 'key' is a shared secret between two parties - the sender and the receiver. When sending a message, the sender uses this key to convert the readable data into a coded format, or encrypt it. Upon receiving the encrypted message, the receiver uses the *same key* to decrypt it back into its original form. While this method is relatively fast and efficient, its security depends on the safe exchange of the key between the sender and receiver. If someone intercepts this key during its exchange, they can decode the entire conversation.

Asymmetric Key Cryptography

Now, let's modify our box analogy a bit. Instead of one key, you now have two keys - one to lock the box and another to unlock it. You keep the unlocking key (private key) safe with you and distribute copies of the locking key (public key) to anyone who wants to send you a secure box. Now, anyone can send you a locked box, but only you can unlock it.

In digital communication, this is asymmetric key cryptography. It involves a pair of keys - a public key known to everyone and a private key known only to the recipient of the message. This makes it more secure than symmetric key cryptography, as even if someone gets hold of the public key, they cannot decrypt the message, as that requires the private key.

Applying it to Online Communications

When you communicate with a website, it's akin to sending a locked box (your data) through the internet. Secure websites use a form of asymmetric cryptography called SSL/TLS to ensure that your data reaches them securely. This is often called end-to-end encryption.

However, it is unfortunately not that simple. For starters, there are several technical steps that need to take place for your device (laptop, phone, etc) to acquire a website's public key and those steps can be compromised and attacked by bad actors. We'll describe some of these techniques and the easy ways to minimize or eliminate the risks they introduce in later sections. But for now, let's address this question: what happens to your data (the contents of the box) once it's with the website?

This greatly depends on the website's data handling policies AND what technical steps and technologies they put in place to enact those policies. They might store your data as is, or they could further encrypt it using symmetric or asymmetric encryption for added security. Unfortunately, as users, we have little control over or knowledge of these practices unless explicitly mentioned in the website's privacy policy, but we can make some educated assumptions.

Can (i.e. do you expect) the website/application/platform (or people operating it) read the content you communicated to or through their servers? If the answer is yes, we say that "we do not hold the keys".

This is a very important to understand. To ensure privacy, we must ensure that we hold the keys to unlock the box.

A simple practical example:

Say Alice has a Gmail account, and say she wanted to send an email to her friend Bob who has a Hotmail account.

1. *Alice logs in to Gmail with her personal password. Her connection to Gmail is end-to-end encrypted and only* ***Alice and Gmail*** *can see her password.*

2. *Alice drafts an email and sends it to Bob. The email is actually sent to Gmail with the note that the final recipient is Bob. Alice's connection to Gmail is still end-to-end encrypted, only* ***Alice and Gmail*** *can read the content of the Alice's email to Bob.*

3. *Gmail sends the email to Hotmail with a note that the final recipient is Bob. Gmail's connection to Hotmail is end-to-end encrypted, only* ***Gmail and Hotmail*** *can read the contents of Alice's email to Bob.*

4. *Finally, Hotmail delivers the email to Bob's inbox. When Bob logs in to read his email, his connection to Hotmail is end-to-end encrypted, and only* ***Bob and Hotmail*** *can read Alice's email to him.*

This quick example demonstrates what happens when we do not *hold the keys*. Alice's email to Bob is readable by at least two third parties, Gmail and Hotmail. Furthermore, there could be any number of additional third parties that are involved in the sending and receiving of the email for any number of business or legal purposes. While each step along the way was end-to-end encrypted, the entire operation was not.
This is applicable to most email providers, as ***e-email is an inherently insecure communication protocol.***

In summary, understanding symmetric and asymmetric key cryptography is critical to navigating the digital landscape. It is equally important to be aware of how and where we share our data online, bearing in mind that our control over it often ends once it reaches its destination.

Staying Secure and Private in Online Communication

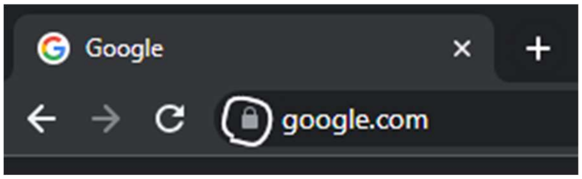
HTTPS: Ensuring Secure Web Browsing

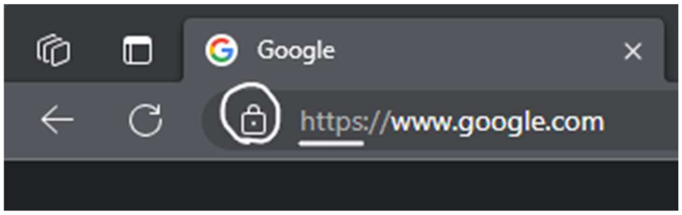
You may have noticed that some website addresses begin with '**https://**' while others begin with '**http://**'. That additional 's' plays a pivotal role in your online security. It stands for 'Secure', indicating that the website is using a protocol known as HTTPS (Hyper Text Transfer Protocol Secure).

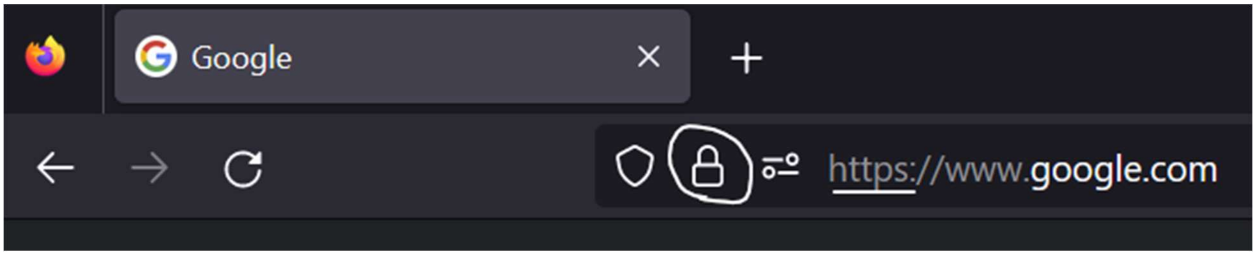
HTTPS establishes an end-to-end encrypted connection between your browser and the website, preventing anyone from intercepting or tampering with the data you exchange with the website. This becomes particularly important when entering sensitive information like passwords or credit card numbers.

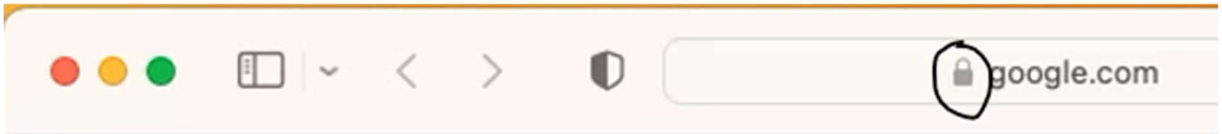
Identifying a Secure Connection

Most modern browsers make it straightforward to identify whether you're browsing over HTTPS. When visiting a website, look at the address bar at the top of the browser, here are some examples of how it might look when you're connected to a website securely:



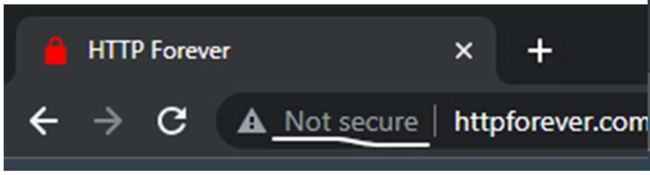


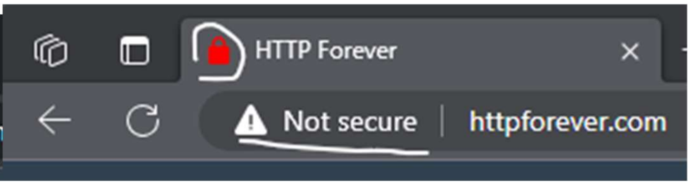


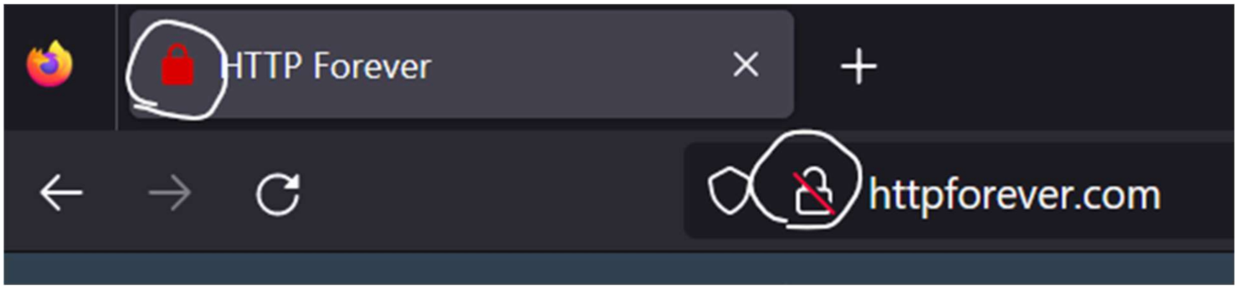


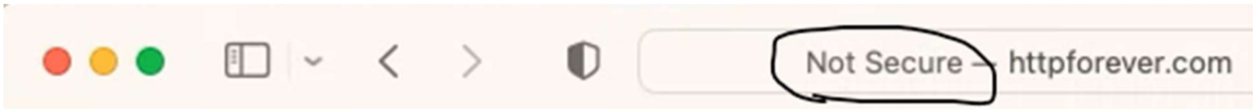
and here is how might look like when you're ***not*** connected to a website securely:

Do note that the provided example is of a website that does not offer any encryption. It loads correctly and looks like a normal website, the only indication that it doesn't offer any encryption is that your browser shows you a red lock icon or the words "not secure."



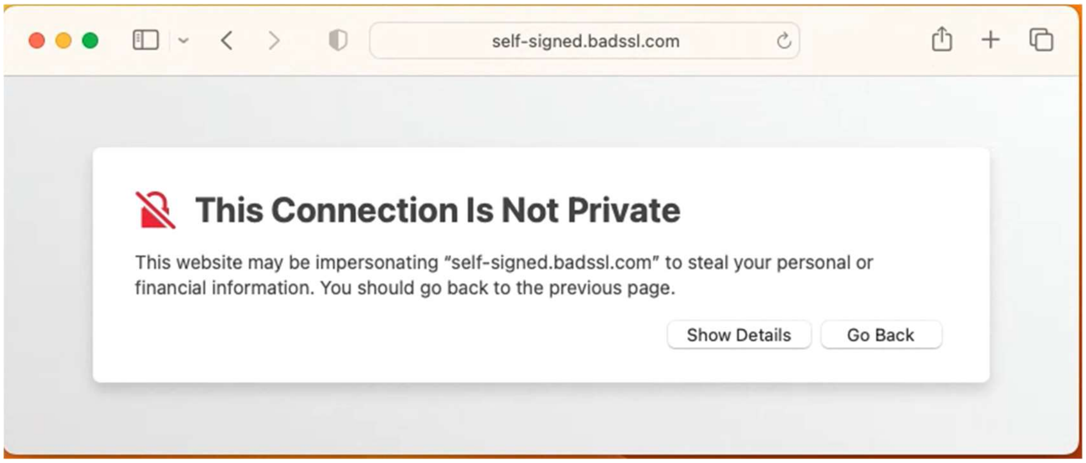






Unlike a website with a broken encryption implementation, your browser does not attempt to stop you from accessing these sites. NEVER input sensitive information into a website without proper HTTPS implementation (refer to Identifying a Secure Connection).

Finally, when a website does have a broken encryption implementation, your browser will attempt to prevent you from accessing it. Unless you fully understand the implications and accept the risk, do not override this block when it occurs. This is what that might look like:



This Connection Is Not Private

This website may be impersonating "self-signed.badssl.com" to steal your personal or financial information. You should go back to the previous page.

Navigating Directly to HTTPS

For optimal security, it's advisable to navigate directly to the HTTPS version of a website whenever possible. Typing 'https://' before the website address in your browser can help ensure this. This approach is crucial to eliminating the risk of man-in-the-middle (MITM) attacks, where attackers can intercept your data if it's transmitted over an unsecured HTTP connection before being redirected to HTTPS.

Many browsers and extensions automatically redirect you to the HTTPS version of a website if it's available. Nevertheless, manually navigating to HTTPS helps provide an additional layer of certainty.

Remember, while HTTPS does a great job of securing the connection between your browser and the website, it doesn't control how your data is handled once it's received by the website. Therefore, it's crucial to be mindful of the type of information you share online, even on HTTPS sites.

MITM

To intuitively grasp the concept of a Man-in-the-Middle (MITM) attack, let's imagine this scenario: You're mailing a private letter to a friend. You drop it in the mailbox, expecting the mail carrier to deliver it. But instead, someone intercepts the letter in transit, reads its contents, and then reseals and sends it on its way. Your friend receives the letter none the wiser, but your private conversation has been compromised. This is essentially how a MITM attack works in the digital world.

In the context of online communication, a MITM attack happens when an unauthorized third party intercepts the communication between two parties (for example, between your computer and a website) without either party realizing it. This could allow the attacker to eavesdrop on, manipulate, or steal the data being transmitted.

When you type a website address into your browser without specifying the protocol (like 'http://' or 'https://'), some browsers will still default to using the less secure HTTP to try to establish the initial connection. If the website uses HTTPS for a secure connection, it will respond back to your browser to switch from the unsecured HTTP to the secure HTTPS. This switch is known as a redirect.

During the brief period of initial connection over HTTP, a MITM attacker could potentially intercept the data being transmitted. A more sophisticated version of this attack relies on the victim connecting to the attacker's specially designed WiFi hotspot, which maintains an HTTP connection with your computer and maintains a separate HTTPS connection with the website you're trying to reach. By doing so, not only can the attacker read all information you send to the website, but they can manipulate it. Going back to our letters in the mail analogy, this is akin to the attacker installing a special portal inside your mailbox where they can open all your outgoing mail, read and edit its content, and reseal it before it gets delivered without anyone knowing what just happened.

In addition to being vigilant and never transmitting data to an insecure website, this is where a secure VPN can add a much needed additional layer of security and privacy.

It is crucial to always make sure that you are connected to VPN when conducting online business that you want to keep private, especially when using public internet services (e.g. public WiFi hotspot at local coffee shop).

Part III: Virtual Private Networks (VPN) - Enhancing Online Security and Privacy

Virtual Private Network (VPNs) employ end-to-end encryption technologies to create a private connection on top of a less secure network, such as the Internet. For our purposes, VPNs are used to ensure our online activities cannot be snooped on by unauthorized parties.

The Purpose of a VPN

Imagine driving a car through a bustling city, with numerous eyes watching your every move. Now, picture that car inside a private, invisible tunnel, moving undetected through the same city. That's essentially the role of a VPN in the digital world.

A VPN works by creating a private, encrypted 'tunnel' between your device and the Internet. This tunnel cloaks your online activities, making them unreadable to anyone who might be trying to view or intercept your data.

What a VPN Hides and From Whom

By establishing this encrypted tunnel, a VPN can effectively hide your:

1. **IP Address:** An IP address is a unique identifier for your device on the internet, somewhat like your home address. By hiding your IP address, a VPN can obscure your digital identity and location.
2. **Online Activities:** A VPN encrypts the data your device sends and receives over the internet, making your online activities unreadable to external parties.

This privacy can protect you from various threats, including cybercriminals attempting to steal sensitive information, ISPs tracking your online activities, or third-party websites logging your digital behavior.

Your IP address and online activity are NOT hidden from the VPN provider. A secure VPN can eliminate the risk of the man-in-the-middle attack described in the previous section, but the VPN provider can conduct their own man-in-the-middle attack.

As an example, let's say you are making a purchase of a product from example.com for $100, here is what an eavesdropper on the network can observe:

http://example.com	https://example.com	https://example.com over VPN
1. browsed to example.com 2. clicked on link to product at example.com/X 3. added product X to shopping cart, then viewed it at example.com/cart 4. Paid $100 with credit card with number xxxx-xxxx-xxxx-xxxx 5. Viewed receipt at example.com/receipt (including content of receipt)	1. browsed to example.com 2. clicked on link to product at example.com/X 3. Browsed to example.com/cart {observer can't see that you added product to cart, but can make a safe assumption that product X was added to shopping cart} 4. Browsed to example.com/receipt {observer can't see that you bought product X or how you paid, but can make a safe assumption that after visiting the product page and then the receipt page, you probably purchased product X}	1. connected to VPN That’s it. That's all an observer is able to see, since even web requests are encrypted end-to end over VPN, observer can't see any websites you attempt to access, or make any assumptions about what you did on said websites*.

* The VPN operator can make the same observations as going directly to https://example.com.

It is crucial to understand that a VPN isn't a silver bullet for online privacy. It primarily protects your data in transit, but it doesn't control how websites or online services handle your data once they receive it.

The Importance of Vigilance with VPNs

While a VPN can provide a significant boost to your online privacy, it doesn't absolve the need for careful online practices. Remember, the VPN provider itself could potentially see your online activities, making it vital to choose a reputable provider that respects user privacy.

Furthermore, a VPN can't prevent phishing attacks or stop malware from being downloaded onto your device. As such, you must continue to exercise caution, such as avoiding suspicious email links and keeping your devices and applications updated.

Even while connected to a VPN, it's critical to:

- Use secure, encrypted connections (HTTPS) whenever possible.
- Keep your device's software, apps, and antivirus protections up to date.
- Be wary of suspicious links and attachments in emails or other communications.
- Use strong, unique passwords for your online accounts.

Choosing a VPN Provider

It's important to recognize that while a VPN hides your activity from the public network you're on (or your ISP), your VPN provider can see your activity clearly. It's very important to choose a VPN from a trusted provider. The most important factors to look out for when choosing a VPN provider are:

- Do they keep access logs?
    - Using a VPN to protect your privacy is pointless if everything you do is stored into neat logs. The VPN providers we trust do not keep any logs.
- Do they use a modern and secure tunneling protocol?
    - Avoid VPN services that only support PPTP.
- Where are they based?
    - Are they based where the government of your place of residence has jurisdiction?
    - Are they based in the "Five Eyes"? (Australia, Canada, New Zealand, and the United States of America). countries These are bound by the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.
    - Are they based in the "Nine Eyes", consisting of the Five Eyes plus Denmark, France, the Netherlands, and Norway?
    - Are they based in the "Fourteen Eyes", consisting of the same countries as the Nine Eyes plus Germany, Belgium, Italy, Spain, and Sweden?
- Other considerations:
    - How many servers do they have? Do they have servers physically near you? The closer you are physically to the server, the faster your connections will be.
    - Do they have bandwidth limits?
    - Do they throttle speeds for any reason?
    - How many concurrent connections can you make? Can you secure all your devices?

Recommended VPN Providers

We periodically assess the most popular VPN services and keep this list of recommended providers. This list is updated as of July 25, 2023.

Every Terra Ventures employee is provided with 10 active VPN connections to protect their online privacy. As of July 25, 2023, our official VPN provider is ProtonVPN.

ProtonVPN

- They keep no logs.
- Based in Switzerland; no jurisdiction in 5 Eyes, 9 Eyes, or 14 Eyes countries, can't be compelled to produce any logs.
- Modern secure protocols
- Open source and audited client applications
- Reliable Internet kill switch

Other recommended Providers that meet the primary requirements for privacy and offer consistently solid performance:

Mozilla VPN (https://www.mozilla.org/en-US/products/vpn/)

- They don't keep logs.
- Modern secure protocols
- Provided by the Mozilla Foundation
- Can they be trusted? It's complicated, but we generally trust them.
  - Mozilla Foundation is based in the United States (Five Eyes) which normally would be a big red flag, but the Mozilla Foundation is a well-established and respected leader in and has a proven track record of protecting and advocating for users' online privacy and security.

NordVPN (https://nordvpn.com/)

- They keep no logs.
- Based in Panama; can't be compelled to produce any logs.
- Modern secure protocols
- Internet kill switch – our experience with Nord's kill switch was mixed, use with caution.

ExpressVPN (https://www.expressvpn.com/)

- They keep no logs.
- Based in British Virgin Islands; can't be compelled to produce any logs.
- Internet kill switch

Part IV: More-Secure Security Techniques

Passwords: Current Practices and the Path Ahead

Passwords have been the primary keys to the gates guarding our online identities and information. In the realm of cybersecurity, the world is gradually moving towards a future with fewer – and eventually no – passwords. Despite this, while they continue to be a part of our online lives, it's crucial to adhere to sound security practices to ensure their effectiveness.

The Evolving Role of Passwords

As cybersecurity evolves, there's a growing shift towards more user-friendly and secure alternatives to passwords, such as biometric authentication (fingerprint or facial recognition) and hardware tokens. This shift is driven by the inherent weaknesses of passwords - they can be easily guessed, forgotten, or stolen, making them a vulnerable point in our online security.

However, until these newer authentication methods become universally adopted, passwords remain an essential element of our digital lives.

Ensuring Password Security

Adopting robust password practices can substantially mitigate the risks associated with password-based authentication.

Unique Passwords

The most common way an attacker gains access to an important online account (GMail, banking, etc) is not by defeating the security of the account itself, but by trying the same password that was used on compromised 3rd party. It's important to use unique passwords for all your accounts.

Remembering a unique password for each online account you may have can prove very challenging. For that reason, we recommend the use of a password manager.

Remember asymmetric encryption and the importance of holding the keys? This applies to password managers as well. In the context of password management, we refer to secure password management services that allow us to control the encryption keys as **zero-knowledge**. That is, the provider and operator of the password management software has zero knowledge about the content of the password vault.

A text document or a spreadsheet is not a secure way to store your passwords!

There are two forms of password management software, local and cloud.

1. Local Password Management

   Local password managers store your passwords in an encrypted file that is saved locally on your device, giving you complete control over how your encrypted data is stored.
   When handled properly, this can be the most secure way to store your data, but it can be

inconvenient to use.
If you’re looking for an offline zero-knowledge password management solution, we recommend **KeePass** (https://keepass.info/).

2. Cloud Password Management

   Cloud password managers store your passwords in an encrypted file that is saved on the provider’s servers. This file is synchronized to your local device and decrypted on your local device when you authenticate with your private key (password). They are more convenient than local password managers, but they require an active internet connection to access your passwords on any new device. Additionally, it is wise to frequently export your vault and back it up.
   If you’re looking for a cloud password management solution, we recommend **BitWarden** (https://bitwarden.com/).

Strong Passwords

When possible, use a long, complex, and randomly generated password that is stored in your password manager.
When you need to create a password that you need to memorize (a password you may need to manually type often, the password to access your password manager, for example), be sure to adhere to these general guidelines:

- Don’t use personally identifiable information.
  Birthdays, anniversary dates, pet or loved ones' names are all terrible ideas for passwords. So are favorite quotes, famous names, or any piece of information that can be easily guessed by knowing you or talking to you.
  Your password should be chosen randomly, it should not reflect your thoughts or feelings.
- Entropy matters!
  A long, memorable password is significantly more secure than a short incomprehensible password.
  Your memorized passwords should be impossible to guess, but very easy to remember. We call those pass phrases.

  Consider the two passwords "yM&Lqg4?S" and "atone long pod wordy calve".
  You may assume "yM&Lqg4?S" is the more secure password, in fact, the second password would fail most "password strength" tests for not containing numbers or special characters; but in reality, the first password is more difficult for us to memorize, and far easier for a computer to guess.

  Choose a passphrase that's easy to remember, sufficiently long, and optionally introduce easy-to-remember typos or letter substitutions to make it more difficult for a computer to guess.

Multi Factor Authentication

Multi Factor Authentication (MFA) or Two-Factor Authentication (2FA) is an additional layer of securing access to your secured resources. It operates on the principle of requiring two different types of identification to verify your identity, thereby making it more difficult for an unauthorized person to access your information.

The "factors" in MFA typically include something you know (like a password), something you have (like a physical token or your smartphone), and/or something you are (like a fingerprint or other biometric trait). Your password maybe easily compromised by a remote attacker, but they cannot access your data without your second authentication factor.

Here's why MFA is crucial:

1. **Enhanced Security:** MFA makes it significantly harder for attackers to access your online accounts. Even if someone manages to guess or steal your password, they would still need the second factor (like the unique code sent to your phone) to breach your account.
2. **Prevent Unauthorized Access:** If an attacker attempts to access your account, the MFA process would notify you via the second factor (for instance, a notification on your phone). This gives you an immediate alert of the attempted breach, allowing you to take necessary actions like changing your password.
3. **Protection Against Phishing:** Phishing attacks often trick users into providing their passwords. With 2FA, even if you mistakenly give your password to an attacker, they would still need the second factor to access your account, offering an additional safeguard against such attacks.

Whenever available, enable and use MFA for your accounts and devices.

Part V: Recommended Applications and Services

These are applications and services that have been vetted and verified by our team. The first recommendation in each category is our preferred choice, but all options listed here are approved for use while conducting official Terra Ventures business.
This list includes applications and services already mentioned in previous sections. This list has been updated on July 25, 2023.

E-Mail

As discussed previously, email is an inherently insecure means of communication. For secure e-mail communication, we recommend **ProtonMail** (https://proton.me/). Keep in mind:

1. ProtonMail emails are end-to-end encrypted *if and only if* both sender and receiver (the two ends) are ProtonMail inboxes.
2. Any email sent to or from another e-mail provider is not end-to-end encrypted.

Instant Messaging

The Signal messaging protocol employs Perfect Forward Secrecy, and when implemented properly, it is the most secure way to privately send messages. Keep in mind that once the messages are decrypted by the messaging application, they sit on the receiver's device unencrypted.
For secure messaging, we recommend:

- **Signal Private Messenger**
  (Android: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms,
  iOS: https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8)
- **WhatsApp**
  (Android: https://play.google.com/store/apps/details?id=com.whatsapp,
  iOS: https://itunes.apple.com/us/app/whatsapp-messenger/id310633997?mt=8)

VPNs

- **ProtonVPN** (https://protonvpn.com/).
- **Mozilla VPN** (https://www.mozilla.org/en-US/products/vpn/).
- **NordVPN** (https://nordvpn.com/).
- **ExpressVPN** (https://www.expressvpn.com/).

Password Managers

- **BitWarden** (https://bitwarden.com/).
- **KeePass** (https://keepass.info/).

File Encryption

- **Gpg4Win** (https://www.gpg4win.org/) for windows.