ZibaSec Awareness Training

Authentication

Authentication is the process of verifying identity. In the context of users, it is the process of establishing the identity of a person. There are different ways to accomplish this (some better than others). Attackers have developed many techniques to attack authentication, and we need to adapt and adopt new approaches to protect our accounts.

Usernames and Passwords

The oldest (and most well-known) approach to digital authentication is the use of usernames and passwords. Users need to provide their username (usually not considered a secret) and their password (which **should** be considered a secret) to authenticate to a system or service.

The problem with this approach is that humans have difficulty thinking up passwords that are hard for a computer to guess and have a hard time remembering multiple, more secure passwords. Because of these human weaknesses, passwords are usually easy to guess and reused. Attackers can take advantage of both of these human weaknesses. == Brute Force Attacks Computers enable the automation of menial tasks, and attackers have developed tools and techniques to use computers to attack passwords. Over time, attackers have built lists of common-used passwords. They can use computers to try different usernames and password combinations automatically. Whether they do it against live systems or against hashed (a form of one-way encryption) values taken from a system/service, they are usually successful in cracking at least a small number of accounts with minimal manual effort.

Credential Stuffing Attacks

Because people have difficulty remembering multiple passwords, they usually cope with this by reusing their credentials. Once an attacker has cracked a user's account on one system/service, they have a high probability of success by trying the same credentials against other services. The practice of reusing credentials means that an attacker can compromise multiple accounts through a single account's compromise.

IMPORTANT

IMPORTANT: Mitigating Credential Stuffing Attacks

The best way to mitigate a credential stuffing attack is to use unique passwords for every account.

This way, if your online game account password is compromised, your bank account is still secure.

Password Best Practices

To overcome these weaknesses in human-generated and remembered credentials, we recommend the following approaches when using usernames and passwords:

- Use a password manager to remember your passwords (making it easier to use different

passwords for each account).

- Use a password manager to generate your passwords. Generating passwords is another thing computers do better than humans.
- If you have to remember a password, then use a passphrase instead. A passphrase is a particular sentence.

NOTE

Password and Passphrase Length

The longer a password or passphrase is, the harder it is to brute force.

An example 19 character password: `C35tPQVhCBZ*rV7CVm&`.

An example 9 word passphrase: `Drainage-Auction-Compacted0-Brussels-Floral-Reliant-Handiwork-Yodel-Jogging`.

Wikipedia has a list of password managers.

A Better Way

So far, we've only discussed authentication using 'something we know,' but there are better ways to authenticate. Using more than one factor or multi-factor authentication (MFA) to authenticate makes an attack that much more difficult for your attacker.

A factor can be any of the following:

- Something you know (like a password or passphrase)
- Something you have (like a key)
- Something you are (biometrics - usually fingerprints)
- Some*where* you are (When's the last time you connected to your account from Russia?)

Note: There may be other factors besides these.

Something You Have

Most people use keys in their everyday life. So using keys is something people generally understand.

Physical tokens such as FIDO2 keys (which you usually plug into a USB port) are a good example.

Alternatively, You can install Authentication apps on most phones that can generate one-time codes. To obtain the code, you must have the device with the app installed and configured.

Some examples of login tokens:

RSA SecurID

The RSA SecurID product is a key-fob that provides a one-time passcode (OTP) which, when combined with a PIN, becomes the login secret. This solution requires that the server and the key-

fob keep close sync with their time.

Universal Two Factor

Another key-fob-based authentication mechanism is to use a Universal Two-Factor (U2F) token.

One such token is a Yubikey.

Something You Are

Biometrics are usually unique to an individual, therefore, usually an effective form of authentication. Biometrics data is replicable and challenging, if not impossible, to change, so it is best to combine it with other authentication factors.

Somewhere You Are

Another less common method of authentication is location. People tend to establish a physical footprint of places they go. If there is an attempt to log in from a location far removed from your fingerprint, systems may block or require additional verification before granting access.

Multi-factor for the Win

Combining multiple factors of authentication before gaining access is the most secure way to safeguard accounts. Whenever possible, use multi-factor authentication.

As passwords become less complicated to attack, the need to switch to multi-factor authentication will become more urgent.

Data Classification and Handling: Protecting and Using Data

Data has sometimes called 'the new oil' (the fuel for our modern economy/society), but it can also be dangerous if not adequately protected. Not all data is created equal. Some data types merit the greatest protections, and other types of data should be more generally available. Data classification and handling are all about categorizing the data appropriately and applying the proper controls.

The Value and Danger of Data

Having the right information available improves decision-making and allows for better allocation of resources. An organization that can obtain, enrich, and utilize data will have significant advantages over its competitors that can't. Data can be a strategic competitive advantage. It is impossible to conceive an organization of significant size that doesn't leverage data in its operations.

Wherever there is the potential to do great good, there is also the potential to do great evil. The potential for significant damage exists if data is not adequately protected. Public embarrassment, fraud, theft, and other crimes come from the misuse of data. Usually, we are only concerned with protecting data confidentiality, but losing access to data could also have serious adverse effects.

So the challenge is ensuring the appropriate use of data while safeguarding from abuse.

Not All Data is Created Equal

Some data types, for example, payment card data, demand and deserve the application of significant protections to prevent fraud. Other data types should have some protections applied, but making this data more accessible is needed for business reasons (for example, business intelligence and financial reports). Still, other types of data should be generally available (they pose no serious risks and are beneficial to large groups (for example, weather forecasts).

Protecting data can be expensive. Encrypting and decrypting data promptly requires significant resources. With some data, it is an appropriate safeguard. With other data is a waste of resources. Understanding your data and applying the right amount of protection is an essential process for most organizations.

Deciding How Much Protection is Appropriate

There are two drivers for the protection of data, internal and external.

Internal drivers for protecting data include:

- Risk management and opportunity costs associated with applying the protections.

- If data loss would compromise an organization's competitive advantage, then more restrictive protections would be appropriate.
- Sometimes, protecting data too much could interfere with the organization realizing its mission. If this was the case, then some controls may work, while others would not.

External drivers for protecting data include:

- Laws/regulations and contracts/relationships.
- Regulatory requirements or contract obligations from a partner may dictate the types of safeguards one must use when protecting data.

While you might negotiate with some partners, usually, most governments are not as malleable. It is essential to understand that compliance is the floor (not the ceiling). These requirements are the minimum.

How Many Classification Levels Should an Organization Have?

The U.S. Military (who has a long history of needing to protect data) has three classification levels:

- Confidential - damage
- Secret - grave damage
- Top Secret - exceptionally grave damage

There is also an 'unclassified' category for data (used for data that doesn't require special protection). The amount of damage that unauthorized disclosure of data would cause defines the classification level.

We recommend finding the right balance between appropriately protecting the data and overprotecting data. Too many data classification levels will confuse people. Too few will result in resources wasted and operations unnecessarily complicated.

Determining the Classification of Data

Making data classification decisions every time someone collects or creates data is inefficient. Therefore, the recommendation is that data be classified when you decide to produce/consume it (upfront). This upfront classification enables all follow-on work and management associated with the data to be well understood and handled appropriately.

NOTE

Data Classification Levels Should be Pre-Defined

As a general rule, average employees should not have to decide what the data's sensitivity is and how to handle it. They should only have to know which pre-defined sensitivity/classification a specific piece of data has. The policy will determine the pre-defined procedures for handling said data.

So this should be a one-time (or rare) process. The earlier one classifies a data type, the better

(though later is better than never). Adding protections to data after you have accumulated it is more expensive (and onerous) than doing it from the start.

Classification Determines Handling

Once data has a classification, it should be clear to everyone involved in using said data what the requirements are. Handling requirements include:

- Marking the media and systems that process the data
- Protections while the data is at rest (in storage), in transit (in motion), and during processing (in use).
- Appropriate disposal of the data once it is no longer required
- Duration for retaining the data
- Who should have access to the data
- Physical environment and system requirements for accessing the data

Data Classification is the Foundation for Information Security

If you don't classify your data, it will become increasingly tricky to protect it appropriately. Information Security is about applying controls (protections) to your organization to enable its mission while adequately safeguarding it. Once you know what your data is worth (and how you want to protect it), then you can get to work (until then, you will waste a lot of time and energy and maybe still not adequately protect it).

Examples of Data Classification

NIST 800-53

The National Institute of Standards and Technology (NIST) created the NIST Special Publication 800-53 to provide security and privacy controls for U.S. federal information systems.

This document suggests you categorize your data in three levels:

- Low Impact
- Moderate Impact
- High Impact

Determine impact level by the amount of damage the disclosure of the data would cause.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a standard that organizations that handle payment cards (credit and debit) need to follow.

One of the requirements of this standard is that the organization in question "Protects Cardholder Data".

This requirement means that storage and transmission of data such as:

- Name
- Full card number
- Security code
- PIN
- Contents of the magnetic stripe

Be encrypted and handled in specific ways.

The levels and requirements of your data classification will be determined by what kind of data you have and from where it originated.

Day to Day Computing Security

As we spend most of our time using computers daily, it’s essential to learn some new basic computing safety habits. We’ll cover some of the simple things you can do to make your day-to-day use of your computer safer.

Operating System and Software Updates

Old insecure versions of installed software are a leading cause of computer exploits.

One of the most simple and powerful things you can do to increase your personal computer security is to make sure you are running the latest and greatest software versions. Most updates are for fixing software security issues, especially the updates to your operating system(OS). These updates will reduce the number of security flaws that attackers can exploit on your system.

Find more details in the "Updates" module of this course.

OS Level Security features

In recent years, operating systems designers have added increased security tools and features. These security tools help mitigate the damage a piece of exploited software can cause

Keep your operating system’s security tools and features running, including:

- Security Software
  - Windows UAC
  - SELinux
  - AppArmor
- Firewalls
- Antivirus Software

Keeping your system up to date and protecting itself is a tremendous first step you can take.

Use Only Verified Software

Installing software from unknown storage devices or downloading software from questionable sites can lead to system compromise. You should only install software from trusted known sources.

Look for the software in your operating systems version of an "App Store".

If you install software from third-party sites, verify that you are on the correct site, and check the site’s security certificate.

If possible, install only signed software (software verified and security signed by the OS would be ideal).

Web Browsing Tips

Securely browsing the web is an essential part of overall computer security. Malicious sites, broken or compromised toolbars, and other malware have to get on our systems somehow; coming from a browser is one such path.

Check the SSL/TLS certificates of any site you "log in" to. Phishing sites often look **JUST** like the proper site. Yes, even phishing sites are using certificates to have you blindly trust that the SSL/TLS certificate is correct.

Use a browser-integrated password manager. Browser-integrated password managers will ensure that the username and password are getting pasted into the correct site. Password managers reduce the chance that you'll fall for a well-made phishing site.

Use multi-factor authentication (MFA) on all sites that support it. Multi-factor authentication will secure your online account by requiring you to submit a second authentication factor other than your password. MFA will make your account more secure. It may also cause you to distrust a phishing site.

Personal Identifying Information (PII)

The name of the game for scam artists, attackers, and hackers is personal identifying information or PII.

PII includes things such as your name, address, birth date, and social security number.

Protect your PII by only entering the data that a website needs for you to get the functionality out of it you need. For example, your social media accounts most likely do not need your social security number. However, you may need to provide your social security number to login into your doctor's web portal.

Be aware of where you post your personal information.

Social Media Concerns

Social media platforms are an attractive target for attackers. We put a lot of information into these platforms and don't often think of the consequences.

An interesting angle for attackers to use is the prevalence of "social media gaming". These games often require you to allow the game publisher to access your personal information in your social media account. Many attacks which stole personal data have used this tactic in the past.

WARNING	*Social Media Games* Social media games, quizzes, and other "apps" can send your personal information to the game's publisher. Double-check the information you are granting to these applications.

The social media platforms have measures to protect their clients, but bad actors are many, which causes issues with enforcement.

Defaults

Default settings and credentials are attributes of a device, system, or service that control their access or functionality without administrator or user intervention.

Most of the time, the users of a system don’t change (or are not even aware of) defaults; therefore, they rarely change. Additionally, they are usually not optimized for security and pose significant risks to the device, system, or service.

Why are Defaults Insecure

Most products target lay consumers. Consumers value convenience and want their things to 'just work'. Frequently, more secure configurations are likely to complicate usage, and therefore, most products are not as secure as they could be out of the box.

Default Credentials

Most devices we purchase come with default credentials (usernames and passwords). If you ever had a hard time logging into your Wi-Fi router, you might have run a Google search and found the default credentials to get in and set up your router. The problem is that (unless you change them) attackers can do the same thing and use it to control your equipment.

While it might be extra work, we recommend that you check for (and change) the default credentials on all of the devices you put into operation. It could prevent you from falling easy prey to an attacker.

WARNING	*Warning* Please use unique and complex credentials for each of your devices/services.

Default Settings

To maximize their products' utility and convenience, vendors frequently enable most of the features and services they think consumers will want. Additionally, they will configure them in a way that will maximize their utility and compatibility with other products and services. Usually, these default settings will not be as secure as they should/could be.

In general:

- Disable all services/features that you are not sure you need (or are going to use). You can always go back in and enable them later,
- Dig into the settings, and see if additional security features are available.

Adjust them to make sure they work but are as secure as practically possible.

Advanced Options

If you are particularly paranoid, you can find and use secure configurations for your systems developed by organizations that specialize in securing systems and services:

- Center for Internet Security (CIS) Benchmarks are guides for configuring your systems to minimize vulnerabilities.
- The United States Military (or DoD) has developed Security Technical Implementation Guides (STIGs) to secure systems and services that consumers and businesses also use.

WARNING	*Warning* The CIS benchmarks, developed to secure mission-critical systems and services, are more strict than a typical system may need. You should adjust them to make a system as usable as you want/need it to be.

Balancing Act

Security and convenience usually work against each other. You will need to adjust the defaults to achieve a position that works for you and minimizes risk.

Email Attacks

The combination of widespread use, ease of creation, and generally weak defenses make email a space rife with deception, manipulation, and fraud. Attackers can (with little effort and expense) mount far-reaching and effective attacks using email. Humans are the ultimate targets and the most effective line of defense.

Deception

Because authentication tools are not widely utilized and the platform enjoys an unearned amount of trust, deception is frequently too easy to accomplish. Victims doubt only when given reason, meaning as long as the attacker doesn't raise red flags too blatantly. Without these red flags, we are willing to believe most assertions.

For example, the famous Nigerian Prince scams took in far too many people. Someone you don't know (and never met) tells you that they need your help and asks you to open bank accounts and deposit checks from financial institutions you haven't investigated.

We must replace trust with doubt. If there is anything out of the usual pattern or any inconsistencies, you should challenge and verify them. Leaders should not just tolerate their people double-checking but demand it and demonstrate appreciation for doing so.

Impersonation

Attackers do their homework. Between information available on the organization's website(s), social media, and publicly available government records, attackers have an abundance of available information. The chance is that they can recreate your organization's organizational chart with reasonable accuracy. If they want to impersonate an external (but real) agency or organization, they have enough information available to create a persona that will mostly 'check out.'

Be wary of unusual requests from people in leadership positions within your organization. Reach out to them via different, trusted channels of communication to verify. Using out-of-band communication methods should be the standard practice. Any request (especially involving money) needs to be independently verified.

It May Feel Real

With ever-improving toolsets and tradecraft, attacks are no longer always detectable by spelling mistakes and cheesy graphics. While you may still encounter them, don't let your guard down because an email looks legitimate. Always take the time to check things out and verify.

What are they after?

What are Attackers hoping to achieve?

- Money (a classic objective)

- Access to confidential information (to use for nefarious purposes)
- Access (People and systems/infrastructure)

The Most Common Attack

Today, the most commonly encountered email attack is phishing. Phishing is the practice of sending fraudulent email messages where the attacker impersonates an authority or trusted person/party to get a victim to reveal confidential or personal information. Phishing is responsible for a large percentage of security incidents (specifically data breaches) today.

The real target of a phishing attack is a human, email (or other communications channels) are only the delivery method. Everyone is vulnerable to being manipulated. Almost all approaches try to get you to respond/act before you have an opportunity to think through and apply procedure or critical thinking.

Simply slowing down and following established procedures will do a lot to reduce the probability of falling victim to a phishing attack. Contacting the supposed sender via a different, trusted communications channel (internal chat, phone, etc.) before taking action is another powerful way to avoid falling victim.

The Most Devastating Attack

Because most of your online life passes through your email account, the compromise and takeover of your email account is - potentially - the most devastating attack. Once an attacker has gained access/control over your email account, there is almost no limit to the mischief they can perpetrate. Among the many things that could happen, they could use control over your email account to take over other accounts (such as credit card, mortgage, or bank accounts).

IMPORTANT	*Secure your Email* Your email account can gain or reset access to other accounts such as bank or credit card accounts. Securing your email helps protect these linked accounts.

Your email account is the one thing you need to safeguard the most. If possible, use multi-factor authentication. You should also use strong, unique passwords/passphrases to secure access to your email account. Strong authentication is generally good advice but particularly important for your email account.

An Emerging Threat

The Cybersecurity industry has observed a new threat emerging in the last few years, business email compromise. Business email compromise is when an attacker gains access to your work email account.

Once an attacker has gained access to your business email account, they can read through your past (and ongoing) email messages and gain powerful insights into you and your organization. They can use these insights to launch powerful phishing and financial fraud attacks that people inside your

organization are more likely to fall victim to (because it comes from a trusted email address and demonstrates a deep understanding of the organization's culture and business practices).

Once again, the safeguards recommended protecting your email account (strong authentication credentials and practices) and phishing (slow down - follow procedures - independently verify requests) are strongly recommended.

Malicious Links and Attachments

One of the most effective ways to bypass an organization's defenses is to attack their humans. One approach to doing so is to craft email messages with links to malicious sites/resources or malicious attachments.

If they can infect your machine with malware, they can pivot using your system to attack other resources.

Do not click on links that you didn't expect to receive (even if they seem to come from someone you trust). You shouldn't download or open attachments unless you were expecting them. If possible, scan the files using your anti-virus or sandbox services.

Email: Best Practices

How you use email can significantly impact the security of your organization and your personal privacy. The following recommendations will help you stay secure when using email.

Use Strong Authentication

Email account compromise (where someone else takes over your email account) is one of the worst things that can happen online. It can place everything else at risk. Securing access to your email account is one of the most important things you can do.

Recommend:

- Enabling/requiring multi-factor authentication (even if your credentials are compromised, this may protect your account)
- Using strong passwords or, even better, passphrases (secrets are best if they are long and unpredictable - recommend using a password manager to store and generate credentials)
- Do not reuse credentials from other accounts (this is an excellent general practice, but for email accounts, it is even more critical)

Scan All Attachments

Attackers will frequently attempt to compromise your system by tricking you into opening an attachment (potentially installing malware).

You shouldn't open any attachment (expected or unexpected) without having it scanned for malware). Hopefully, your organization scans all inbound email for malware, but it is always a best practice to perform a manual scan of attached files (specifically unexpected email).

If available, use sandbox scanning services. They can detect new malware that your standard antivirus might not detect.

Don't Click on Any Links

What you see and where a link in an email message takes you can be radically different. If you want to check out a site referenced in an email, it is far safer to go to the site independently of any links in an email message.

Even the 'Unsubscribe' link in an email can be malicious.

Beware of Phishing

You will be subject to a phishing email attack. Always verify any assertions or requests made in an email message. Reach out to the person or organization that a message supposedly came from to verify its authenticity before taking any action.

Usually, multiple people within an organization are targeted by a phishing attack. Therefore, promptly report any suspicious email messages to your IT or information security teams. They could take action to investigate and prevent messages from reaching others.

Don’t use Organizational Email for Personal Use

Mixing your personal communications with the business’s services (like email) could compromise your privacy and increase the organization’s risk. Companies can read anything you send via their email service. If you don’t want your boss knowing about something, then keep it clear of company equipment and services.

Check Your Account Settings Regularly

One way you can detect a compromised email account is to check the settings. If you find unusual settings, you should report them to your IT/Information Security team (preferably not over email).

Some things to look out for:

- Unexpected forwarding rules for inbound messages
- Unexpected suppression settings that would hide inbound email messages
- Unexpected changes to your email account credentials
- Unusual inbox activity - Unexpected messages

Don’t Use Email for Confidential Communication

By default, email communication is not secure from eavesdropping. Email was created a long time ago (when message confidentiality wasn’t a general concern). There are secure communications tools that work in conjunction with email, but their usage is not as widespread as they should be.

While you might implement something internal to your organization, eventually, the need to share sensitive information outside your organization will arise; in these cases, we recommend finding and using a secure portal service.

Refer to your IT department for suggestions on the proper secure communication platform.

Email Mistakes

Email is one of the oldest and most commonly used communications services on the Internet. Nearly everyone uses email nearly every day. Like other parts of our lives, there are many ways to make mistakes while using email.

Weak and Reused Passwords

While the reuse or use of weak passwords is always discouraged, these mistakes can prove particularly dangerous/problematic when it comes to email. The reason is that most online services allow you to reset your credentials (if you forgot or suspect that they are compromised) using email. A compromised email account places almost all of your online accounts at risk.

Recommendations:

- Use a password manager to generate and store unique credentials
- Do not reuse passwords (especially when it comes to email accounts)
- Use passphrases for added security (length is the most crucial element of a secret's security)

Intermingling Work and Personal activities

Using work email for personal use can compromise your privacy. Business accounts are frequently monitored (or at least subject to inspection), which means your personal affairs are no longer private.

Depending on your business and jurisdiction, using personal accounts for organizational purposes could be illegal. Usually, in litigation, relevant email is discoverable, which means that you could have lawyers crawling through your personal email. To safeguard your privacy, avoid using personal accounts and equipment for business purposes.

Think work and personal like church and state, keep them separate.

Sending Sensitive Information

Without applying additional protections, email is more like a postcard than a sealed envelope. Anyone (and anything) that your email passes through (or is stored on) has an opportunity to read the contents.

We will talk about some measures you can take to safeguard email in other modules, but understand that many of these measures are not commonly utilized or require both parties to support them. You should not send information such as government identification numbers, payment card data, personal financial or credit data via email. There may also be other types of data that are too sensitive to send over email. When in doubt, assume that email is insufficiently secure to send sensitive data.

Unintended Recipients

Even though email is not secure enough to send sensitive data, you will frequently conduct such sensitive communications via email. Due to human error and autocompletion of email addresses, it is too easy to send an email to someone you didn't intend to.

You should double-check the recipients before sending an email message (primarily if the content is for specific audiences).

Clicking on Links

Clicking on links is a pattern of behavior we bring with us from browsing the web. The problem is that what you see in the email application may vary from where the link takes you. An intelligent attacker could cause some significant harm from you clicking on a link they've crafted.

We recommend going to the website/service independently of the link. Even if it looks like it is coming from a legitimate account, it could be someone spoofing the origin email address or the sender has a compromised account.

General Guidance

Pause and think before you act.

Nothing is so important or urgent that you can't reach out to the sender via another communications channel to verify a request made via email.

Double-check the receivers and content before sending a message.

High-Value Targets

Because of the nature of the access that high-value targets have, they make an extremely enticing target. Protecting high-value targets in your organization poses some unique challenges.

As attacks against high-value targets are often more sophisticated and subtitle, one must focus on defending them. And failure to protect the high-value target can have far-reaching effects.

Who Are High-Value Targets

How do you know if you are a high-value target?

There are a few classic examples of a high-value target, including executives, VPs, HR, and IT.

However, instead of focusing on the person or role, a better solution would be to look at the type of information and level of access granted to the person.

Are you a high-value target?

- Do you have access to any of this information?
  - Executive-level information.
  - Access to core business tools/information.
  - Payroll or HR-related information.
- Physical access to restricted areas.
- Full (aka `root`) access to digital infrastructure.

When to Focus on Defending High-Value Targets

While defending high-value targets is an everyday thing, defenders should take extra care during specific events and times.

High-value targets should take extra care during any significant event in the business (layoff, merger, acquisition, IPO). Attackers will troll for businesses in these phases to send targeted phishing attacks. Disgruntled employees could potentially take advantage of these chaotic events as well.

When a high-value target is traveling overseas, there are some additional considerations.

When traveling overseas, you want to ensure the integrity of corporate information. It may be a good idea to issue a "burner" device for the high-value target to use while traveling. Enforcing the use of a VPN is also a good idea.

IMPORTANT	*High-Value targets Overseas* Issue a "burner device", a laptop or phone which IT can wipe upon return for use during an overseas trip. This device should enable the high-value target to utilize a VPN to connect to corporate data and should have minimal data on the device itself.

There are also concerns about searches by US customs and border control upon returning to the US. Please consider the above when designing IT policies.

Types of Attacks on High-Value Targets

High-value targets often have different routines, and attackers will leverage this.

Travel Concerns

Executives and leadership roles often travel for work-related reasons. Always being on the move can make one fall into some bad habits.

When at a hotel, don’t broadcast your room number; write the room number on the check to charge items.

Don’t trust hotel safes. A hotel safe often has a default code set that attackers can use to access your possessions.

Verify you have all of your belongings when exiting a taxi or public transit.

Personal Digital Devices

If you use personal digital devices (tablets, cell phones, smartwatches), do not connect them to corporate information or networks. Attackers like to use what is known as a "pivot attack" to gain access to the less-protected personal devices, then "pivot" to corporate data.

A better solution for high-value targets is to let corporate IT secure your devices using the latest techniques.

General Security Practices

As a high-value target, it is vital that you continue to follow the basics of any digital security policy.

Attacks such as credential stuffing are just as common as for all of the other employees; however, the stakes for a successful attack are much higher.

High-Value Targets at Home

The network infrastructure at the home of a high-value target also requires some additional considerations.

Look into things such as:

- Smart home assistants, these devices contain microphones and sometimes cameras and can be very difficult to detect if they are compromised.
- Smart locks, any device with a network connection and running software can be compromised.
- A high-value target should use a VPN for all traffic on personal devices.
- It might be a good idea for high-value targets to have a more secure area in their home to discuss sensitive topics (door which closes and locks, no smart assistants inside).

High-Value Targets Operational Security (OPSEC)

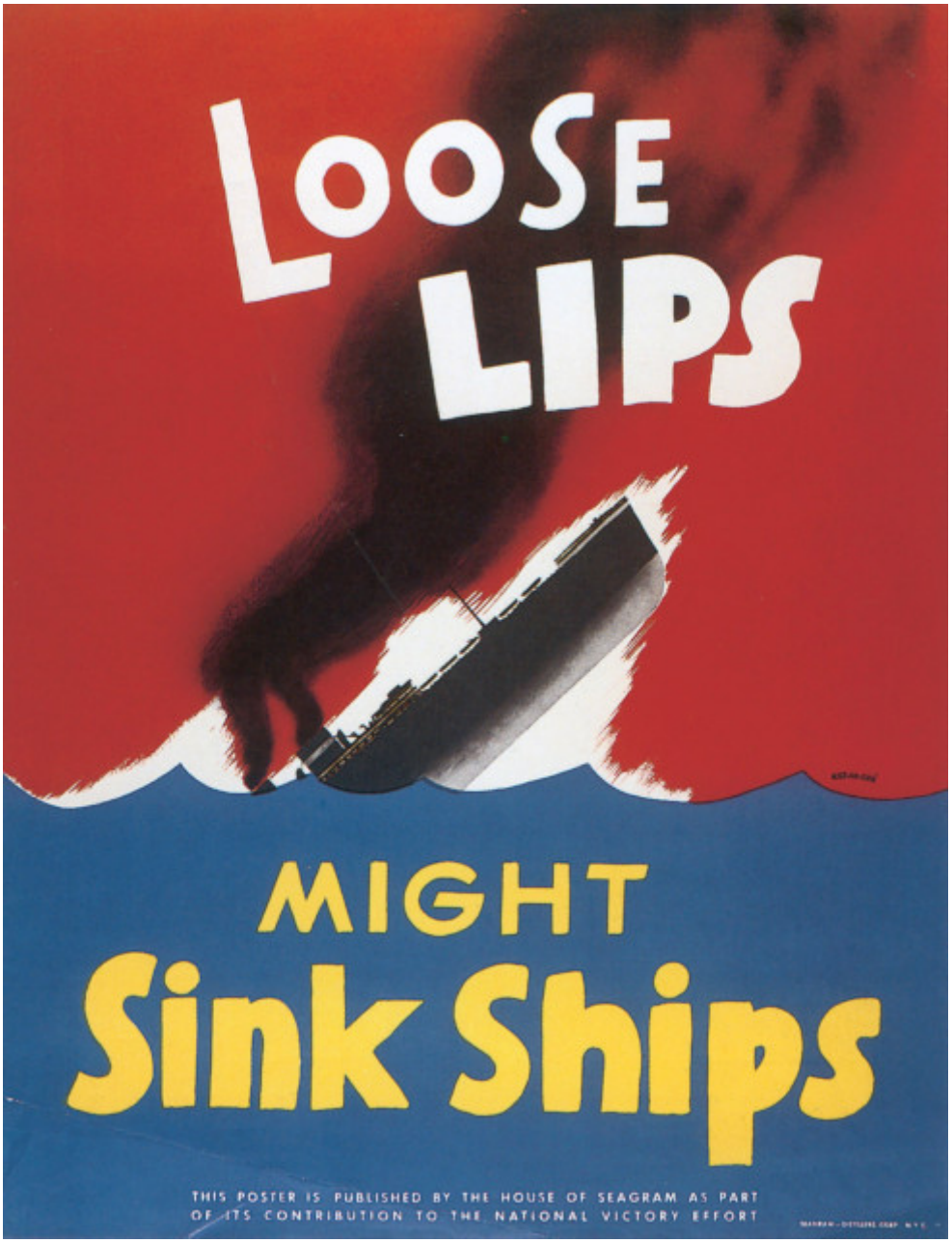
Operational Security (OPSEC) is the process of protecting data in aggregate to prevent use by attackers.

To practice good OPSEC, one must look at the entirety of the data to determine if sharing said data might compromise security. Look at the background of the photos you take. Are you sharing more information than you planned?

Could someone determine from your CEO’s social media that they have traveled to the the city that houses the home office of a competitor multiple times, thus leaking the the potential of a merger or acquisition?

Good OPSEC is not a checklist but rather a mindset. You should view all of your actions with the mindset that you may be a target and act accordingly

The campaign "Loose Lips may Sink Ships" from World War II is a good example of an OPSEC practice.



Some high-value targets may choose to do the following:

- Harden personal devices.
- Harden home networks.
- Regularly take security training, including OPSEC training.
    - Test high-value employees' responses to simulated attacks, and re-train when needed.
- Keep a separate "public" social media profile.
    - Private social media profiles could be used for friends and family.
- Enroll their email in more advanced security profiles (such as the Advanced Protection Plan provided by Google).
- Require the use of a password manager.
- Use made-up or obfuscated answers to "security questions".
- Require requests of a specific type to be verified "out of band".

- For example, a phone call to verify the text message requesting a wire transfer.
- Better yet, specific requests could always require multiple people to verify.

General Practices for Information Distribution

High-value targets often need to distribute information to large groups. A suitable method for this distribution is to generate the information in an internal wiki and post the link to the wiki page into the email for broadcast.

This method does two things, makes the canonical location for the information the wiki, which can be updated at will and helps to verify that the information is valid as an an attacker would have to compromise both the wiki and email logins to post it there.

There should also be a global policy in place for **EVERY** coworker to report suspicious activity **EVERY TIME**. Constant reporting is vital to help IT and security teams to see trends around these suspicious events.

Another critical policy that relates tangentially to high-value targets is a policy on the secure destruction of sensitive information. When the company has finished with hard drives or paper information, there should be a defined policy to determine the proper way of destroying said information.

Malware

If you can use a tool for good, then it is possible to use that same tool for evil. Malware is malicious software. Malware can do great harm to your systems and organization.

Types of Malware

Malware has taken many different forms; here are a few of the most prevalent types:

- Virus (spread themselves through replication)
- Worm (a virus that spreads itself using computer networks)
- Trojan (Misleads users of its real intent)
- Ransomware (Encrypts or steals data and requires payments to regain access)

These are not the only forms malware have taken. In the future new forms will be developed.

Prevention

> A pint of sweat is worth a gallon of blood.
>
> — General Patton

The most desirable position to maintain is to avoid becoming 'infected' with malware. While they are not always practical, many efforts to prevent infection are usually worth taking.

Prevention: Hygiene

A user's behavior significantly impacts the probability of getting infected with malware. Some of the things you can do are:

- Only install software from known (reputable) sources.
- Update software frequently (to minimize vulnerabilities)
- Only visit reputable websites, don't click on links in emails unless you were expecting them, and trust the sender. When in doubt, contact the sender via an alternate communications channel to verify (for example, phone).
- Disable unused services.

Detection: Antivirus Software

You should install and enable Antivirus software on the systems you own/operate. Programs marketed as antivirus also usually protect against other forms of malware.

Antivirus software uses a database of malware definitions to detect malware on your systems. Because new malware is continuously in development, it is vital that you keep your definitions up-to-date to keep your antivirus software effective. If possible, enable your antivirus software to

update automatically.

Detection: Antivirus Software Configuration

You should ensure that your antivirus software has the following features enabled to protect your systems better:

- Scan all files downloaded from the Internet and Network
- Conduct scanning of your system at regular intervals (usually daily)
- Scan removable media when it is attached (or inserted) into the system
- Disable 'autorun' of any removable media

Detection: Sandboxes

Some malware is so new that the antivirus programs don’t yet have definitions for them. Because of this, you should use sandbox services to scan untrusted or suspicious files.

Sandboxes interact with possibly malicious files within a controlled environment to evaluate their behavior to determine if they are malicious.

Detection: Sandbox services

There are several 'free' sandbox services available. They will scan submitted files and report back their findings. Antivirus vendors pay these services to gain access to the submitted files and their associated findings. Because of this, you should not submit any files to such services if you believe the files contain confidential information.

If your organization needs to sandbox files with confidential information, they should either subscribe to a dedicated sandbox service or operate and maintain their own.

Detection: Human as a Sensor

In addition to the tools we’ve identified and described, humans can be an essential way to detect malware. If you detect any of the following signs or symptoms, you might want to report them to your IT or Information Security teams.

Unexplained/Unexpected:

- High CPU (processor) usage
- High network usage
- Excessive usage of storage
- Slower than usual system performance
- Other odd system behavior

Recovery

If your system(s) get infected by malware, it will be necessary to contain, eradicate, and restore your system(s) and data.

Recovery: Containment

Most antivirus software will quarantine any files that contain malware to reduce the harm they could do to your system(s).

Additionally, you should disconnect your system from the network if you suspect that it is infected (this is to prevent the further spread of the malware.

Do not turn-off or modify a system you suspect may be infected. Forensics personnel will need to investigate the system to determine where the malware came from and the damage it has done.

Recovery: Eradication

Once you have contained the malware, it is time to remove it from your system(s). Sometimes, this is as simple as deleting the malicious file. Because attackers are likely to take additional steps to ensure they continue to have access to your system, the only sure way to eradicate the malware is to erase the device's local storage and reinstall. If an attacker is sufficiently advanced, it may be necessary to wipe the local storage and destroy the device.

What measures you take will vary based on the system's criticality and the suspected expertise of the attacker.

Recovery: Restoration

If you plan to use the previously infected system, you may need to reinstall the operating system and software to restore the system to a usable state. Additionally, you may want/need to restore your data from backups.

Having backups is critical to getting back up and running. You should enable automatic backups to ensure that you minimize the time lost. Before restoring from backups, you should scan them to ensure they are clean.

WARNING	*Warning: Test your Backups* A backup is only as good as a tested restore. Test your restore method to a different location and compare data to the source to ensure you have a safe backup.

Backups also become very useful when you have multiple levels or incremental backups.

Events like a ransomware attack are less costly if you can restore files from incremental or off-site backups.

Password Managers: Improving Security and Usability

A password is a secret that you use to authenticate yourself (prove you are you) to a system or online service. There are many problems associated with human weaknesses and passwords. Password Managers help solve these problems.

Why We Use Passwords

At some point in the past, we found it necessary to prove our identity to computer systems. It was probably because it was expedient; an identifier (usually a username) and a secret was the solution. Generally, it seemed to work, and so whenever the need for authentication arose, we defaulted to this solution.

Problems with Humans and Passwords

Over time, we have come to identify some serious problems associated with using passwords to authenticate humans.

Humans struggle with two things that make using passwords problematic.

First, humans struggle to think of strong passwords. Strong passwords are hard to guess. Humans are (sometimes) lazy and creatures to habit. We frequently do only what is required (this makes guessing a password much easier). Additionally, we are creatures of habit, and these habits mean that the passwords we create are usually predictable.

Second, humans struggle to remember things. Because of this, we prefer simplicity and reusing those things we do have to remember. Both of these preferences result in generally bad practices with passwords.

How Adversaries Exploit Bad Password Practices

There are several approaches adversaries use to attack passwords:

- Brute Force Attacks
- Password Lists
- Rainbow Tables
- Credential Stuffing

In addition to these approaches, adversaries can (and will) develop other ways to attack weak password practices. These are just the most prominent attacks used today.

Brute Force Attacks

Brute force attackers are when adversaries use computer systems to try a large number of possible passwords against a service/system to search for the right one. While there are some ways that systems/services can protect themselves from these attacks, there is always the possibility that a system may be vulnerable.

Short passwords are particularly vulnerable to these kinds of attacks. Of all the types of weaknesses, short passwords are the easiest to attack.

Password Lists

Whenever data breaches occur, there is an opportunity for adversaries to study the data to enable additional attacks. Frequently they build lists of common passwords that they can then use against other systems/services. These lists of common passwords usually meet with significant success.

Rainbow Tables

Sometimes, an adversary can acquire a copy of the database that stores the hashes used to verify if a password is correct. In this context, a hash is the result of a one-way processing of a password. While it shouldn’t be possible to process the hash and retrieve the original password, it may be possible to use previously cracked hashes (Rainbow Tables). When they work, they are a quick way to get passwords.

Using previously used passwords will make your passwords vulnerable to this kind of attack.

Credential Stuffing

An increasingly common attack against password reuse is 'Credential Stuffing.' Once an adversary has obtained some usernames and passwords, they will attempt to use them against other systems/services. Credential stuffing is frequently effective and enables an adversary to take over (at least a large) part of the victim’s online life.

Password Managers as a Solution

Now that we are familiar with how human weaknesses in creating and using passwords make us vulnerable, we are ready to discuss a solution (Password Managers).

While Password Managers' functionality varies, they all help generate strong passwords and facilitate using unique passwords for each system/service.

Generating Strong Passwords

Strong Passwords (or even better, passphrases) have specific characteristics:

- Length (to defend against brute force attacks)

- Complexity (again, to defend against brute force attacks)
- Unique (so that the compromise of a password doesn't expose other services to attack)
- Hard to guess (sometimes called entropy)

Usually, significant care, understanding, and thought have been put into enabling password managers to generate strong passwords. A password generated by a password manager will fare better than a password a human can generate.

Using Unique Passwords

In addition to generating strong passwords, password managers will enable you to store a different password for each of your accounts. You will need to remember the password that gets you on your local computer and access the password manager, but after that, you won't need to remember any of the passwords for your online accounts.

Password managers make it a lot easier to use unique passwords for your accounts (significantly improving your digital security).

Selecting a Password Manager.

If you work for an organization, they have likely selected a password manager for you to use. If this is the case, you should familiarize yourself with it (so that you use it securely and obtain the most significant benefit from it).

If you want to use a password manager for your own needs, you should investigate the available options. Yes, you want security, but you also want it to be as useful (and usable) as possible (a solution you don't use is not a solution). After reading about the various options, We recommend that you try a few of them out.

In the end, you want to find a solution that will work for you in the long run.

Wikipedia has a list of password managers.

Safeguarding Your Password Manager

Once you decide to use a password manager, it will become one of your online life's essential parts.

Whatever solution you select, it is vital that you safeguard your password manager. In some cases, it will mean selecting a particularly strong password to prevent unauthorized access to your password manager. In other cases, it will also include making sure you have a safe backup of your password manager data file.

One Last Thing

Password Managers can significantly improve your security online, but it is still highly recommended that you use multi-factor authentication whenever (and wherever) possible.

Multi-factor authentication involves using something besides just a password to gain access to an account. Some examples are physical tokens, biometrics, and location.

Combining multi-factor authentication and strong passwords will give you a high-level of confidence in the control of your online accounts.

Phishing

Phishing is a form of social engineering that attempts to obtain confidential or classified information using deceptive electronic communication forms. Commonly the attacker presents themselves as a trusted party to cause the target to give up personal information, usernames, passwords, or credit card numbers.

Types of Phishing

Based on the target, phishing can be classified differently:

General Phishing

Any attempt to gain access to protected data or information.

Spear Phishing

Targeting a single individual in a phishing attempt

Whaling

Targeting high-value individuals (Senior Management, VP, CEO level)

Spear Phishing targets a specific type of access or data. For example, targeting the IT administrator because of the higher-level access they may have, or HR department employees to gain more info on higher-value targets.

Whaling is targeting high-value individuals who may have information that is worth much more. For example, the C-Level employees will have access to information that lower-level employees might not have. This access and information make the C-Level employees a lucrative target.

Avenues of Phishing

Phishing deals with electronic forms of communication, leading to common exploitations by attackers.

Email Spoofing

Forged E-mail sender addresses. Email is an insecure protocol, and spoofed sender addresses are easy to create. An email purportedly coming from a known person may be faked.

Instant Messaging

Posing as a coworker or other trusted party using instant-messaging tools. (either internal to the company or external) If an instant message seems to be suspicious, verify the sender is whom they claim to be.

Website Spoofing

Attackers often gather info by creating a fake site that copies a legitimate site (complete with images). Verifying TLS/SSL Certificates and domain names can help defend against these fake sites.

Website Spoofing Techniques

Attackers can use the following techniques to trick you into believing a website is legitimate.

- Using JavaScript to change the content of a website.
- An improperly configured web server can leak information to another site using a Cross-Site-Scripting(XSS) exploit.
- Using a sub-domain to appear legitimate.
    - e.g. `mybank.attacker.example` vs `mybank.example`
- Using improper HTML anchor targets and descriptions. (the link appears to point in one direction and sends the victim to another
- URL shorteners commonly hide the destination of malicious links.

Phishing Email Examples

Phishing emails prey upon our lax attention. Here are some of the tactics used in common phishing email attacks.

Things to Verify

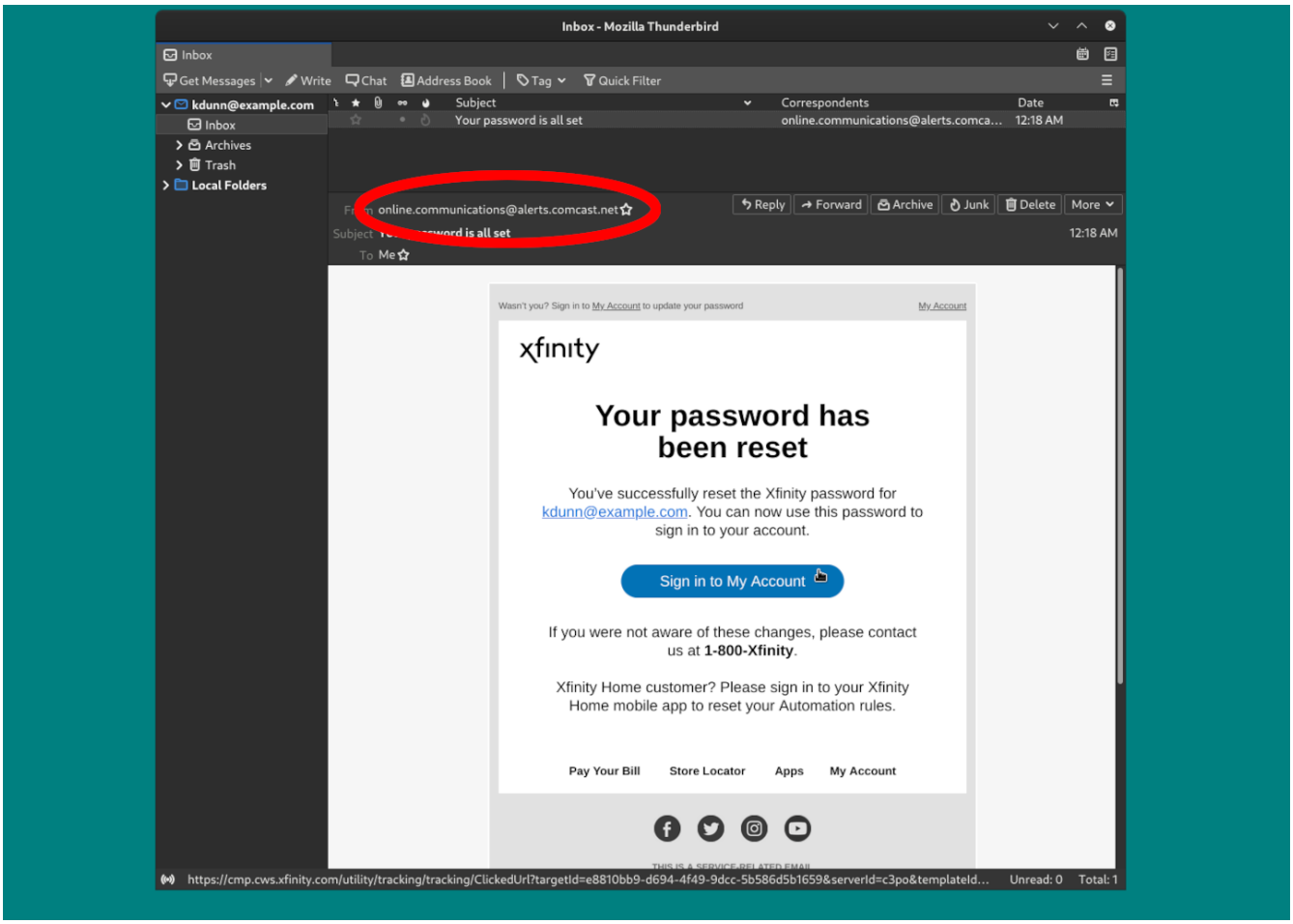
Verify sender address

Even though sender email addresses can be spoofed to appear from a legitimate source, you should verify that the sender's address is what you expect.

NOTE

Legitimate Address

Note that the sender address in this legitimate email from Comcast/Xfinity has a `comcast.net` domain.

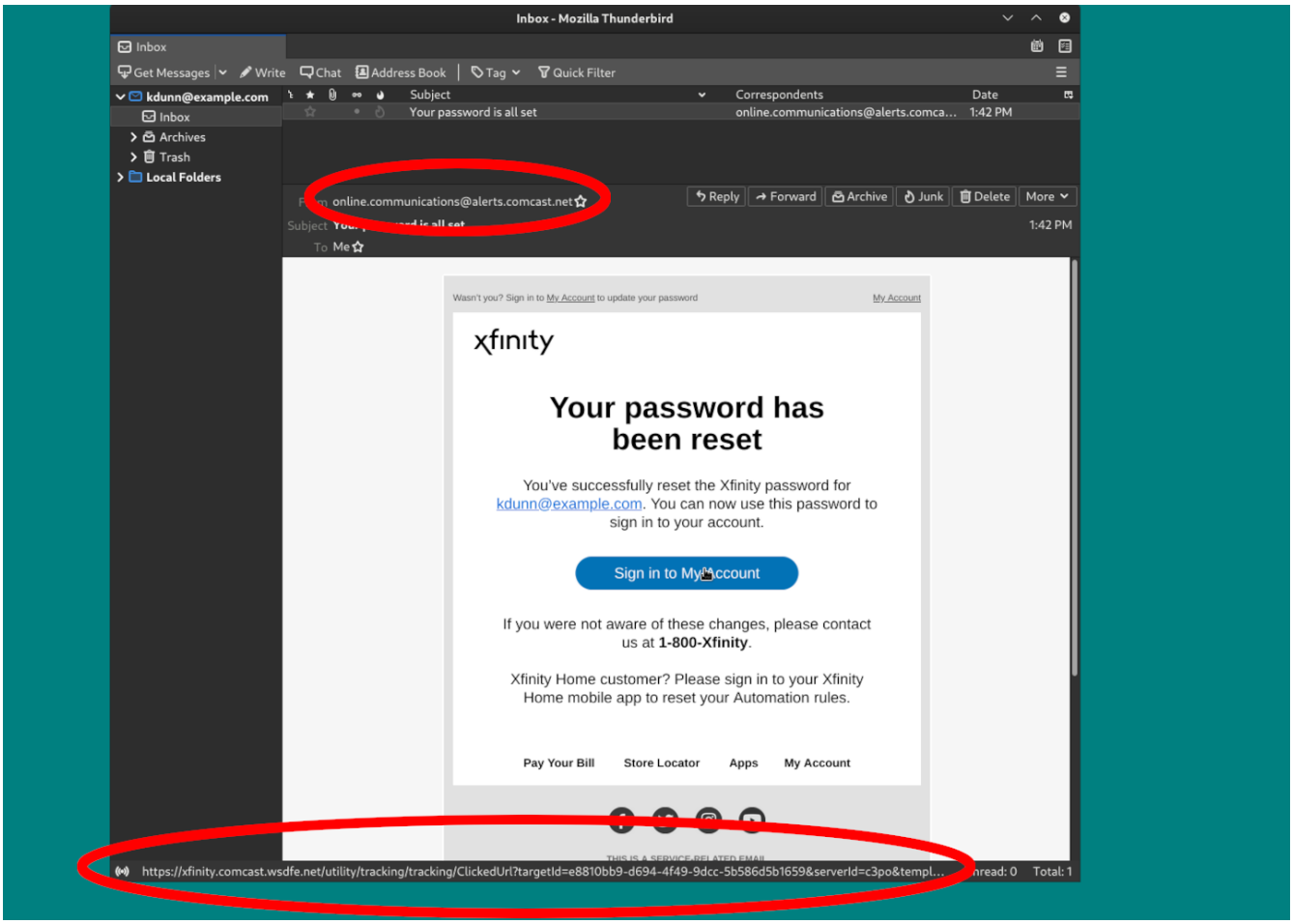


CAUTION

Legitimate Address; Phishing Email

Note that the sender address in this phishing email also uses a `comcast.net` domain. It is possible to spoof the sender's address.

You should still verify the addresses of links before you click them. Look at the URL on the bottom of the image to verify.



Verify URL Destinations

Phishing emails use links to send you to websites where while they look legitimate, they are not legitimate.

Use your mouse to hover over links or long-press on a touch-based device to show where the link will send you before you click on it.

Attackers hide dangerous links in the following ways:

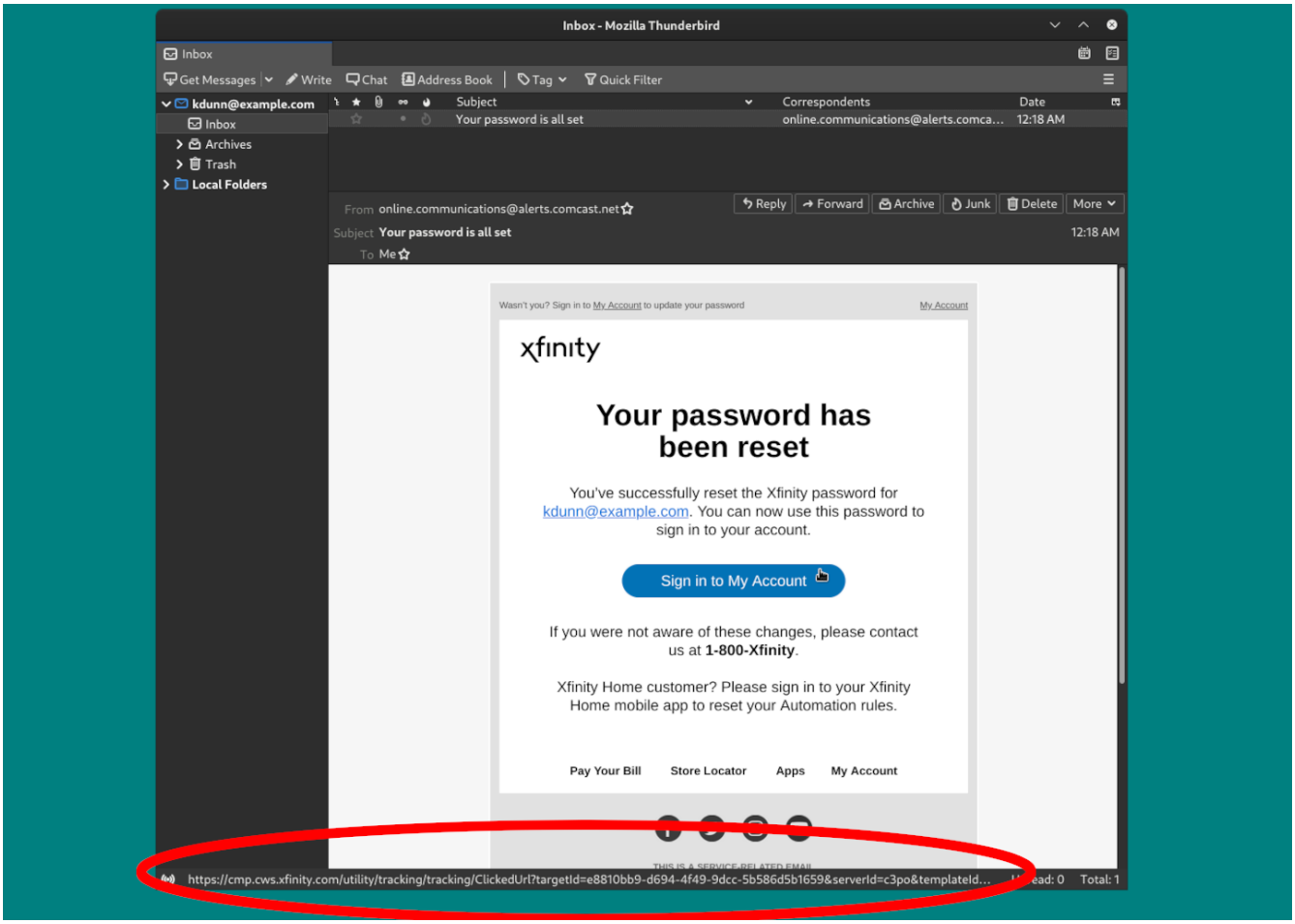
- Using a "look-alike" domain, `comcast.com.rse2d34s.attacker.url` instead of `comcast.com`, for example
- Using URL shortener to hide URLs.
    - Something like `tinyurl.com` or the like.

NOTE

Legitimate Email; Legitimate Link

Hover over or long-press the link or button before you press it.

This email has safe links as they point to an `xfinitiy.com` domain.



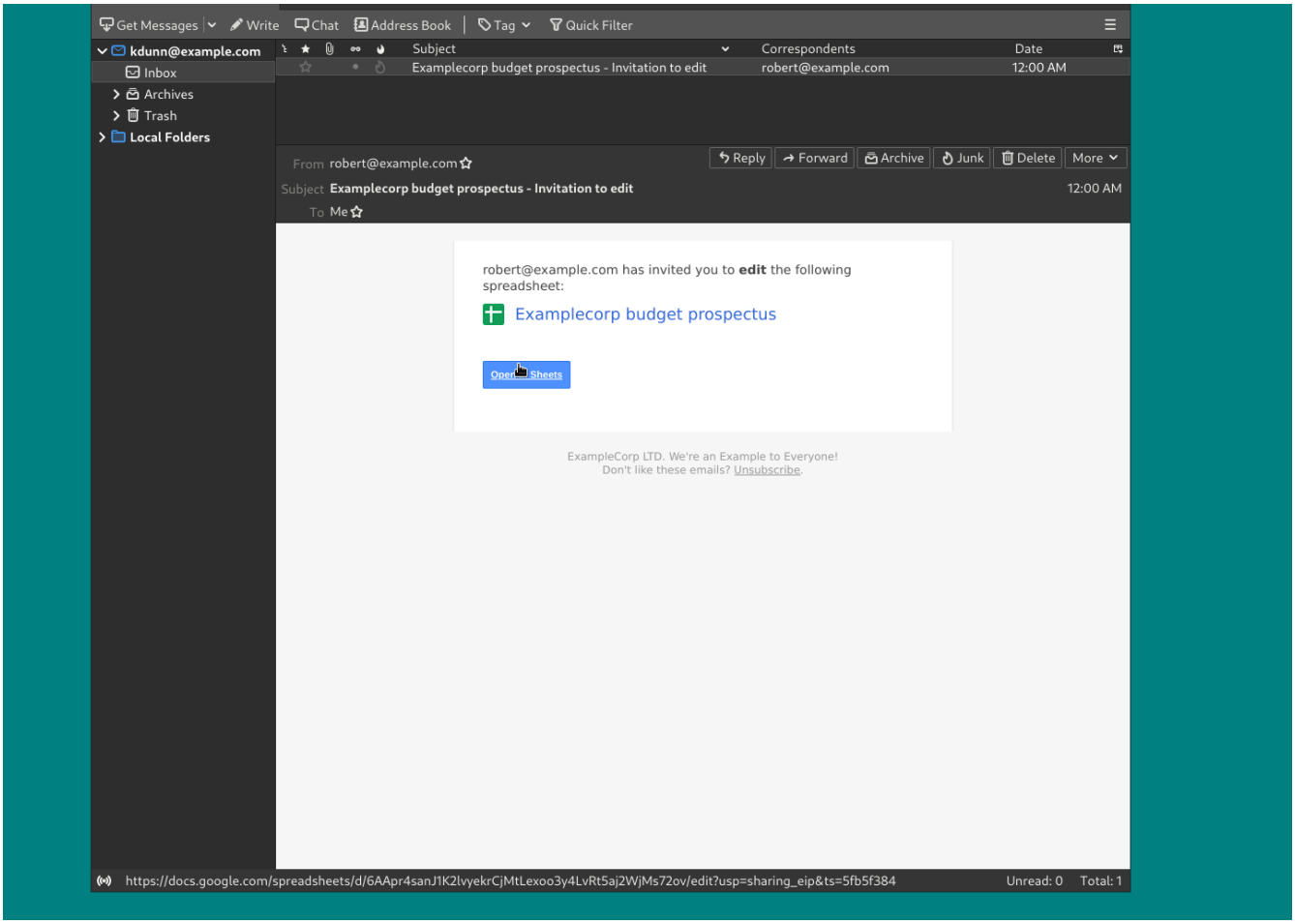
Example of a legitimate email from Google Docs

NOTE

Legitimate Email; Google Docs

Hover over or long-press the link or button before you press it.

This email has safe links as they point to a `docs.google.com` domain.

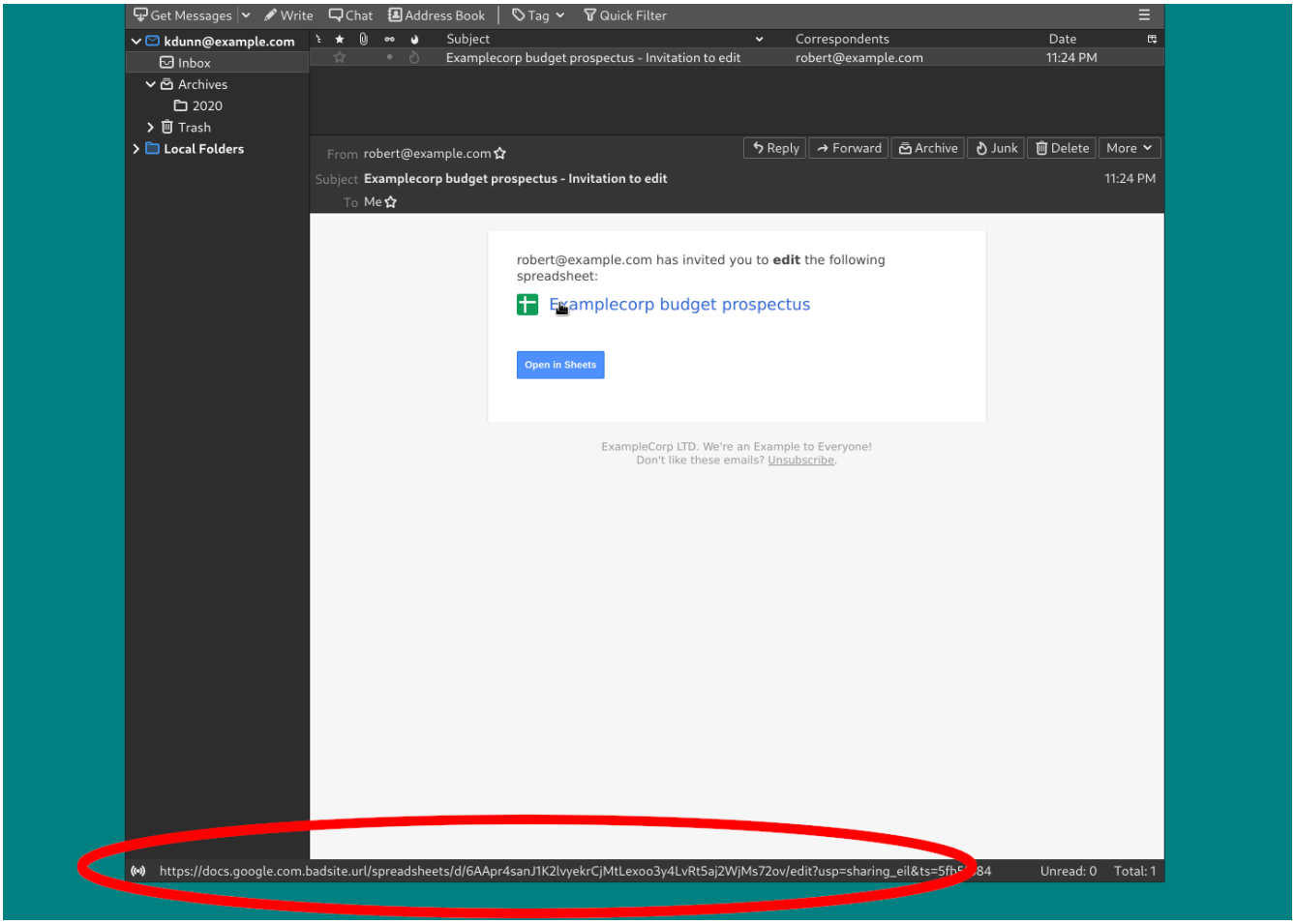


Phishing Email; Google Docs

CAUTION

Compare the above email to this one.

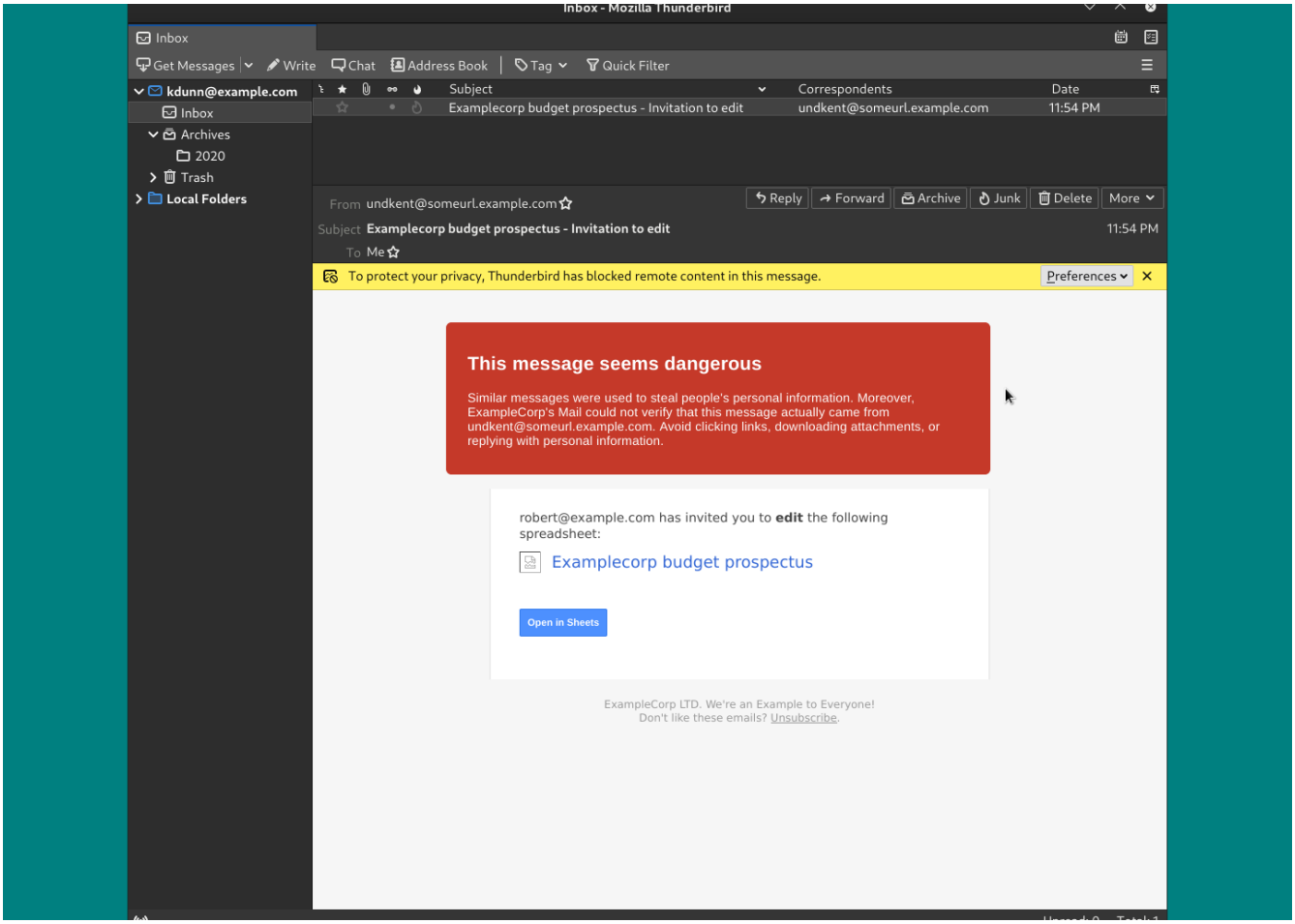
This email does not have safe links as they point to a `badsite.url` domain.



Trust Your Email Provider and Email Client Warnings

Often you will get warnings either from your email provider or the email client itself.

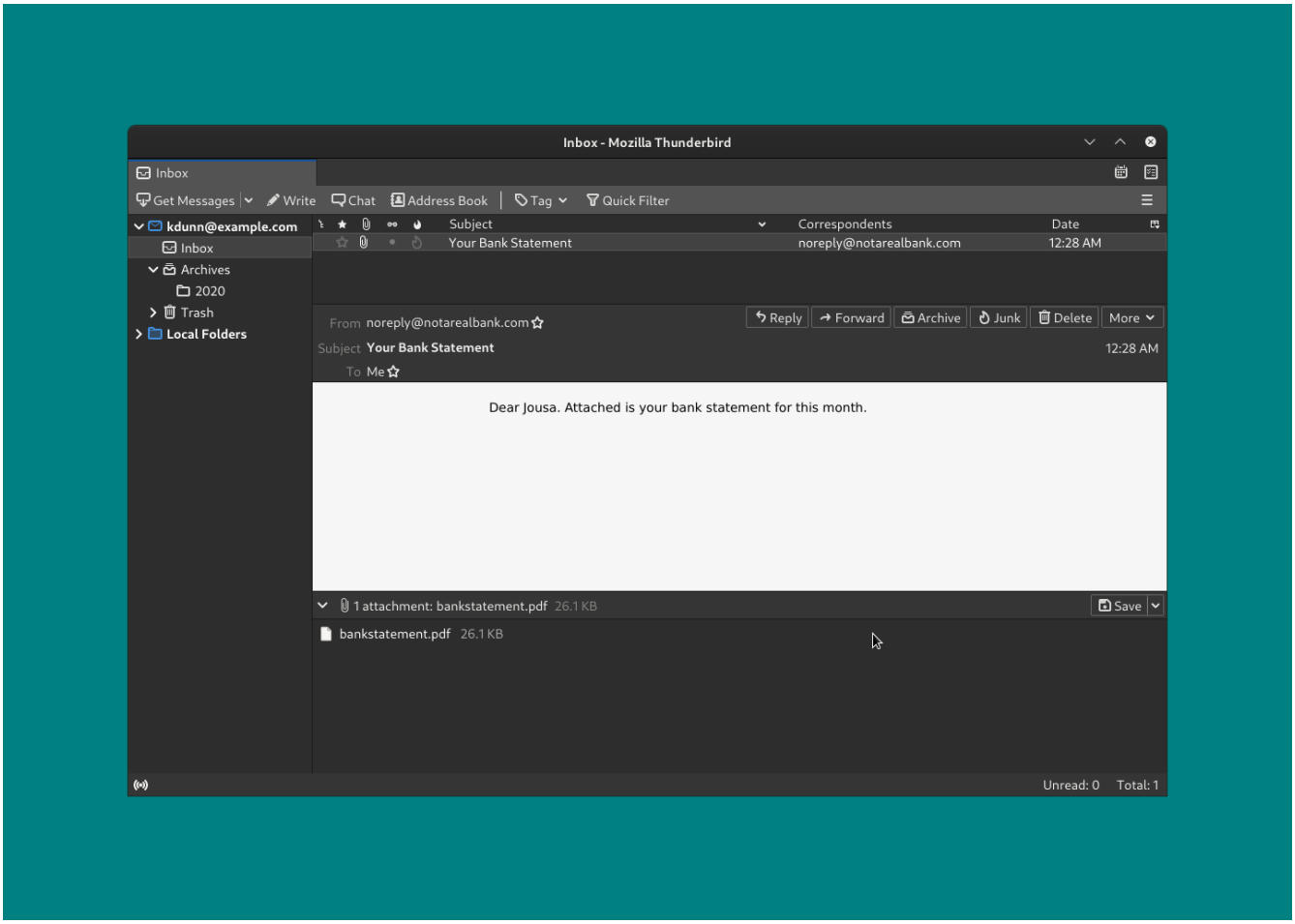
You should trust those warnings and give any email containing said warnings a thorough vetting.



Verify Attachments are Expected

Computer Viruses and malware are often included in attachments.

You should not open an attachment you are not expecting, even if it is from a contact you know and trust.


Inbox - Mozilla Thunderbird
Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
kdunn@example.com
Inbox
Archives
2020
Trash
Local Folders
Subject
Correspondents
Date
Your Bank Statement
noreply@notarealbank.com
12:28 AM
From noreply@notarealbank.com
Reply
Forward
Archive
Junk
Delete
More
Subject Your Bank Statement
12:28 AM
To Me
Dear Jousa. Attached is your bank statement for this month.
1 attachment: bankstatement.pdf 26.1 KB
Save
bankstatement.pdf 26.1 KB
Unread: 0
Total: 1

Physical Security

> Physical security is as important to the overall security of your organization as any other type. The best digital security can easily be circumvented if your physical security is compromised.

Why Physical Security?

Physical security as a component of an overall security framework can help mitigate espionage, theft, and loss. Physical security is also an essential part of specific compliance frameworks. Your organization may have to implement specific physical security policies to meet these compliance frameworks.

Securing Your Building

The first thing to look at concerning physical security is the security of your building.

Locks and Access Control

Depending on your compliance needs, you may have to implement access controls to certain areas of your building. Often this is done using a digital key card or lock system. Some secure areas need multiple factors (a PIN or biometric auth) to operate the lock. Key cards by themselves are not a super-secure method for higher security needs.

Tailgating

Tailgating is the act of multiple people entering a secured area on a single key card read. Mitigate tailgating by either policy and enforcement or technology, such as a turnstile or laser sensor.

Clean Workspace Rules

A part of some compliance frameworks requires a "Clean Desk Policy". A clean desk policy means that any sensitive information or notes need to be cleaned up and secured if there is no person at the desk.

Other considerations

Window and desk placement should be such that monitors and desks' contents cannot be observed from outside. Additionally, use polarizing filters on windows and screens to obscure secure information.

Use video surveillance to audit security issues, and allow for remote monitoring.

USB and Computer Security

USB thumb drives and other removable media are an avenue of attack. A malicious person plants

an infected USB storage device in the parking lot or common areas of a victim's workspace. The victim plugs in the storage device, and the malware infects the victim's computer allowing a foothold into the network. A study by the University of Illinois, Urbana Champaign, University of Michigan, and Google found that 45-98% of people plugged in "Found USB Drives" Matthew Tischer, Zakir Durumeric, et al..

Computers that access secure information should have security settings that disable removable media.

Unlocked computers should also not be left unattended. Configure a locking screensaver or use some other method to lock computers when not in use.

References

Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey (May 2016). Users Really Do Plug in USB Drives They Find IEEE Symposium on Security & Privacy ("Oakland")

Mobile Security: Protecting that which goes with you

Mobile devices (phones, tablets, and other devices) are the ubiquitous objects of modern life. They present an incredible concentration functionality, but they also present significant security concerns. Understanding the risks and what you can do to mitigate them will help you make informed decisions about how and when you use mobile devices.

Tracking Devices That Make Phone Calls

About a decade ago, a security expert referred to mobile phones as 'tracking devices that make phone calls.' The way mobile phone networks have been architected and a principal focus on functionality, mobile phones (and most mobile devices) have de-emphasized privacy and security.

These devices, even if not infected/compromised, leak important data about you. For example, even if you are not making a phone call, the people who manage the phone network can track your real-time location. Until recently, any application installed on your device could access the 'clipboard' (where you cut, copy, and paste data temporarily) at any time. Voice commands are usually processed in the cloud (at the vendor's data centers), which means they likely have access to anything you say in the device's proximity.

Efforts to make them 'just work' mean that when designers chose between privacy/security and usability, the choice was almost always prejudiced towards usability. Since the global surveillance disclosures in 2013, some of the vendors have started to enable privacy/security features without compromising the value proposition that mobile devices present to users.

We will talk about the risks and the things you can do to improve your mobile device usage. Still, if you ever absolutely need a private conversation, it is recommended that you keep the phone/tablet in a different room.

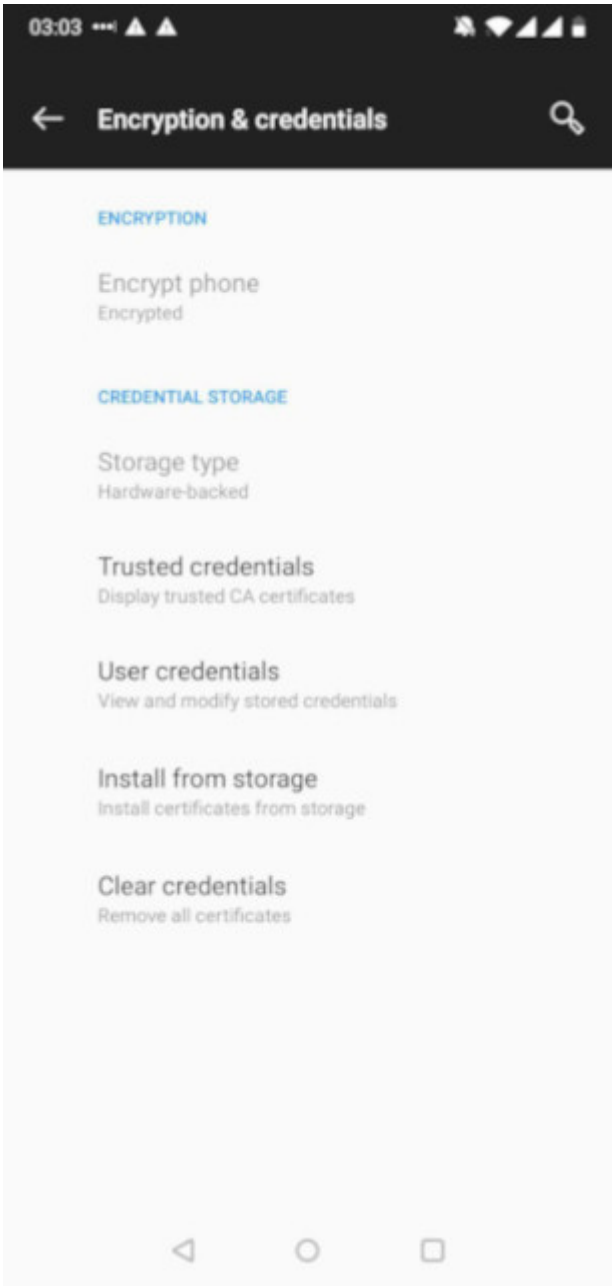
Being Popular Paints a Target on Your Back

Any system, service, or device that becomes sufficiently popular (and mobile devices certainly qualify), will attract adversaries (both criminal and nation-state) to compromise and exploit them. Even with the vendors' best efforts, there is still a high probability that a determined adversary will find a way to gain access or subvert it.

Not to say you should give up hope (or throw away your mobile devices), but that you should realize the potential of the hostile environment in which you operate. Be mindful of the clues we will talk about, and take the measures we recommend, and you can significantly improve the security of your mobile devices.

Make Sure Your Devices are Encrypted

There is always a chance that your mobile devices might leave your physical control (for example: lost or forgotten). When that happens, you will want to ensure that the device's data is protected from those who have it in their possession. Today, most vendors will enable encryption on mobile devices by default. Still, it is a good idea/practice to verify that this is the case. Usually, you can go into the device's settings and check/enable this.



For the iPhone, encryption is enabled by default.

Symptoms of Infection/Compromise

While not always the case, if you notice any of the following signs or symptoms, then you should consider it likely that your device has been compromised:

- Unusual battery consumption/Short battery life

- Unusual or unexpected storage, CPU, or memory usage
- Unusual device behavior or 'slowdown.'
- Unexpected Apps or services installed or running

If you notice any of these (or particularly many of these), you should consider the device possibly compromised.

What to do if you suspect your device is compromised

To reduce the risks associated with a suspected compromised device, you should do the following:

- Change/reset the credentials associated with any account that was accessible on the device.
- Place the device in 'Airplane mode' (disable network connectivity - Wifi/Cell network access).
- Either get the device securely wiped or inspected by a provider capable of assessing the device's security.
- Depending on your security needs, you might want to have the device destroyed and securely disposed of.

Mobile Device Management

Suppose you use a mobile device (either personally or organizationally owned) for business. In that case, there is a strong probability that the organization you work for will require that you enroll it in their mobile device management system.

Mobile device management enables the organization to lock, wipe, inspect, update, or selectively delete a mobile device. Tools like this are a requirement because the organization has an interest (or obligation) to safeguard the data/services that the device can access. Understand that you will lose a measure of control over the device if it is enrolled in mobile device management. If you want/need to keep your personal activities private from that organization, then it is recommended that you don't conduct those activities on a managed device.

Jailbreaking or Rooting a Mobile Device

'Jailbreaking' or 'rooting' a mobile device is disabling some/all of the mobile device security controls. Jailbreaking is frequently done to install software or configure the device that the default controls would otherwise prevent.

It is essential to realize that you take a significant risk when you do this. The built-in controls on mobile devices are (at least in part) meant to prevent you from installing potentially malicious software or expose you to other uncontrolled risks. If you want to do this, recognize that this is not a supported or encouraged action, and you accept additional responsibility for what happens with your device.

Suppose you are curious and want to play with programs/functionality that isn't generally available through official sources. In that case, we recommend that you don't do so with the device you use daily. In this case, purchase or use another device.

Physical Security

If a hostile actor gains physical access to your device, then you should probably consider it compromised. They can implant software/hardware on the device to grant them control or access to the device in the future. It would be best to physically secure your devices when they are not in your possession (for example: using a safe).

SMS Security

Many people use short Messaging Service (SMS) to send text messages. It is important to know that these messages can be read, intercepted, or diverted to/by others. Like email, this service was initially conceived and designed without concern for how attackers could abuse it, and therefore should not be trusted for sensitive communications.

One application that SMS has been used for is an additional factor for authentication. Adversaries have learned how to exploit SMS, and using it for multi-factor authentication is not recommended. Instead, you should use applications built explicitly for this purpose.

Additionally, adversaries have developed tactics and techniques to compromise mobile devices remotely using maliciously formed SMS messages. It is best to immediately delete (without opening) messages from people you don’t know).

Updates

Most updates are principally security fixes. Therefore, it is helpful to check for and install updates on your mobile devices frequently. Sometimes, updating your system is done differently than updating your applications. Please check both regularly.

Bluetooth Attacks

Bluetooth enables you to attach or utilize nearby devices wirelessly to extend the functionality of your device. The problem with Bluetooth is that it can also expose your device to attacks.

One example of an attack is 'Bluesnarfing.' This attack enables others to gain unauthorized access to information on your device (for example, calendars, contact lists, emails, text messages). In addition to 'Bluesnarfing', there are other possible attacks that exploit Bluetooth.

Disable Bluetooth on your mobile devices if you don’t use it. Enable it only for the time you need/use it. Frequently check your mobile devices to see which Bluetooth devices have paired with them. Remove any/all unexpected devices.

Juicejacking

Because most mobile devices use their charging interface for additional purposes (for example, sending/receiving data), it is possible to attack a mobile device by operating a malicious charging station. Only use charging devices that you own and control to charge your mobile devices, including cables and not just charging bricks. Attackers have successfully created malicious

charging cables which can compromise your devices.

Spyware

Any application installed on your mobile devices has access to a lot of the information available on your device. Exercise care in selecting what applications (and what permissions you give them) you install on your mobile devices (even from the official application stores.

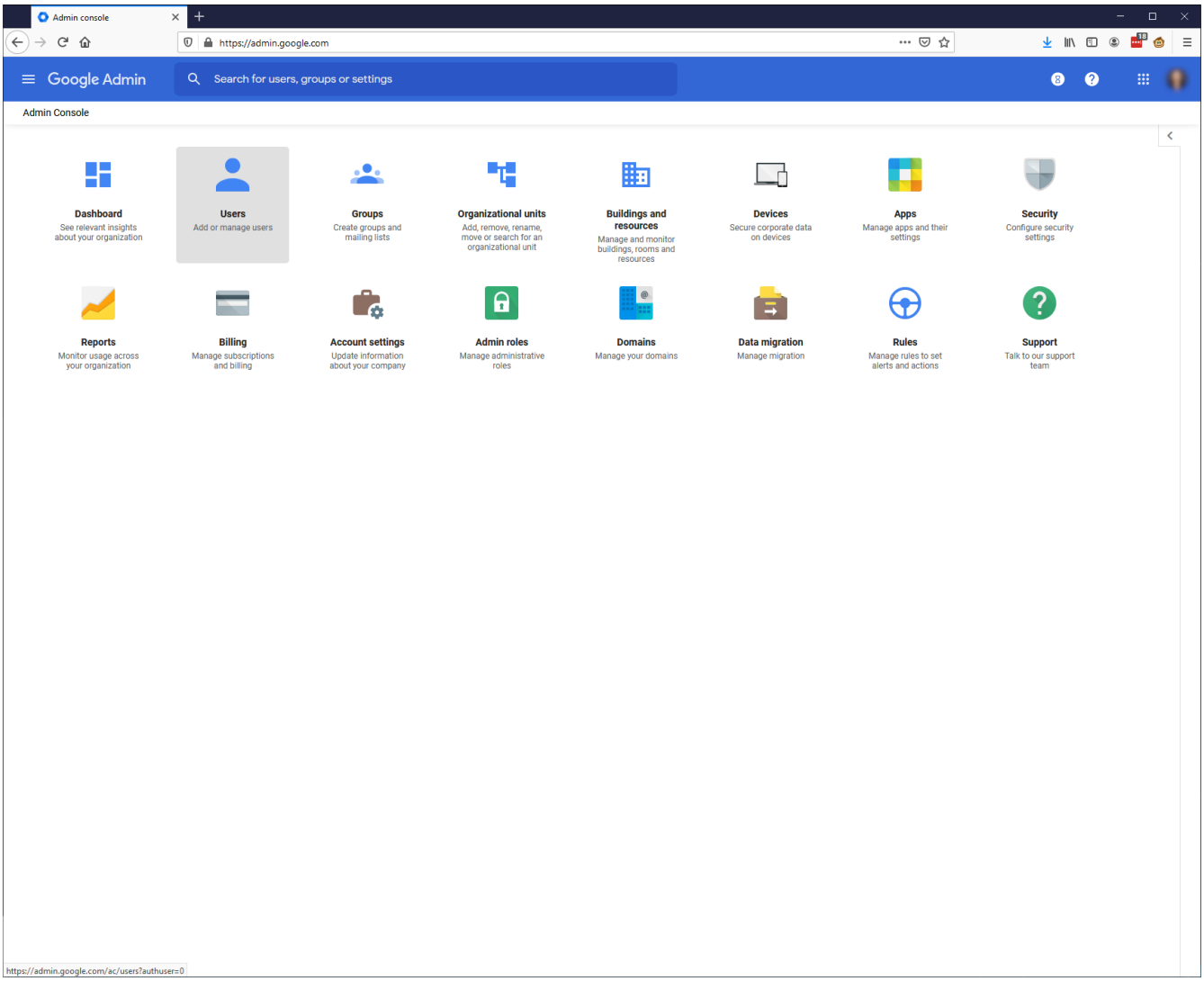
Security Settings in your Google Admin Interface

If you use Google's infrastructure to run your company's email infrastructure, you should be aware of some additional security options.

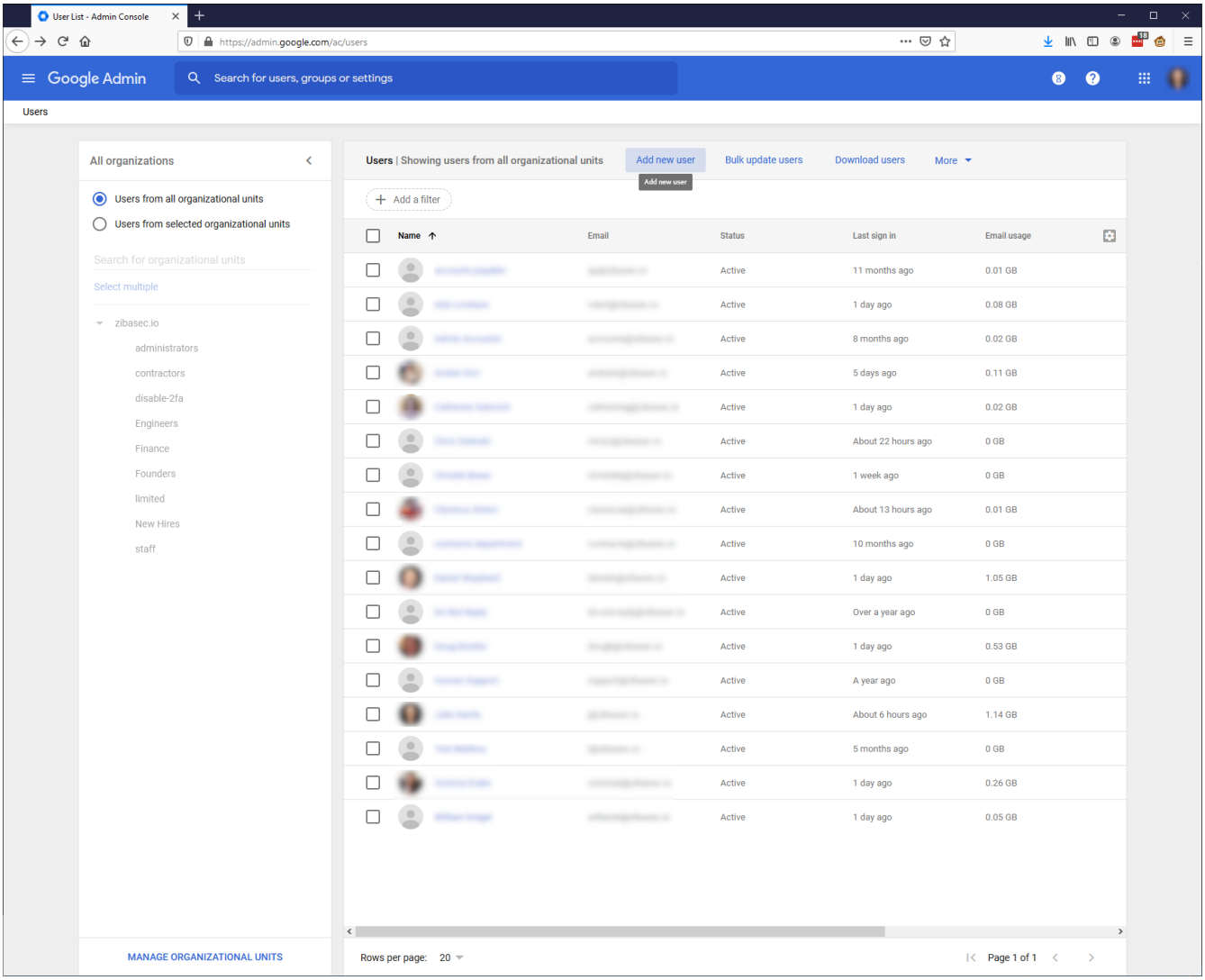
Adding New Users

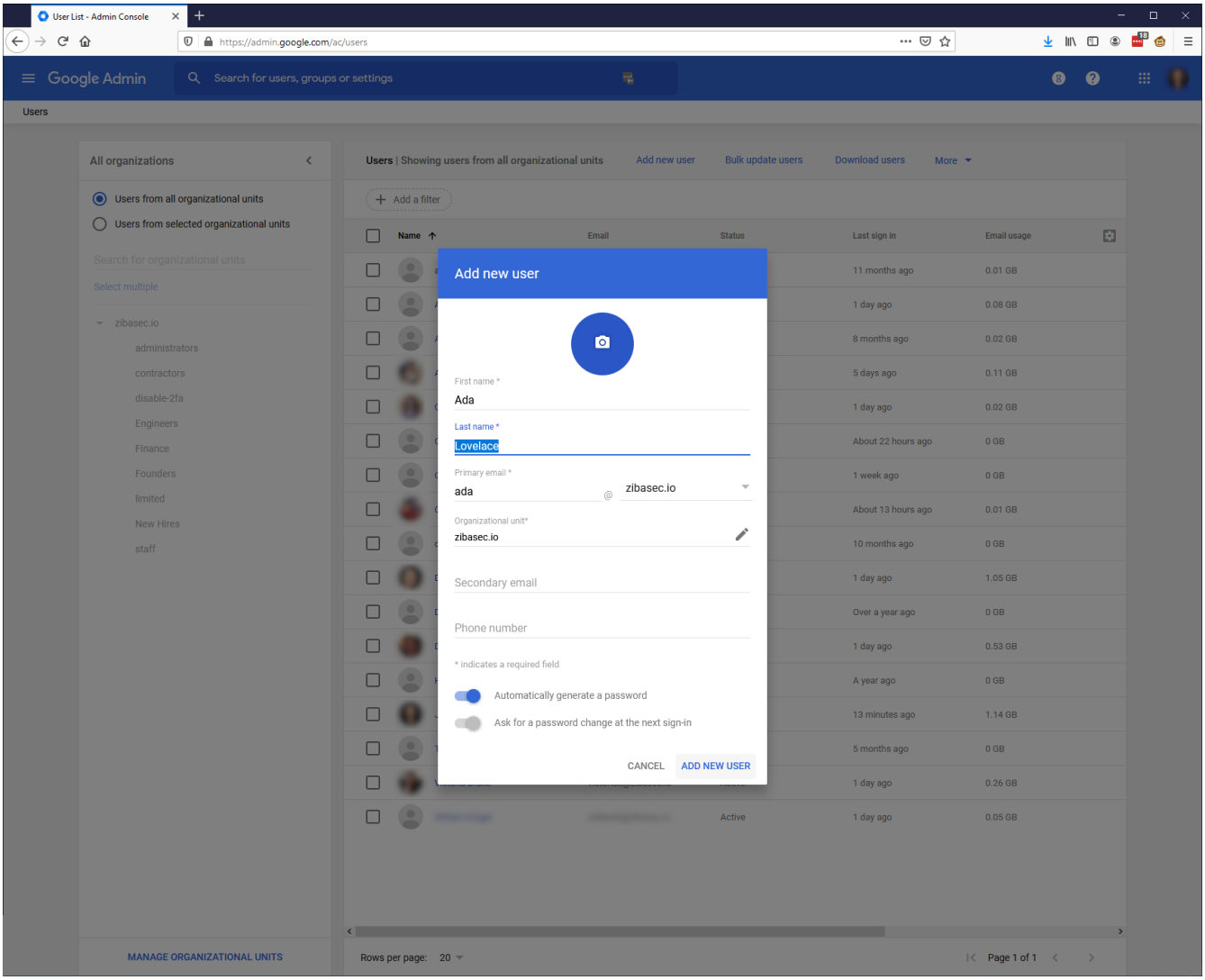
The interface for adding a new user looks a little different.

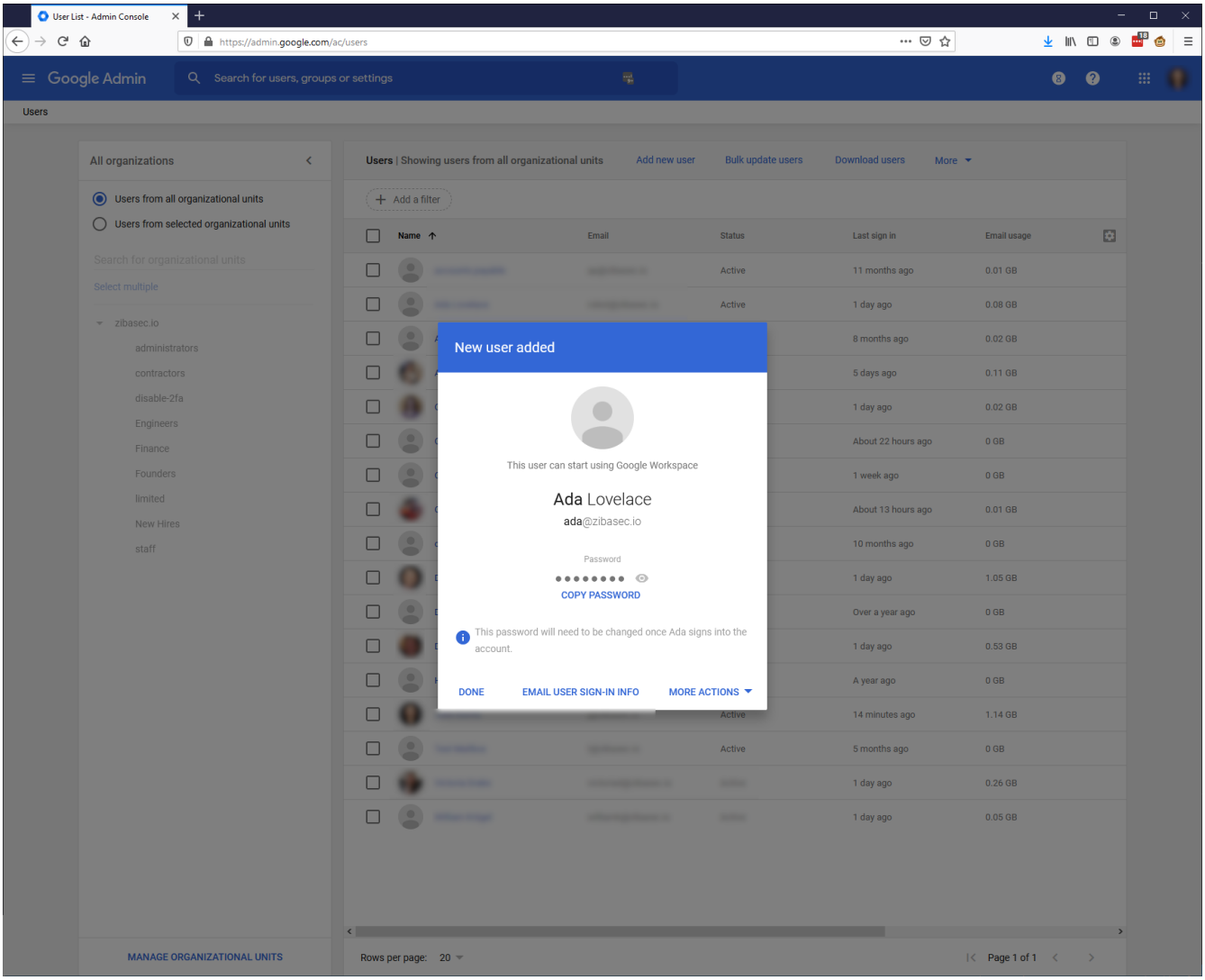
Click the "Users" button in the admin interface.



Click the "Add new user" button.


User List - Admin Console
https://admin.google.com/ac/users
Google Admin
Search for users, groups or settings
Users
All organizations
Users from all organizational units
Users from selected organizational units
Search for organizational units
Select multiple
zibasec.io
administrators
contractors
disable-2fa
Engineers
Finance
Founders
limited
New Hires
staff
MANAGE ORGANIZATIONAL UNITS
Users | Showing users from all organizational units
Add new user
Bulk update users
Download users
More
Add new user
Add a filter
Name
Email
Status
Last sign in
Email usage
Active 11 months ago 0.01 GB
Active 1 day ago 0.08 GB
Active 8 months ago 0.02 GB
Active 5 days ago 0.11 GB
Active 1 day ago 0.02 GB
Active About 22 hours ago 0 GB
Active 1 week ago 0 GB
Active About 13 hours ago 0.01 GB
Active 10 months ago 0 GB
Active 1 day ago 1.05 GB
Active Over a year ago 0 GB
Active 1 day ago 0.53 GB
Active A year ago 0 GB
Active About 6 hours ago 1.14 GB
Active 5 months ago 0 GB
Active 1 day ago 0.26 GB
Active 1 day ago 0.05 GB
Rows per page: 20
Page 1 of 1


User List - Admin Console
https://admin.google.com/ac/users
Google Admin
Search for users, groups or settings
Users
All organizations
Users from all organizational units
Users from selected organizational units
Search for organizational units
Select multiple
zibasec.io
administrators
contractors
disable-2fa
Engineers
Finance
Founders
limited
New Hires
staff
MANAGE ORGANIZATIONAL UNITS
Users | Showing users from all organizational units
Add new user
Bulk update users
Download users
More
Add a filter
Name
Email
Status
Last sign in
Email usage
Add new user
First name *
Ada
Last name *
Lovelace
Primary email *
ada
@
zibasec.io
Organizational unit*
zibasec.io
Secondary email
Phone number
* indicates a required field
Automatically generate a password
Ask for a password change at the next sign-in
CANCEL
ADD NEW USER
Rows per page: 20
Page 1 of 1

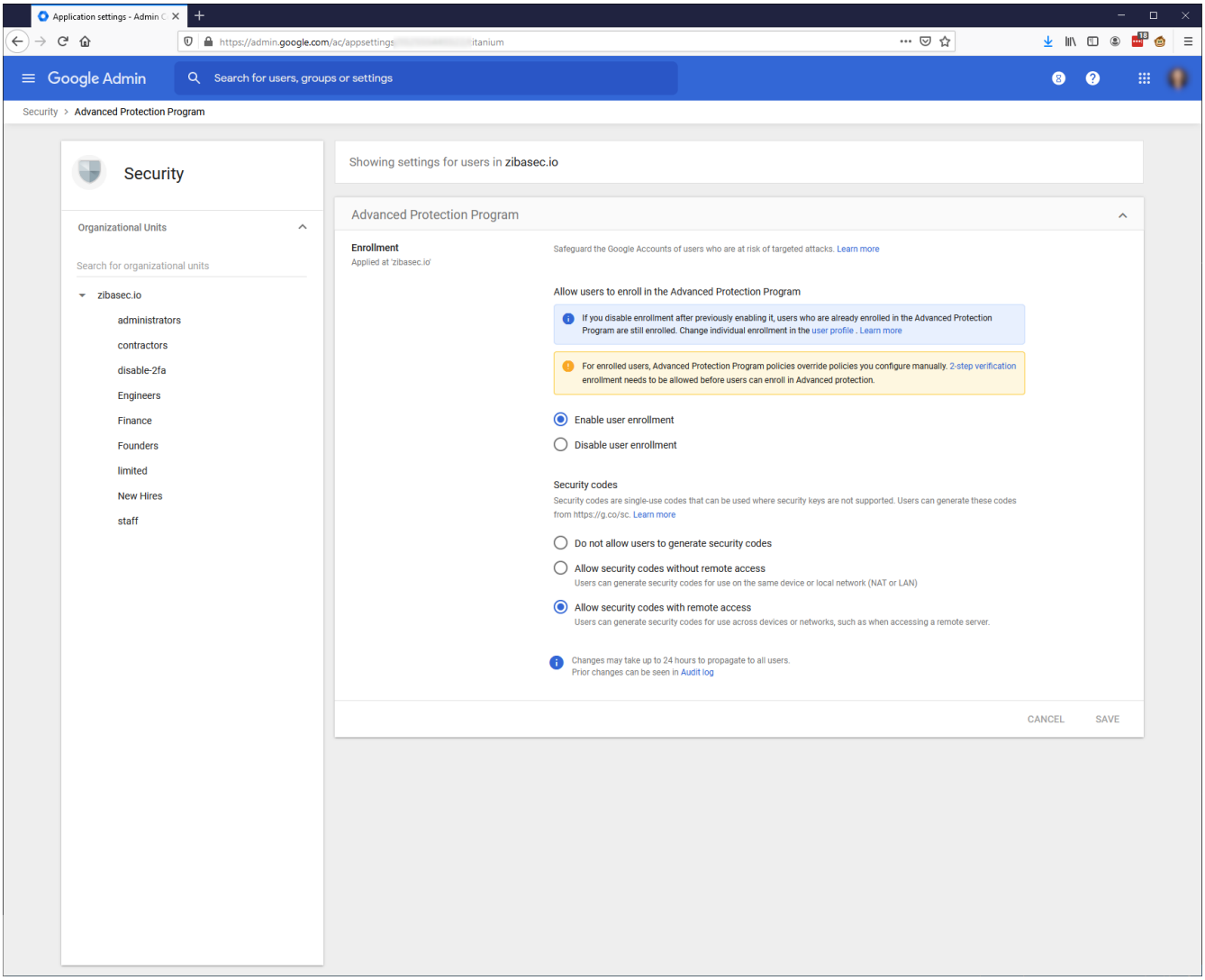


Securing the Admin User Account

It is imperative to secure the administration user of your Google account.

It is a good idea to have a separate user from the one you use day-to-day.

This admin user should have a secure passphrase, two-factor authentication enabled, and should likely be enrolled in the Advanced Protection Program.



IMPORTANT

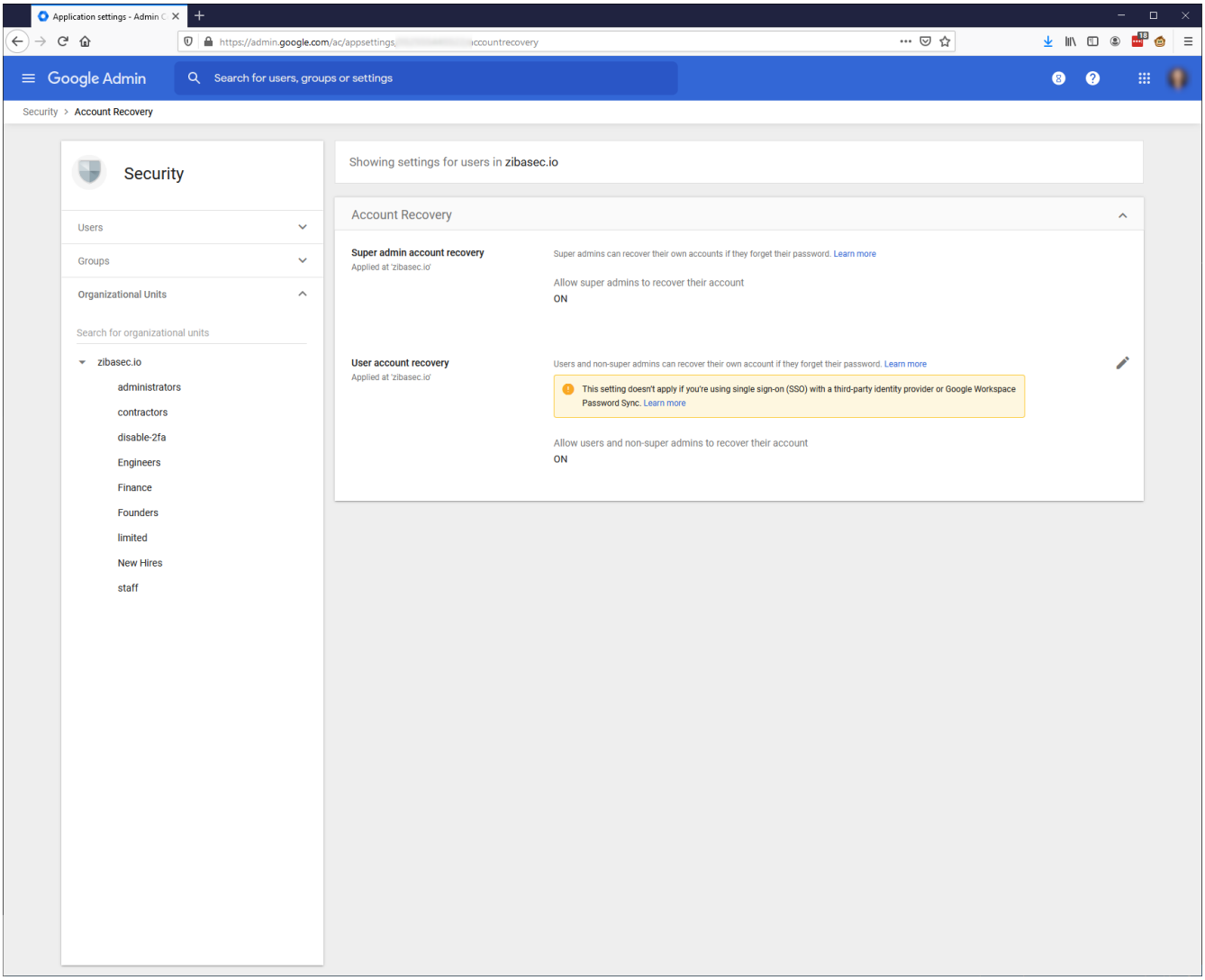
IMPORTANT: Secure your Admin Account

It is essential to secure your administrator account properly.

One setting that you can change on your super admin account is to disallow that account to recover its password.

This means you need to have multiple super admin accounts (preferably owned/managed by separate people), so that another super admin account can unlock the other.

You can also restrict regular users from recovering their accounts, thus needing and admin to unlock and reset the password.



Default Security Settings

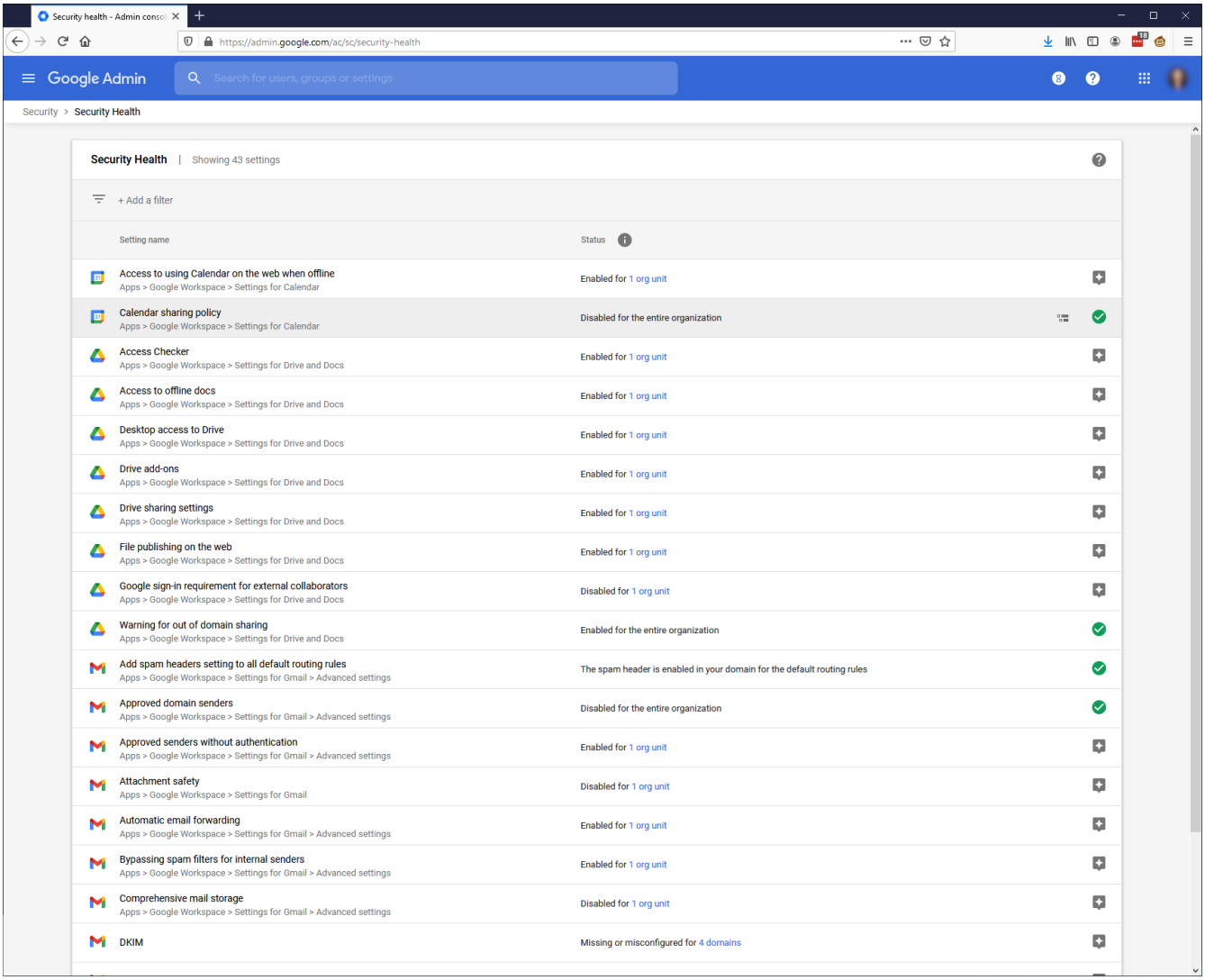
To further secure your organization's account, you can enable specific security settings.

Enable or Disable Features

You can enable and disable features of the Google platform on a user by user, group, or organizational unit.

- Calendar
- Drive
  - Offline Docs
  - Publish on the web
  - Sharing settings
- Mail
  - Approved domain senders
  - Automatic email forwarding
  - Attachment safety.

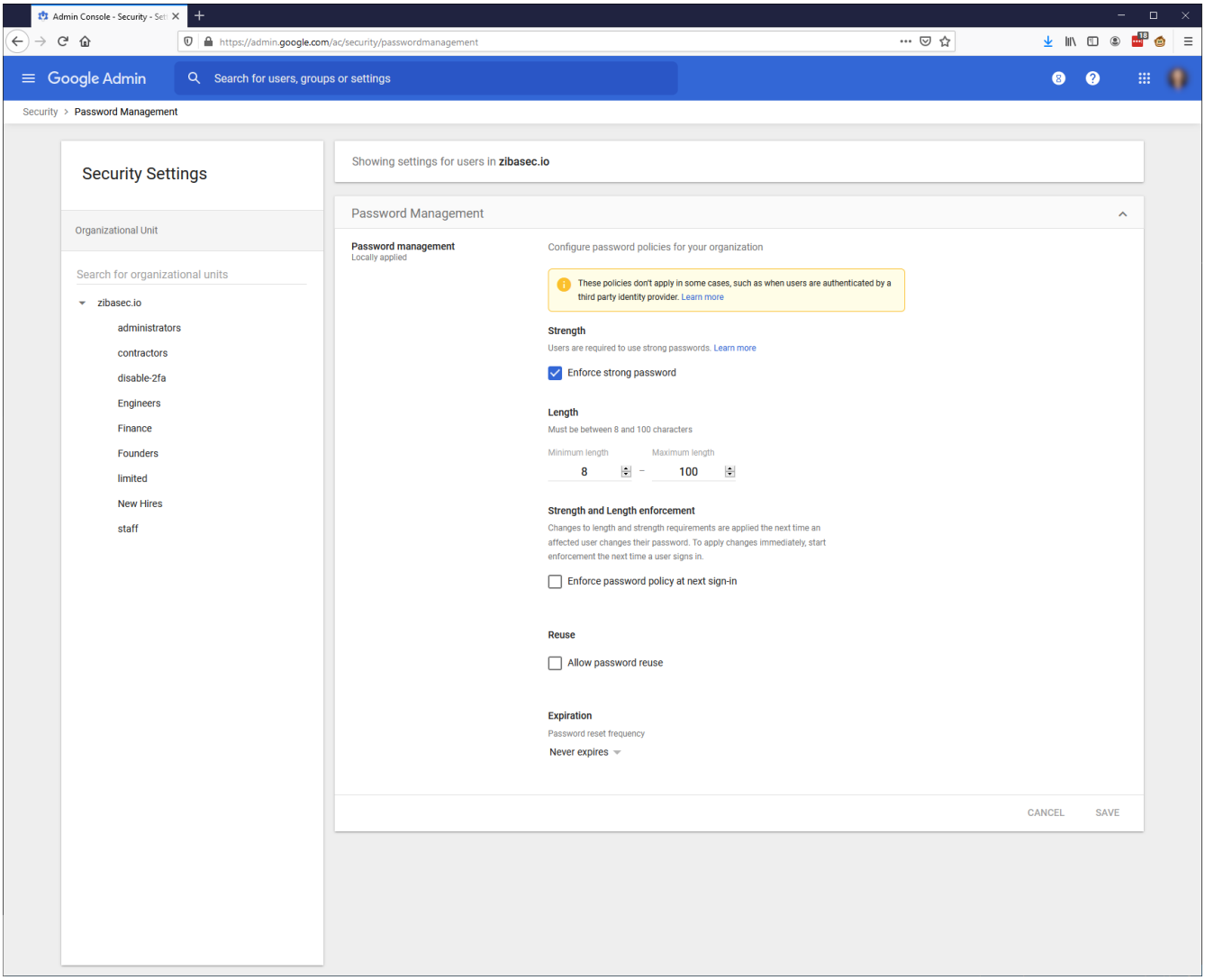
These are just a few of the possible options you can enable or disable in your account.



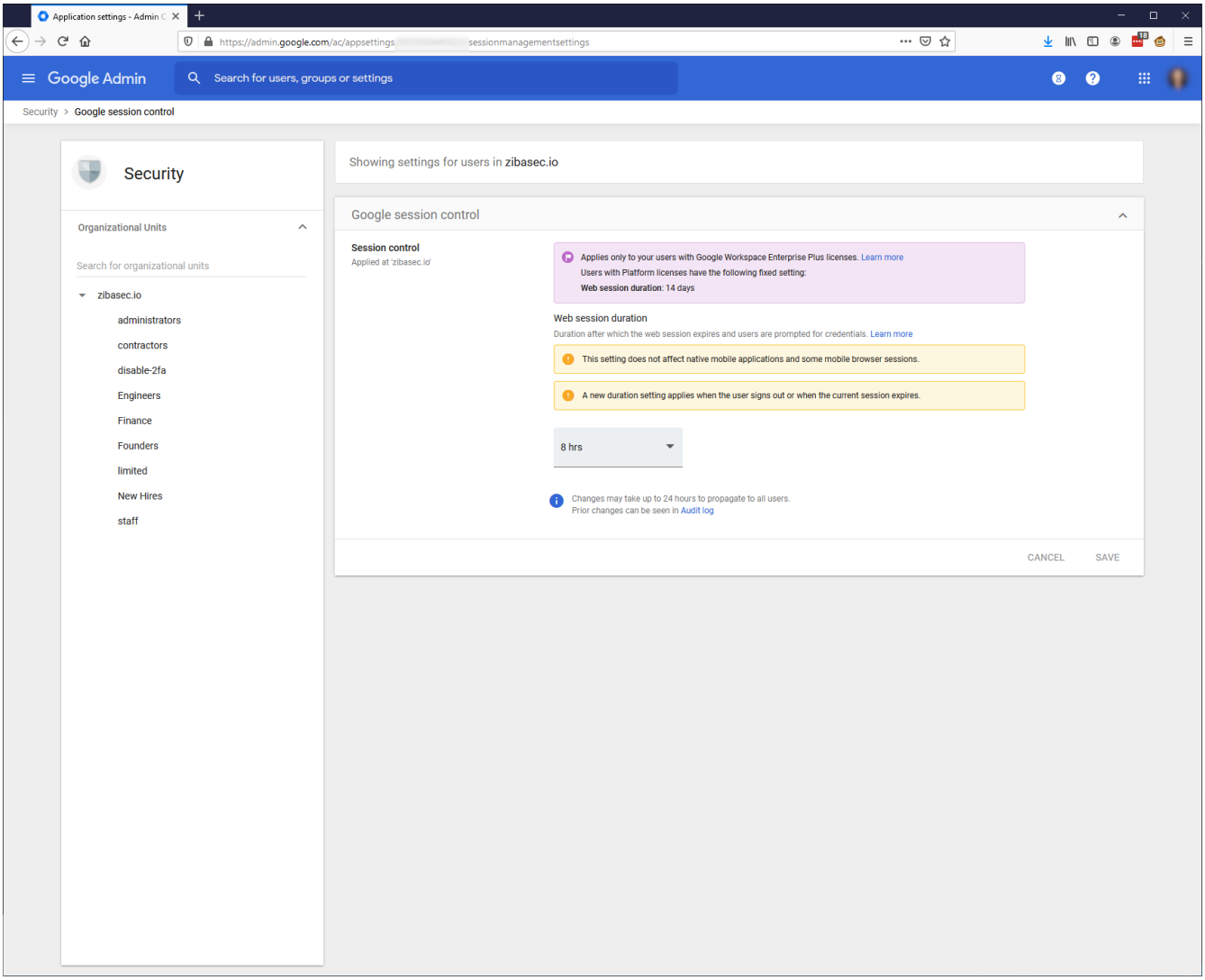
Password and Login Settings

Password and login policies are a typical setting you can also find in your Google account.

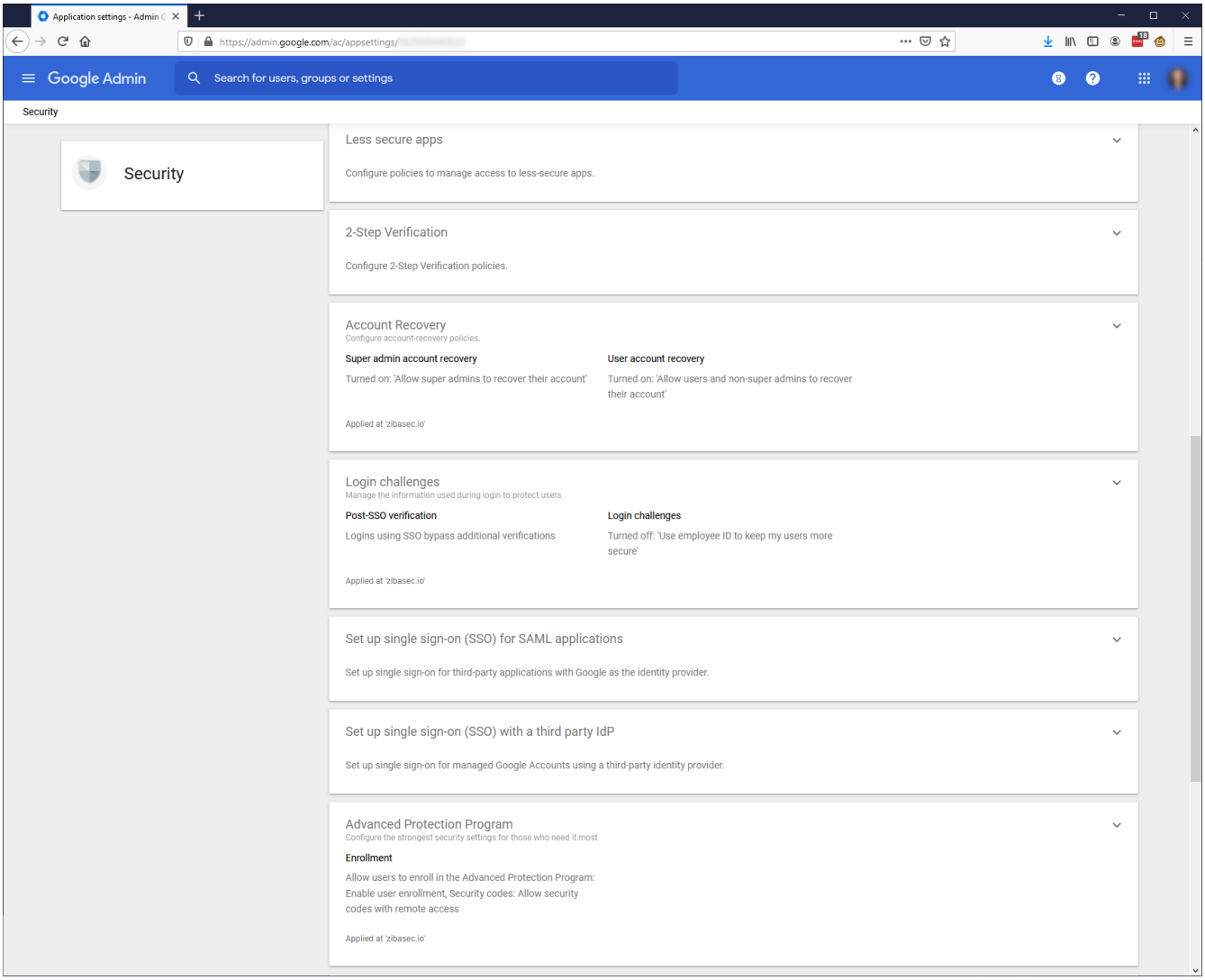
You can force strong passwords, disable password re-use, and cause password resets on a regular schedule.

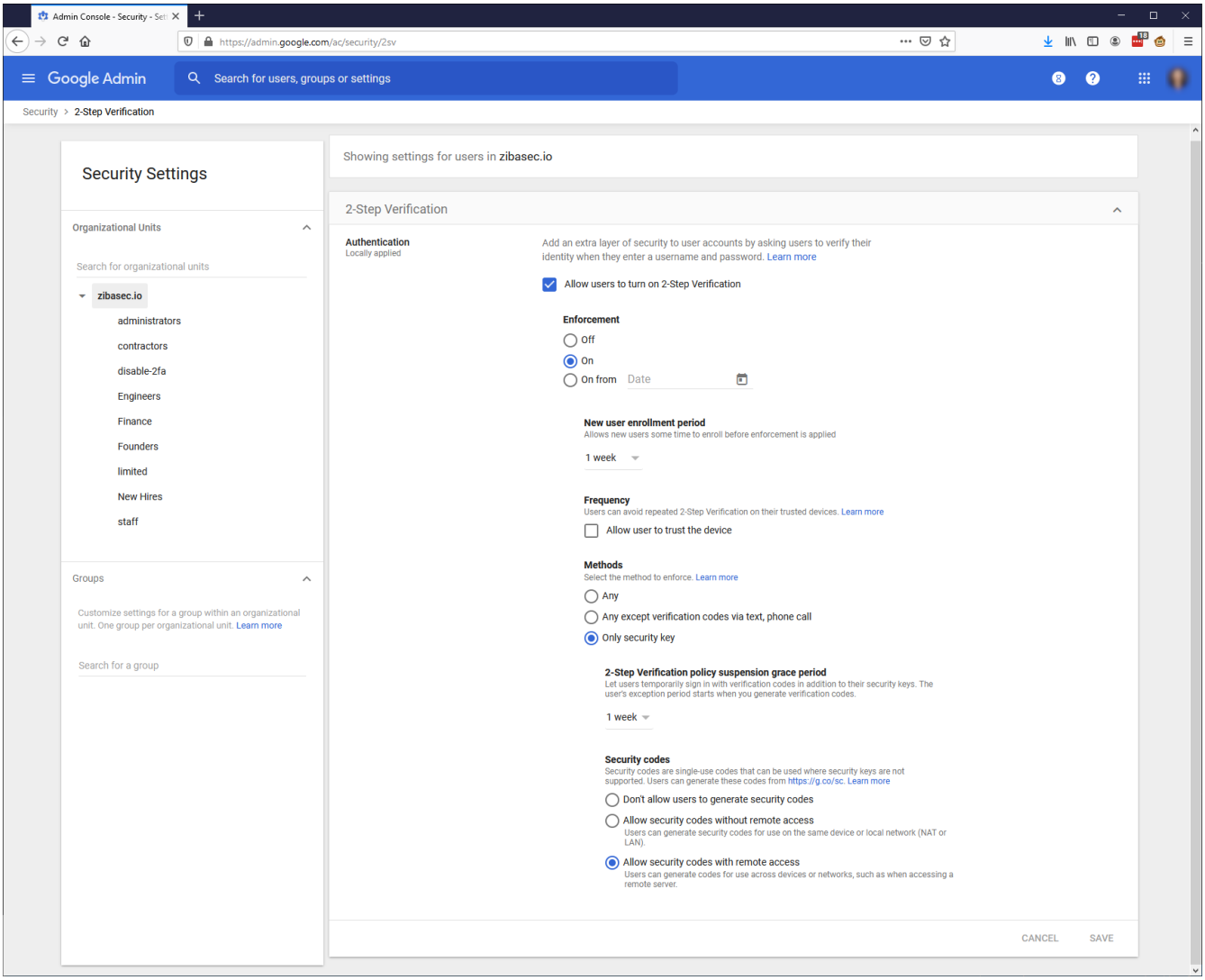


You can force a session to expire after a set amount of time.

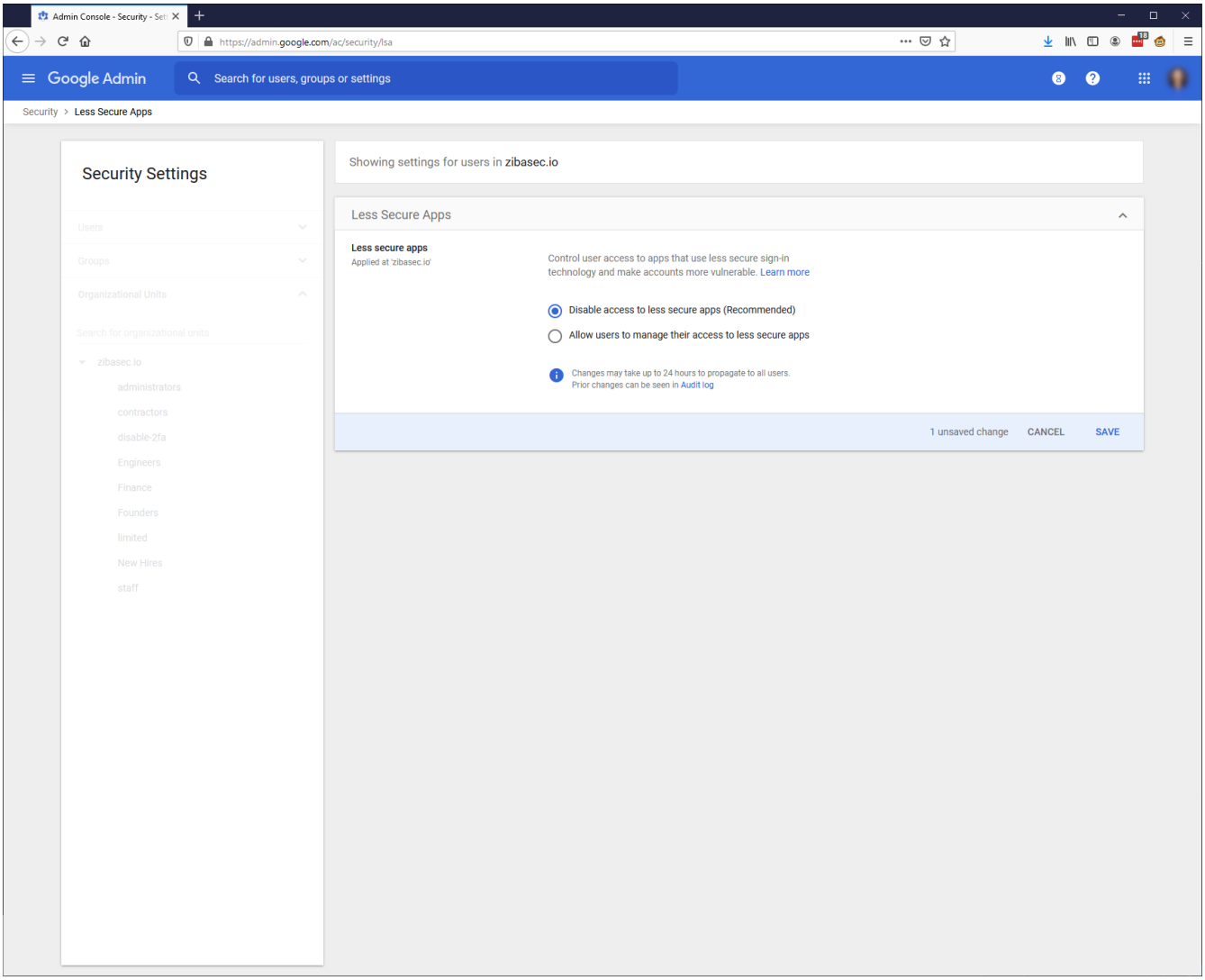


You can enforce that accounts have two-factor auth enabled.

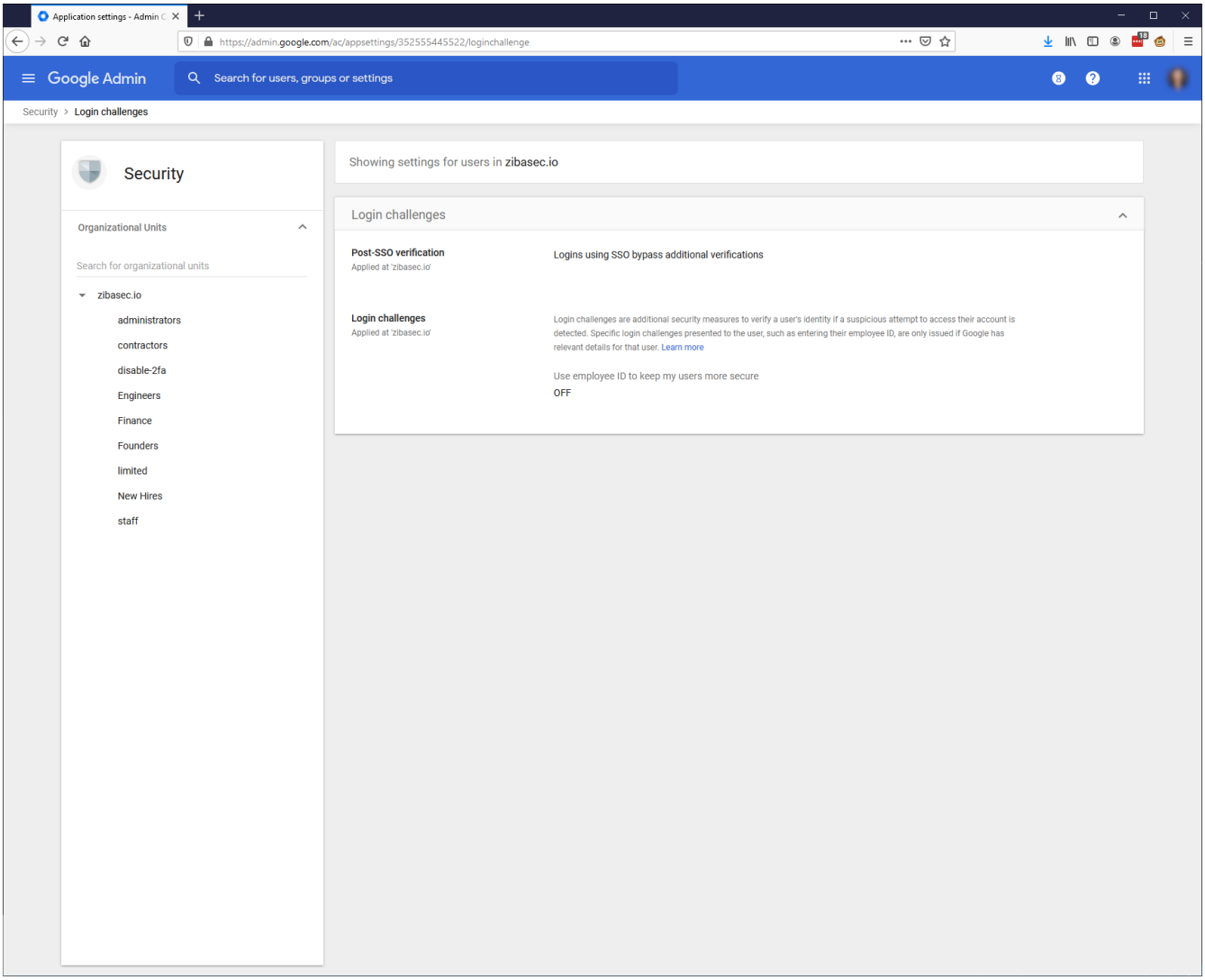

Application settings - Admin
https://admin.google.com/ac/appsettings/
Google Admin
Search for users, groups or settings
Security
Security
Less secure apps
Configure policies to manage access to less-secure apps.
2-Step Verification
Configure 2-Step Verification policies.
Account Recovery
Configure account-recovery policies.
Super admin account recovery
Turned on: 'Allow super admins to recover their account'
User account recovery
Turned on: 'Allow users and non-super admins to recover their account'
Applied at 'zibasec.io'
Login challenges
Manage the information used during login to protect users.
Post-SSO verification
Logins using SSO bypass additional verifications
Login challenges
Turned off: 'Use employee ID to keep my users more secure'
Applied at 'zibasec.io'
Set up single sign-on (SSO) for SAML applications
Set up single sign-on for third-party applications with Google as the identity provider.
Set up single sign-on (SSO) with a third party IdP
Set up single sign-on for managed Google Accounts using a third-party identity provider.
Advanced Protection Program
Configure the strongest security settings for those who need it most
Enrollment
Allow users to enroll in the Advanced Protection Program: Enable user enrollment, Security codes: Allow security codes with remote access
Applied at 'zibasec.io'



You can disable access from "Less Secure Apps," such as third-party clients that don’t meet Google’s security standards.



You can enable "Login challenges", which will do extended verification (such as employee ID) if the login seems suspicious.



Context Aware Access

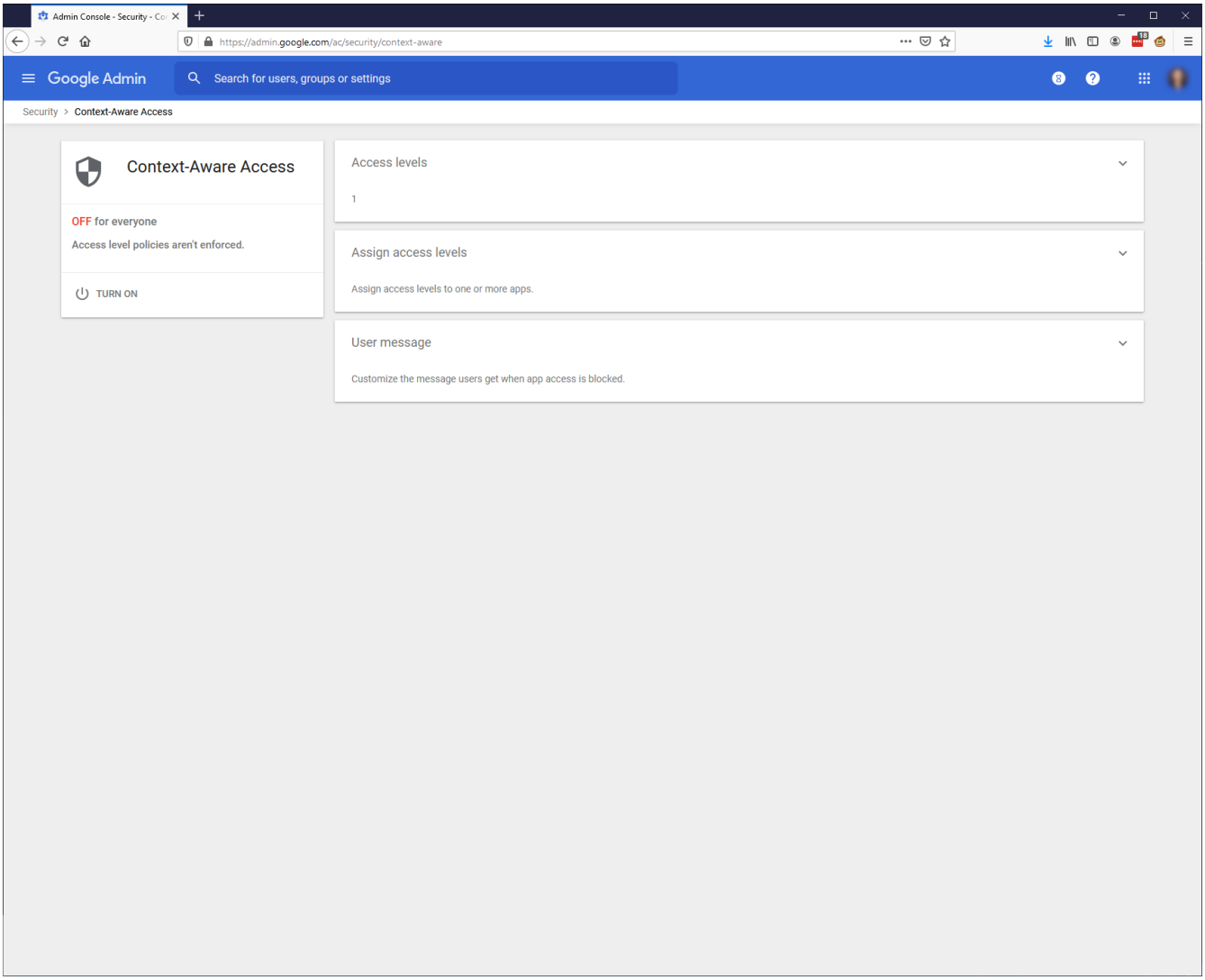
Advanced context-aware access rules are also an option.

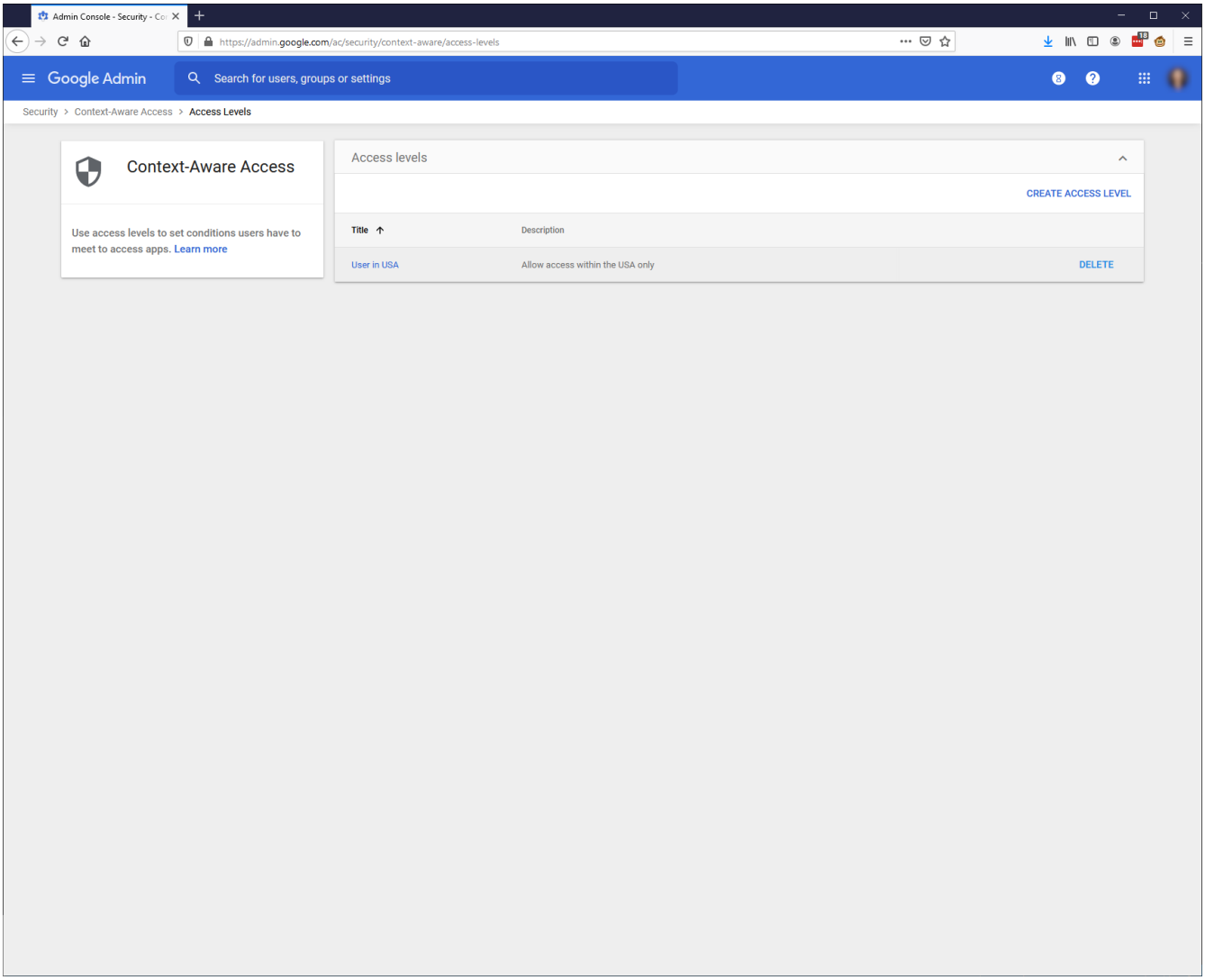
You can set up rules that, when matched, require additional security.

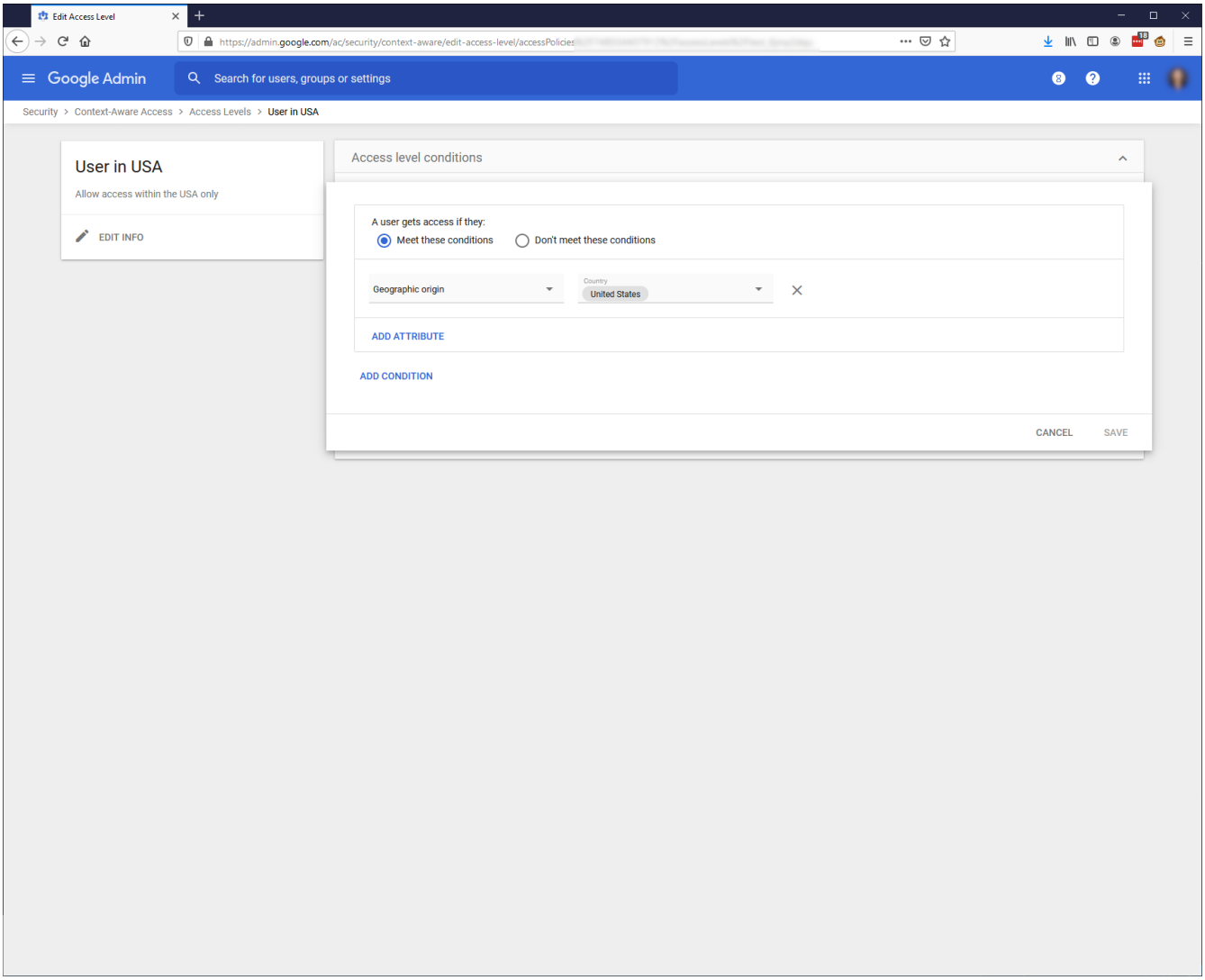
First, you set access levels; tied to accounts/OUs or groups.

Then an access level is configured with one or more rules.

For example, if you wanted to create an access level 1 which limits logins to IP addresses from the US only.


Admin Console - Security - Co
https://admin.google.com/ac/security/context-aware
Google Admin
Search for users, groups or settings
Security > Context-Aware Access
Context-Aware Access
OFF for everyone
Access level policies aren't enforced.
TURN ON
Access levels
1
Assign access levels
Assign access levels to one or more apps.
User message
Customize the message users get when app access is blocked.

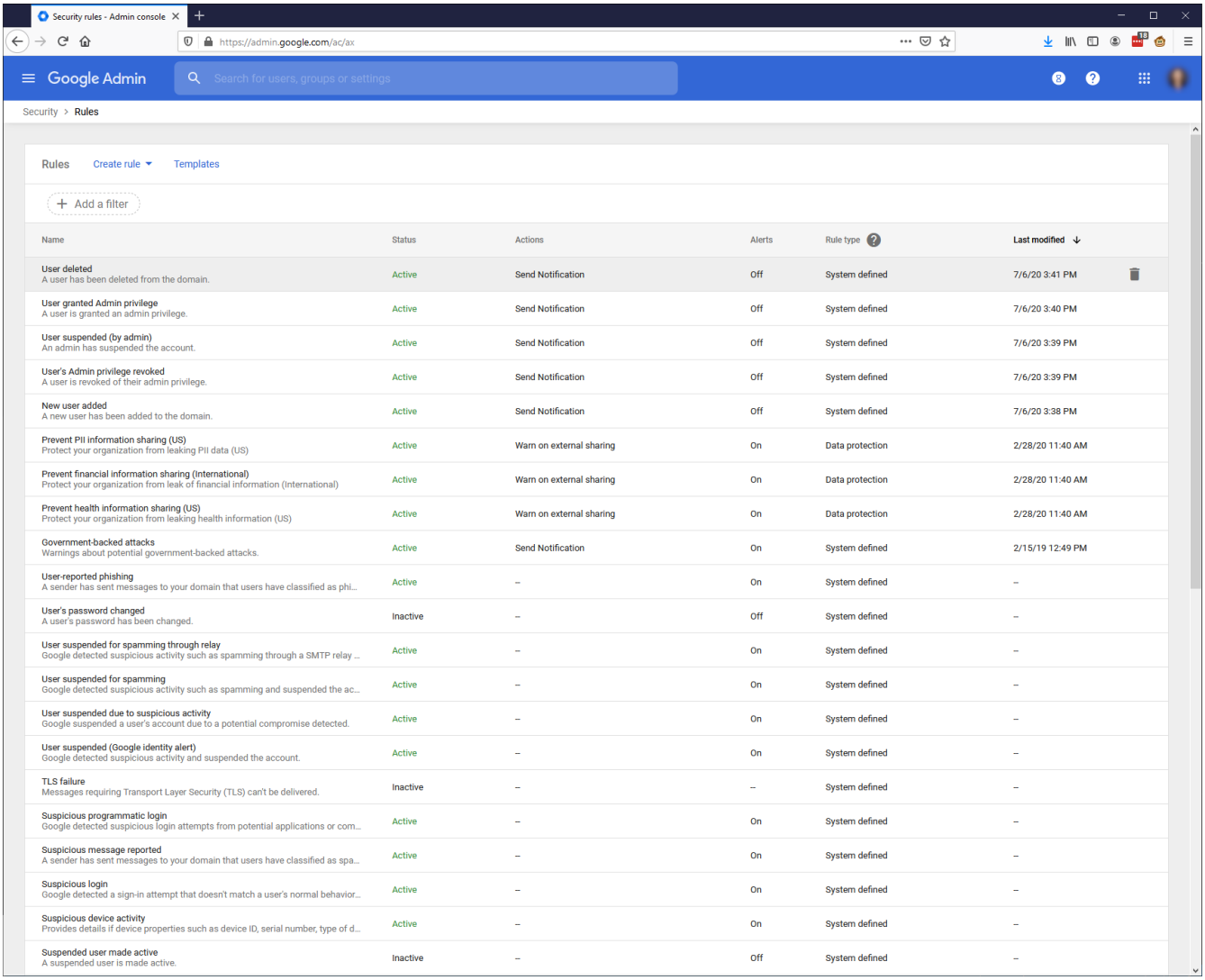

Admin Console - Security - Co
https://admin.google.com/ac/security/context-aware/access-levels
Google Admin
Search for users, groups or settings
Security > Context-Aware Access > Access Levels
Context-Aware Access
Use access levels to set conditions users have to meet to access apps. Learn more
Access levels
CREATE ACCESS LEVEL
Title
Description
User in USA
Allow access within the USA only
DELETE



Advanced Rules

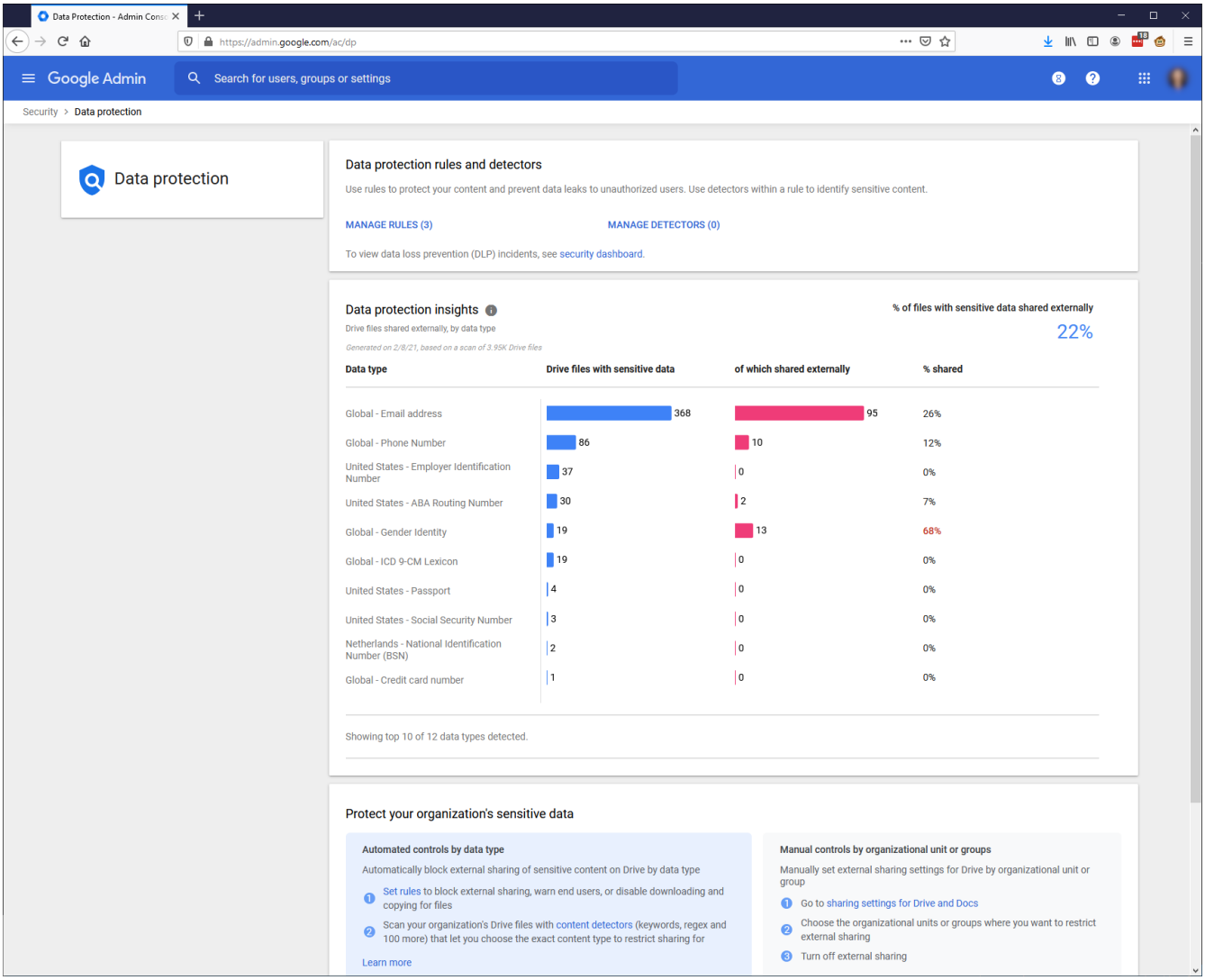
If the above settings don't cover your needs, you can also define more advanced specific rules.

This page is where you can also tie in audit events to warn about security issues.



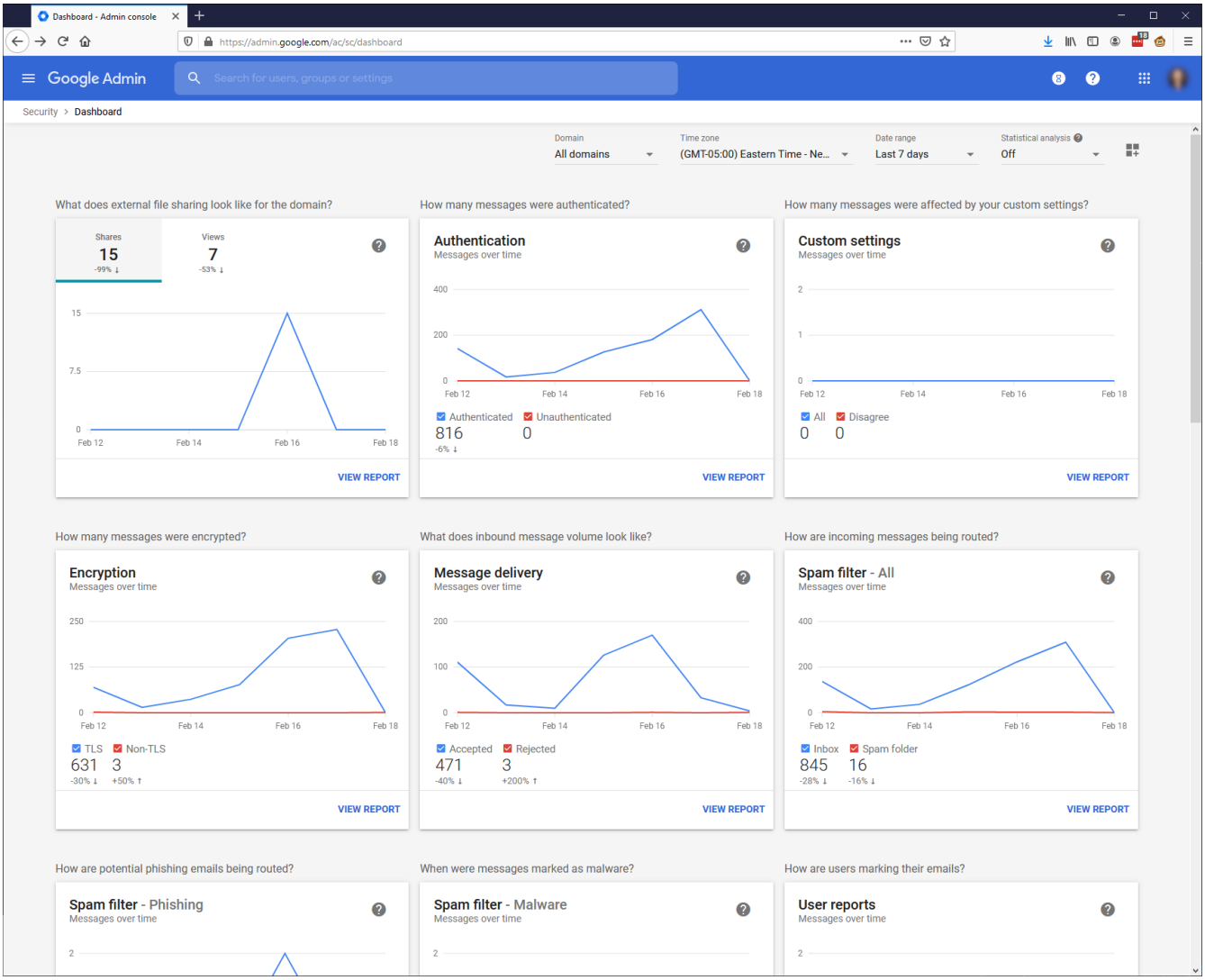
Data Protection

Google will monitor the data in your account and generate a report on what types of data are there, and how much of each type has been shared.



Monitoring Dashboard

There is also a monitoring dashboard with some important metrics.

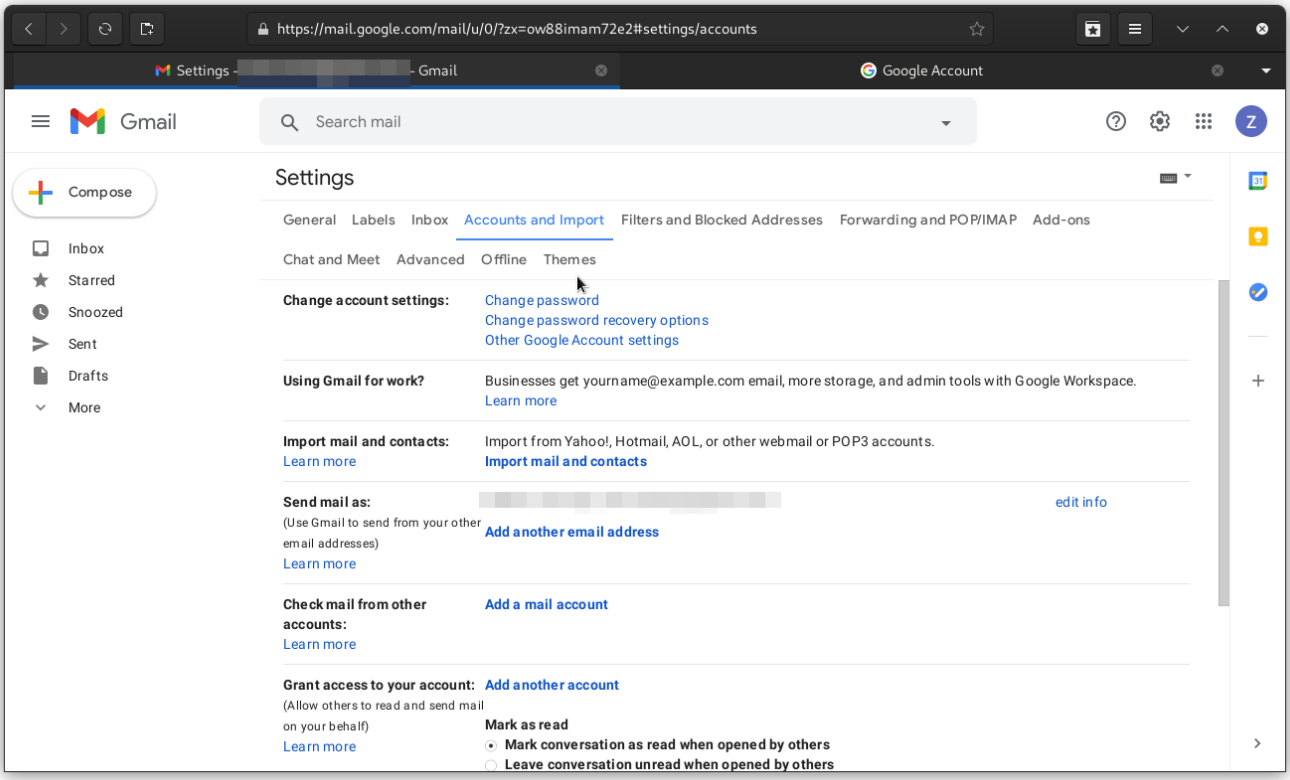

Dashboard - Admin console
https://admin.google.com/ac/sc/dashboard
Google Admin
Search for users, groups or settings
Security > Dashboard
Domain
All domains
Time zone
(GMT-05:00) Eastern Time - Ne...
Date range
Last 7 days
Statistical analysis
Off
What does external file sharing look like for the domain?
Shares
15
-99% ↓
Views
7
-53% ↓
15
7.5
0
Feb 12
Feb 14
Feb 16
Feb 18
VIEW REPORT
How many messages were authenticated?
Authentication
Messages over time
400
200
0
Feb 12
Feb 14
Feb 16
Feb 18
Authenticated
Unauthenticated
816
-6% ↓
0
VIEW REPORT
How many messages were affected by your custom settings?
Custom settings
Messages over time
2
1
0
Feb 12
Feb 14
Feb 16
Feb 18
All
Disagree
0
0
VIEW REPORT
How many messages were encrypted?
Encryption
Messages over time
250
125
0
Feb 12
Feb 14
Feb 16
Feb 18
TLS
Non-TLS
631
-30% ↓
3
+50% ↑
VIEW REPORT
What does inbound message volume look like?
Message delivery
Messages over time
200
100
0
Feb 12
Feb 14
Feb 16
Feb 18
Accepted
Rejected
471
-40% ↓
3
+200% ↑
VIEW REPORT
How are incoming messages being routed?
Spam filter - All
Messages over time
400
200
0
Feb 12
Feb 14
Feb 16
Feb 18
Inbox
Spam folder
845
-28% ↓
16
-16% ↓
VIEW REPORT
How are potential phishing emails being routed?
Spam filter - Phishing
Messages over time
2
When were messages marked as malware?
Spam filter - Malware
Messages over time
2
How are users marking their emails?
User reports
Messages over time
2

Securing a `gmail.com` Email Account

> As Gmail is a common Email provider, this module will walk you through some basic security settings you should enable and use on your account.

Most of these options and settings exist as part of the Google account.

Click through the settings to "Other Google Account Settings" to find them:



Choosing a Passphrase

The first step of securing an online account is to have a secure password/passphrase.

A passphrase of multiple words is usually easier to remember and more secure.

Look at the "Authentication" module of this training course for details.

IMPORTANT

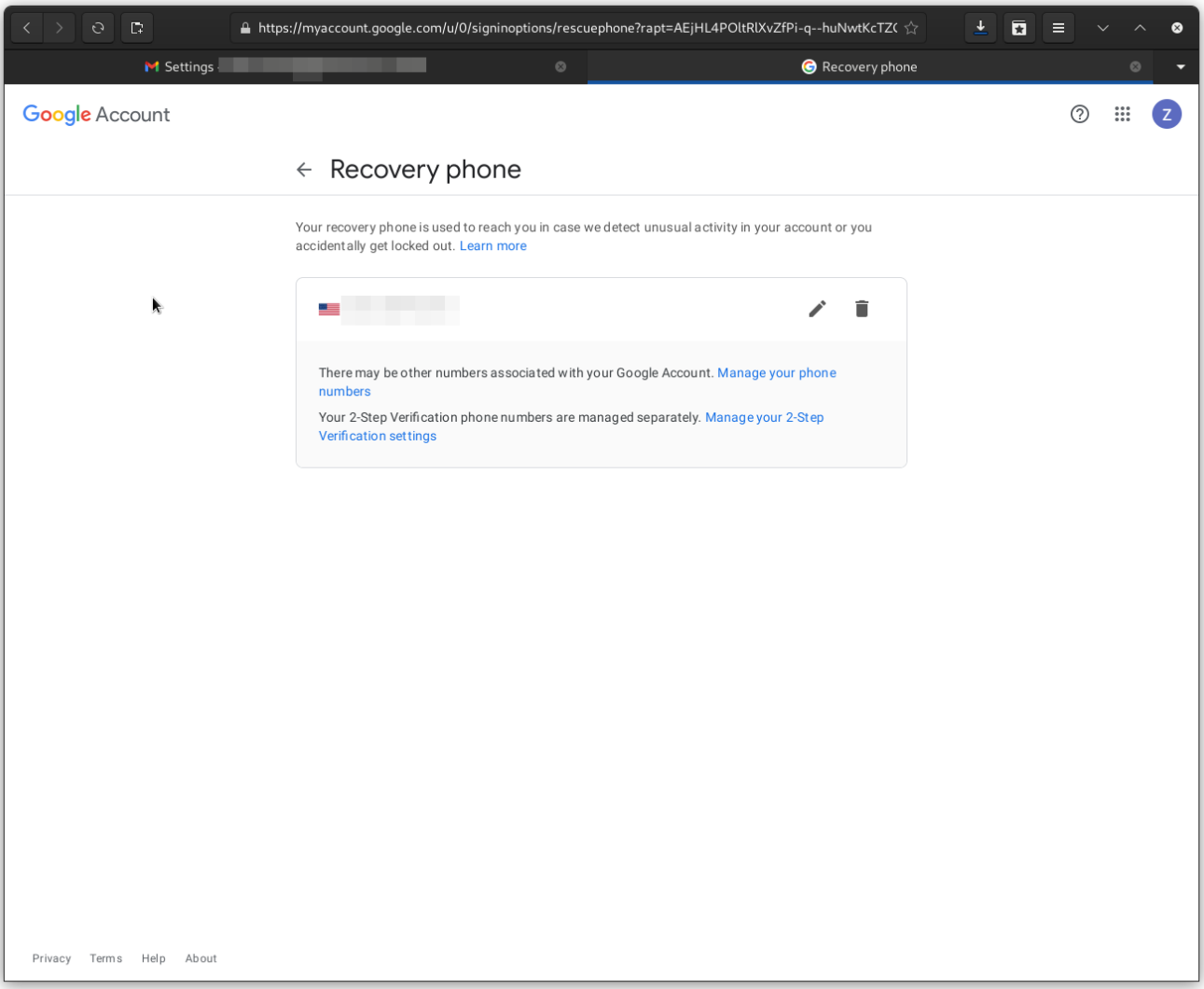
IMPORTANT: Use a Password Manager

Using a Password Manager is a more secure way to ensure you have the highest security passwords for an account.

Look for more information in the "Password Manager" module of this training.

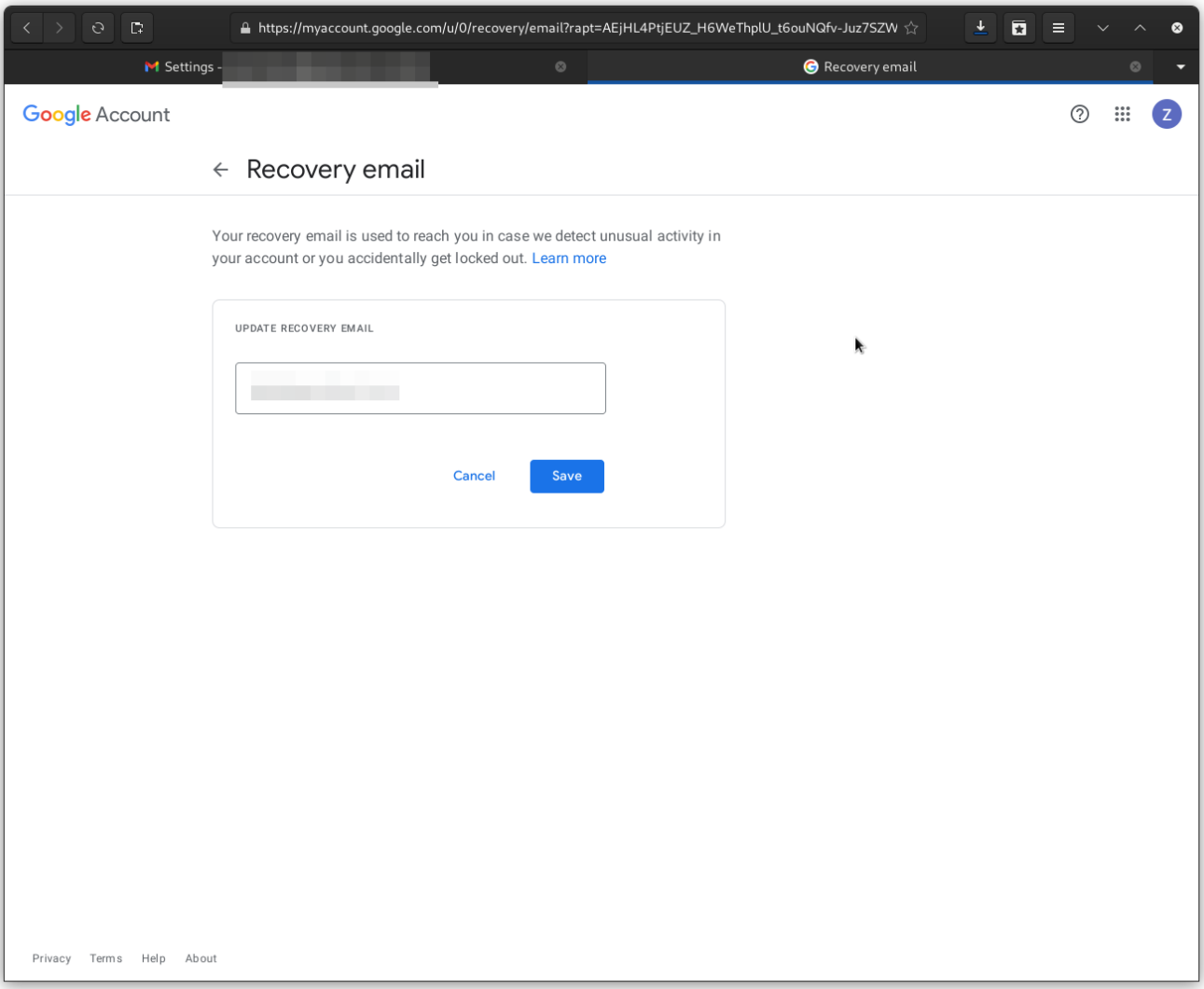
Associate a Phone Number to the Account

Adding a mobile number to the account gives you one more way to recover or verify your account.



Setup a Secure Recovery Email Address

One of the security features of a Gmail account is the recovery email address. Use this address if you are locked out of your account and need to reset the password or verify that you are the account owner.



You should choose an address where you have complete trust, as this is essentially a back-door into your Gmail account.

TIP

TIP

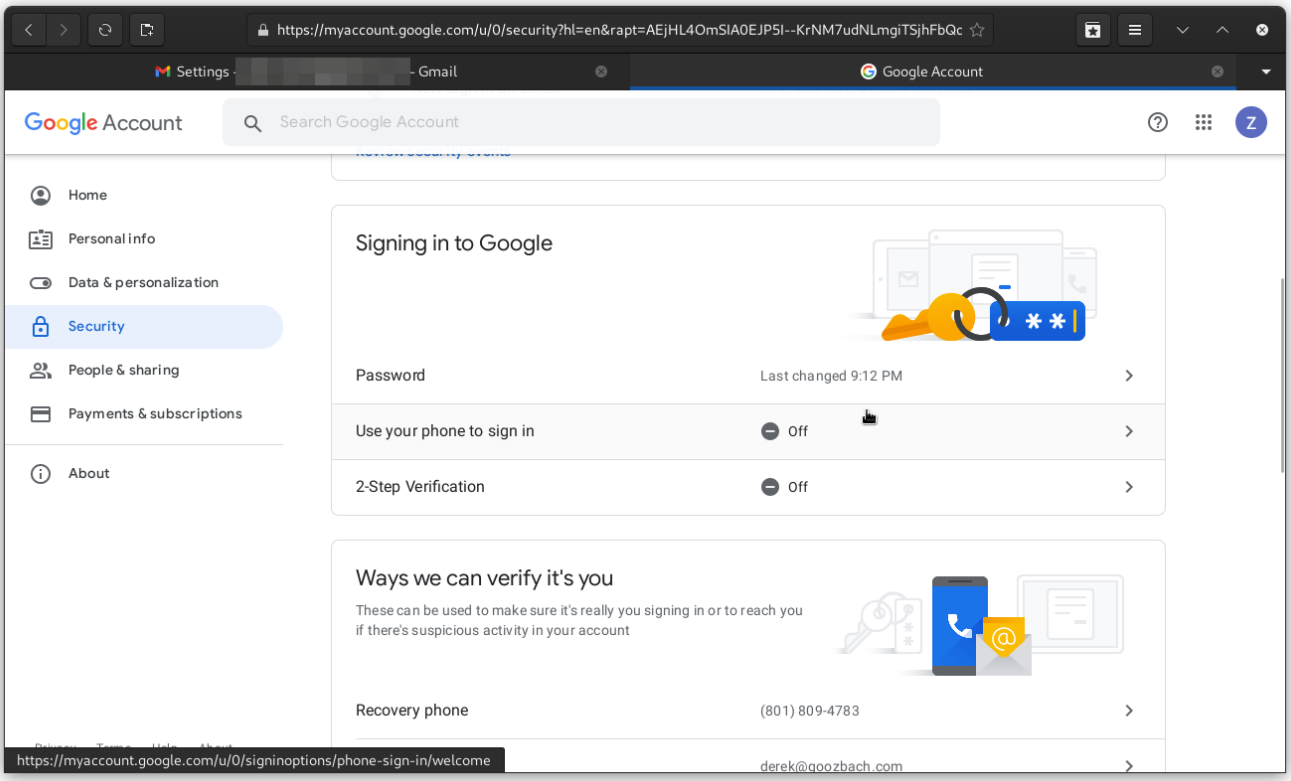
Use another personal account on a different provider for the highest level of security.

Turn on Multi-Factor Authentication (MFA)

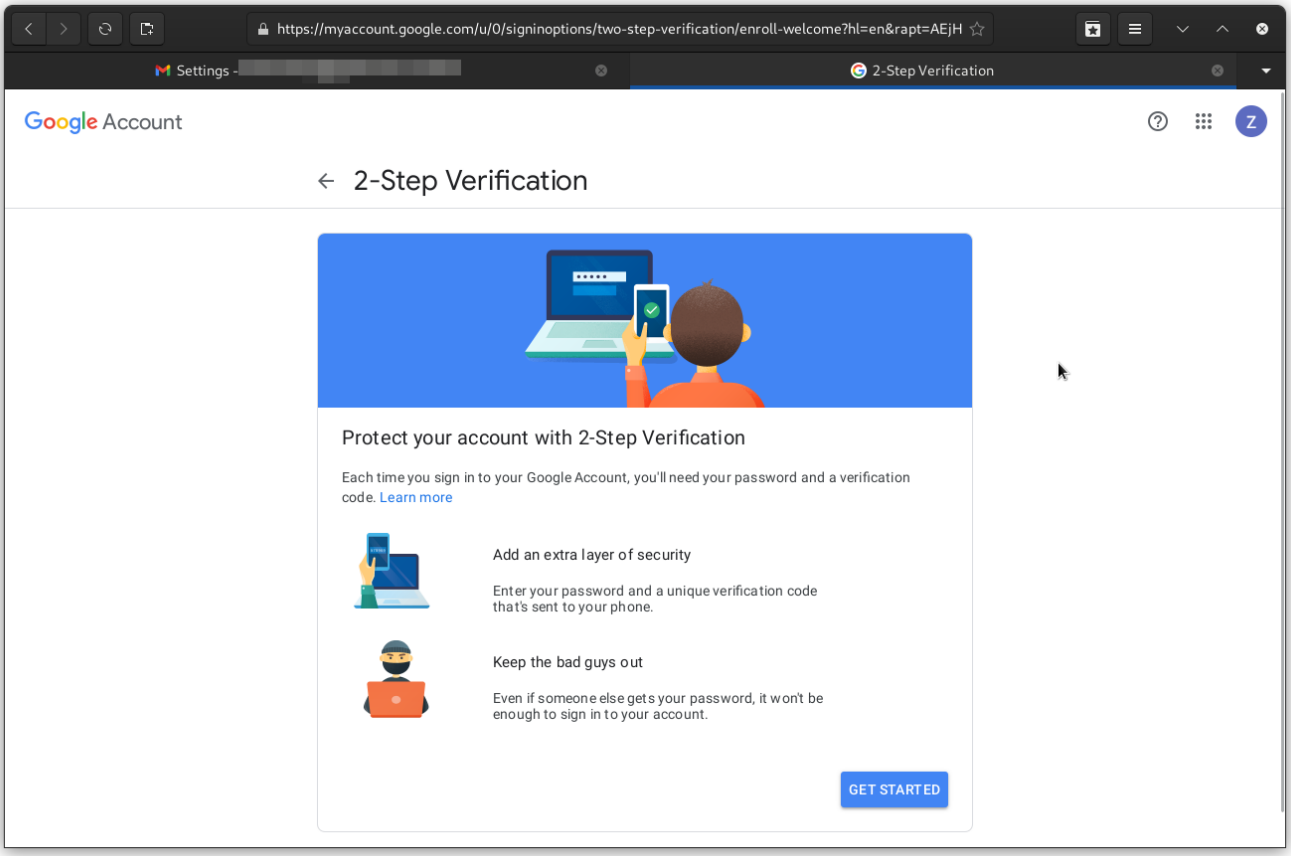
Compromised logins to your accounts are more likely if you don't have Multi-Factor Authentication(MFA) enabled. It would be best if you turned on MFA on your account.

Setup MFA

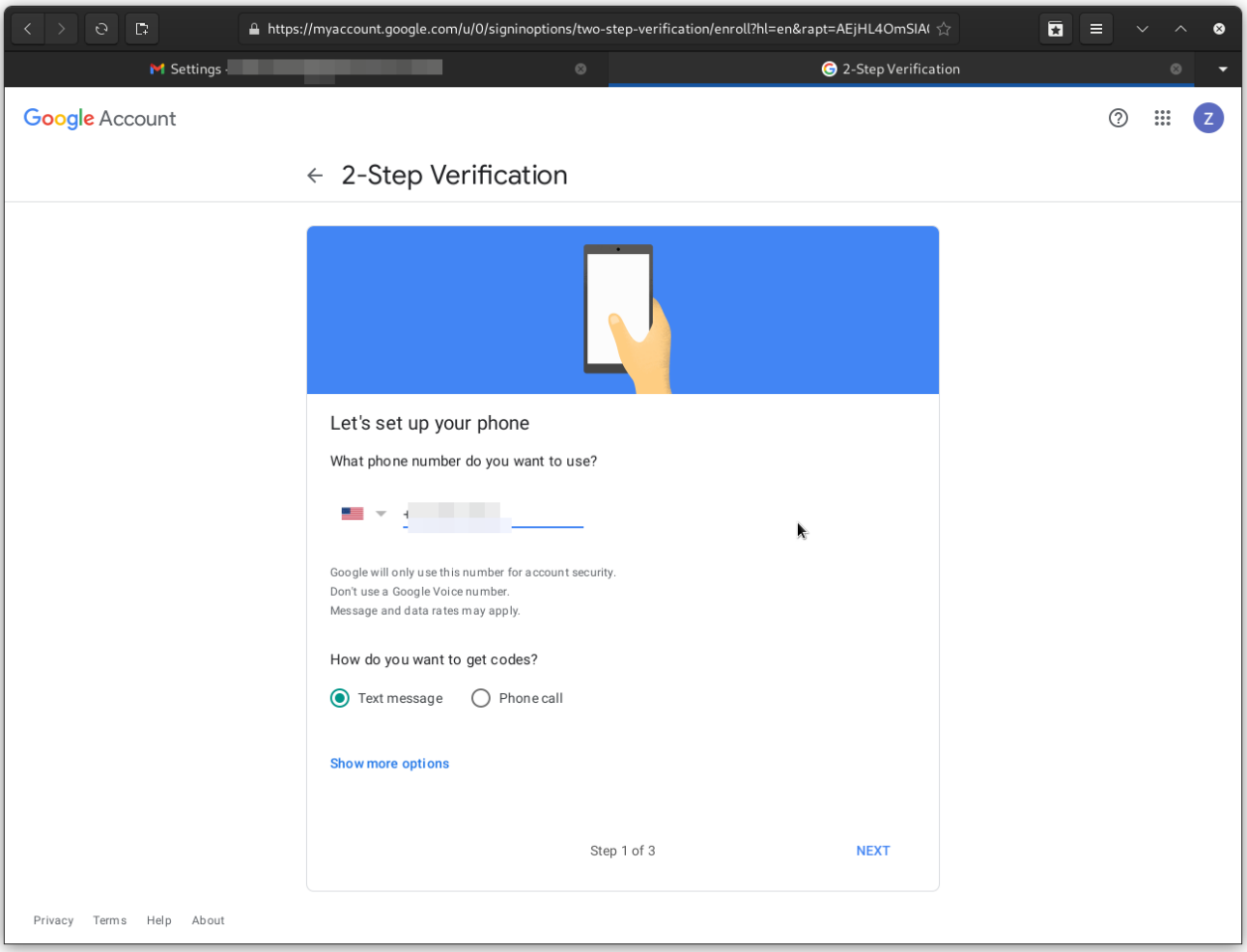
Start the enrollment of 2-Step (MFA) from the Google Account menu:



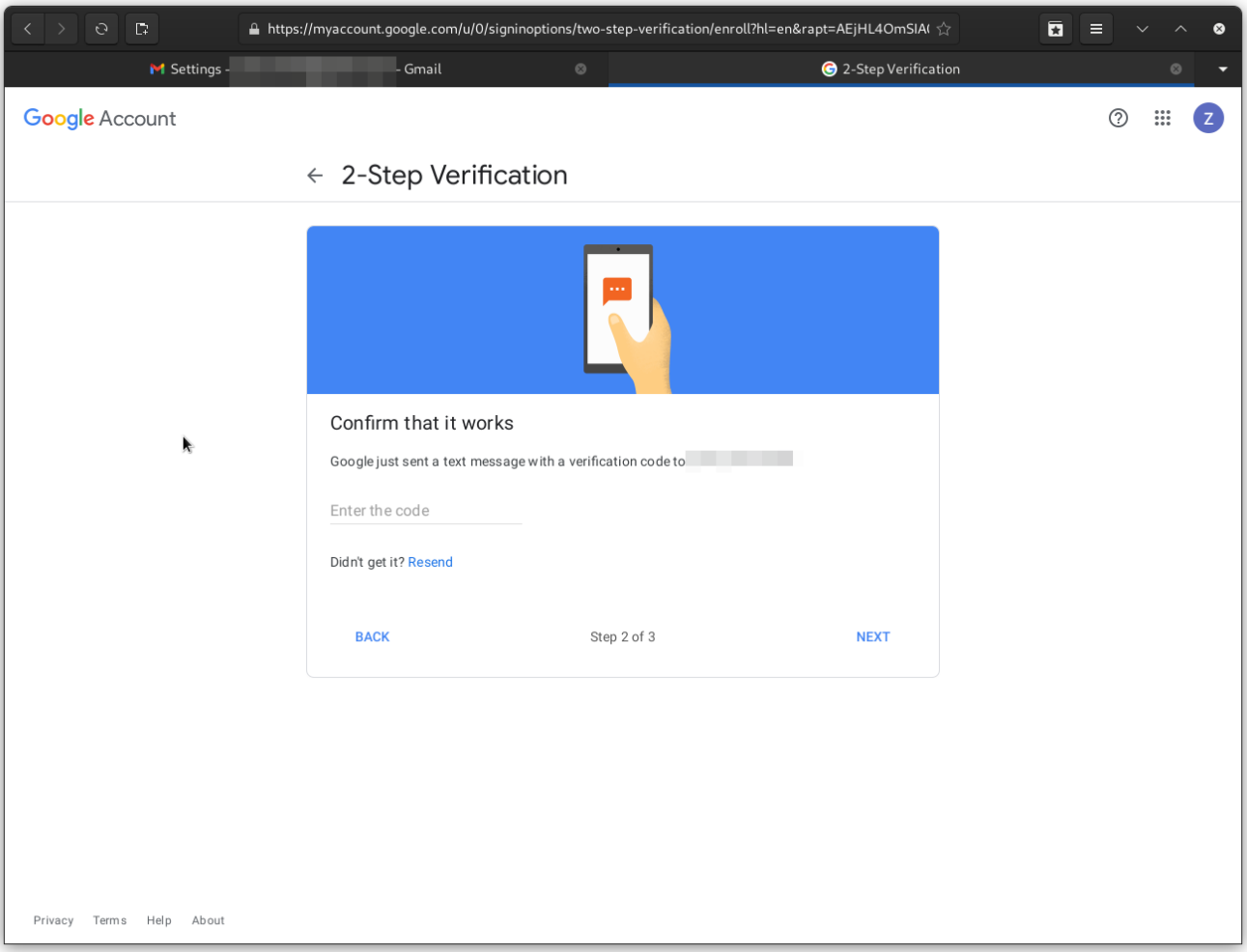
Choose 2-step Verification from the settings menu:



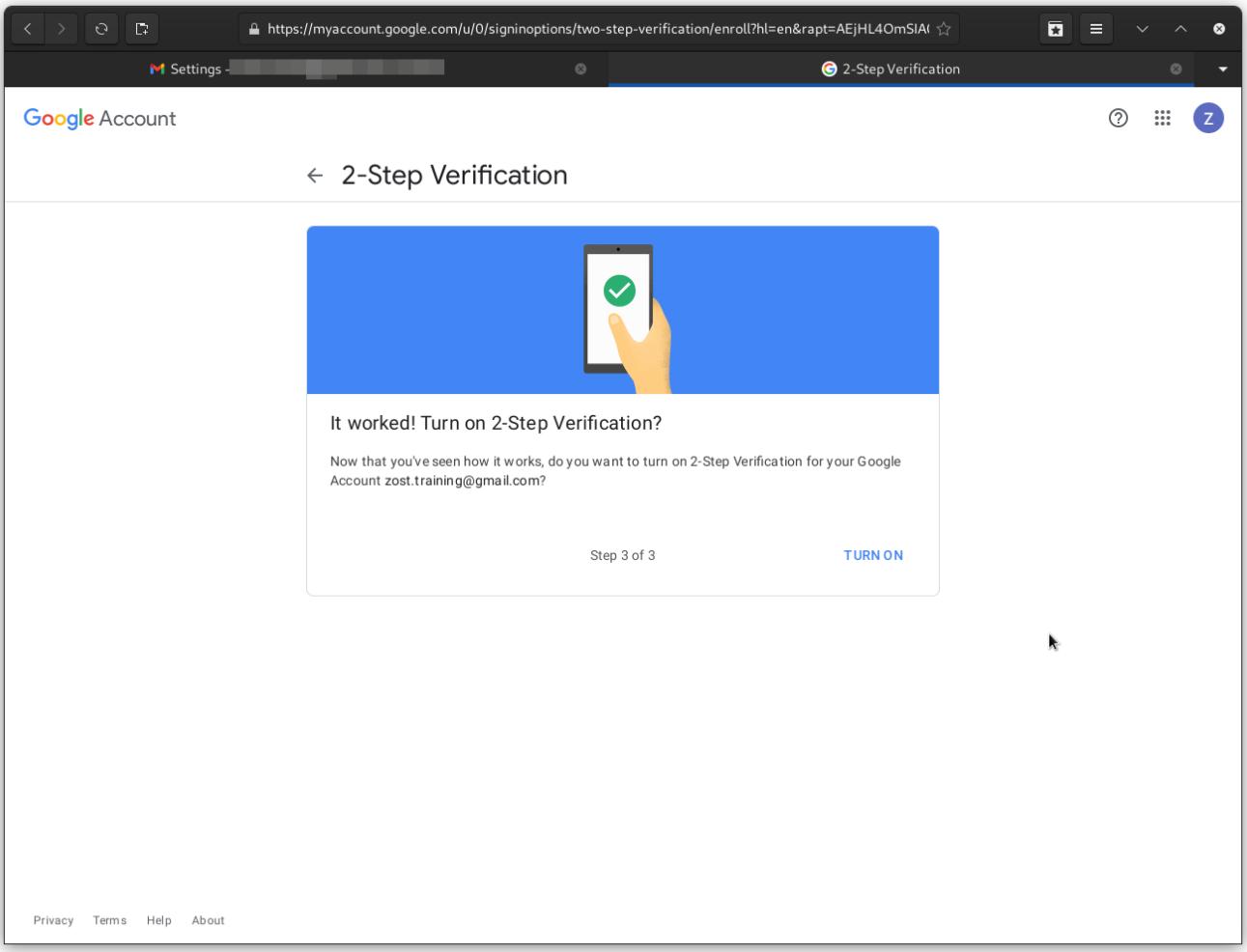
You'll have to choose your phone as the first MFA option:



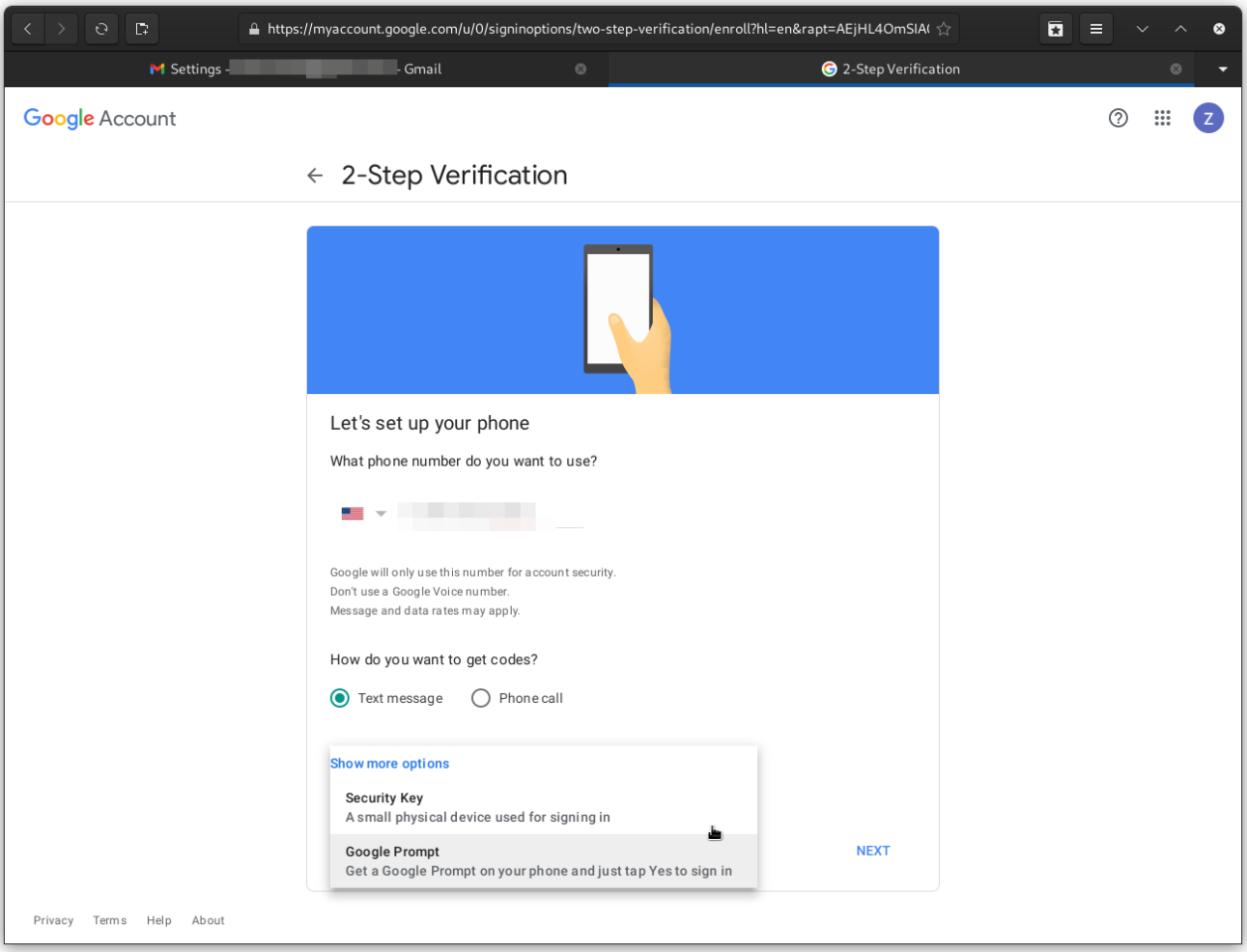
The second step is to verify the code sent to your phone:



The last step is to complete the MFA enrollment and turn it on for your account:



Other options include hardware tokens or a Google Prompt (If you are signed in to Google on your phone):

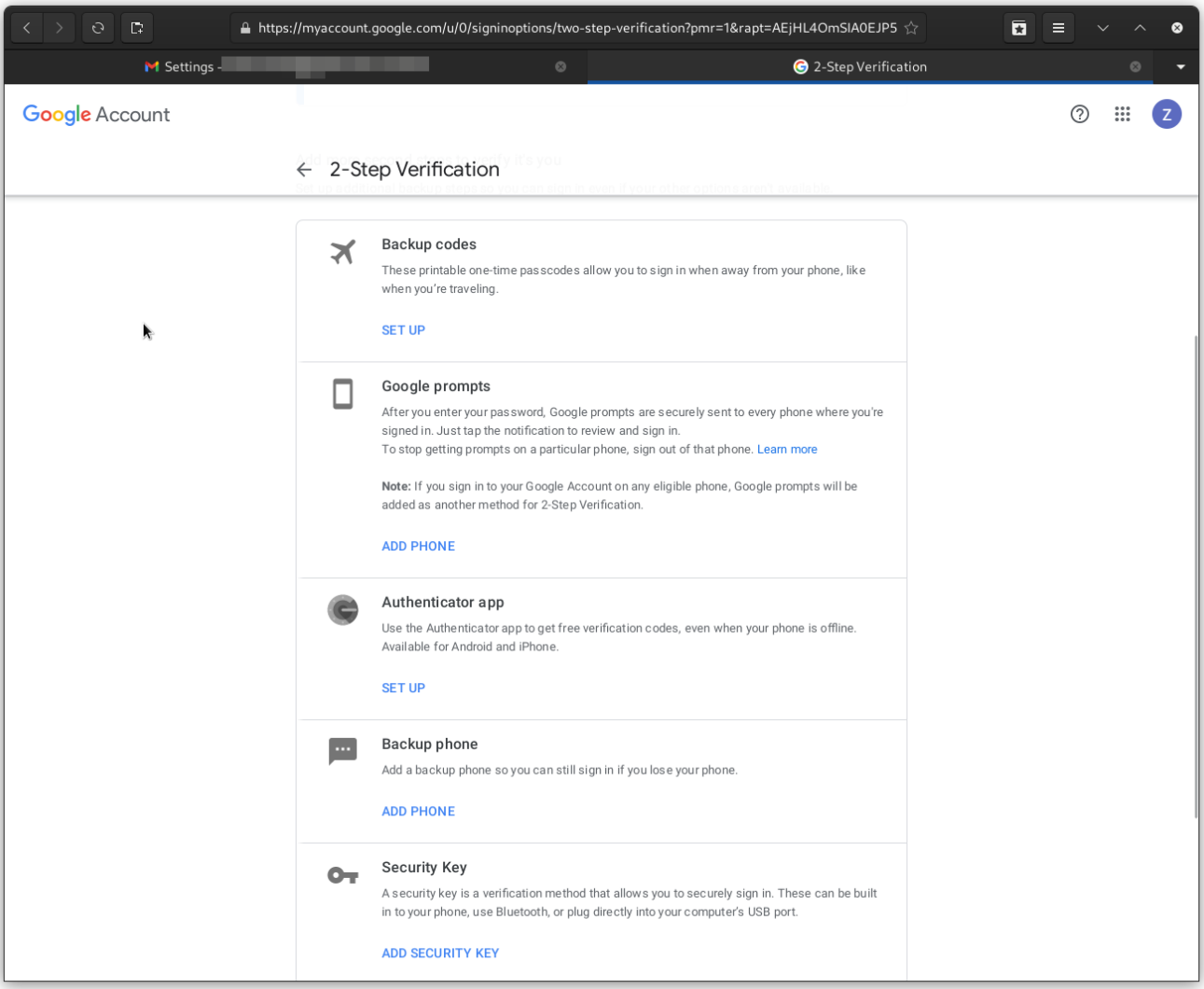


Generate Backup Codes

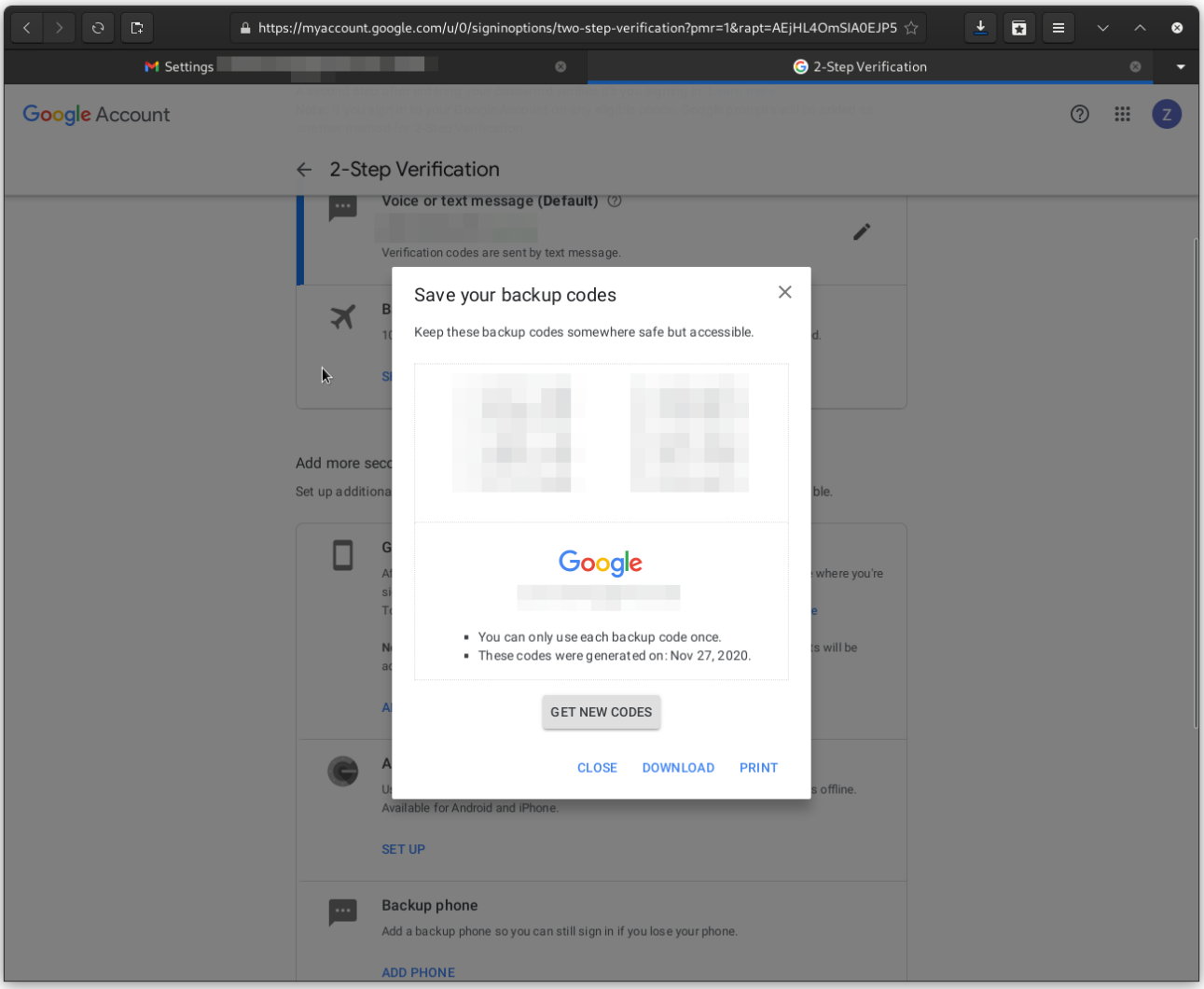
When you turn on 2-step (MFA) on your account, you need a way to access the account if your second factor fails.

The easiest way to do this is to generate some one-time "Backup Codes".

Select "Backup Codes" from the account settings page:

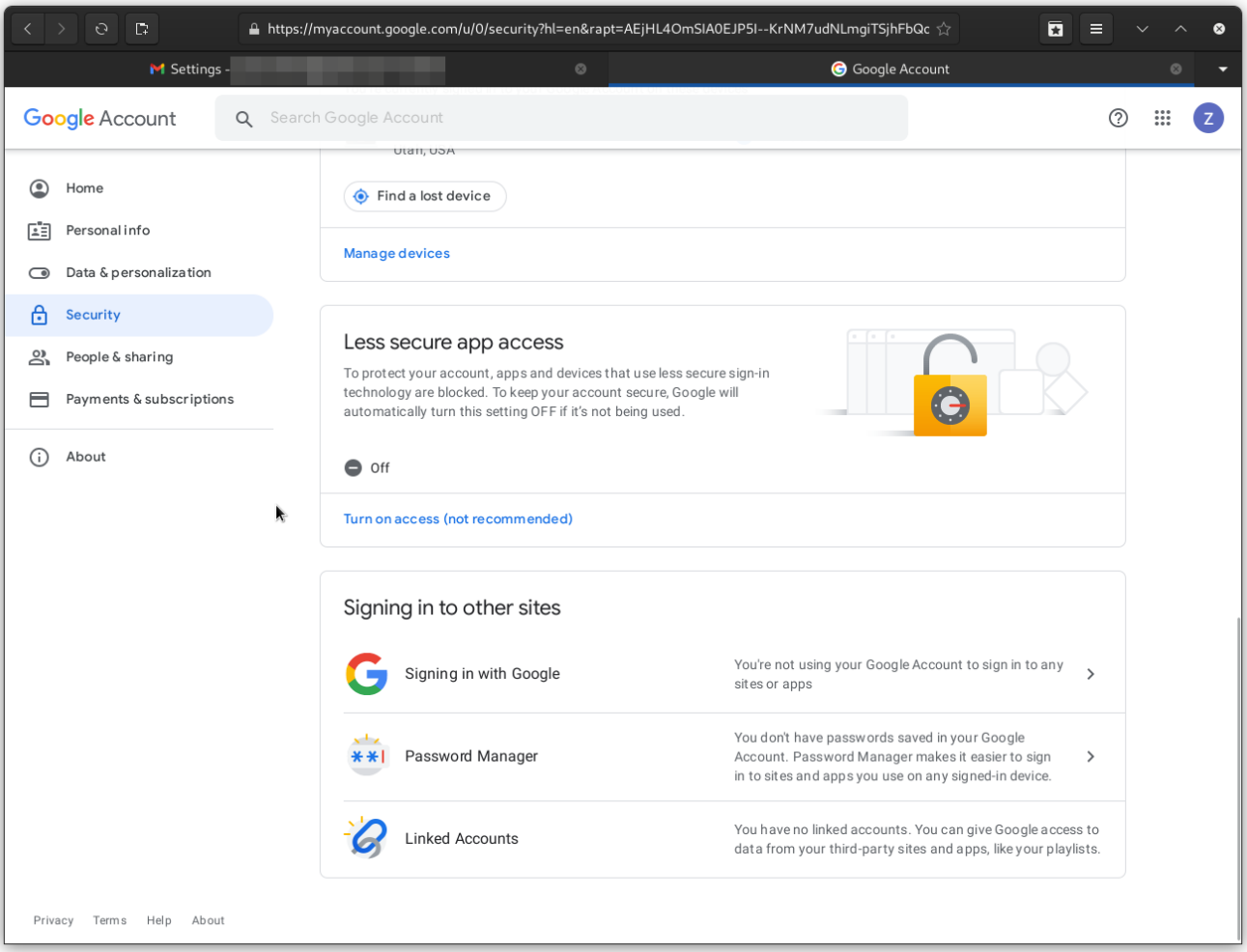


Download, print, or otherwise secure these codes; once you click away, you will have to generate other codes, and these codes will fail to work.



Turn Off Less Secure App Access

Your Google account can generate access tokens for less-secure applications. Unless you need to use one of these applications, it's a good idea to disable such access.



(OPTIONAL): Enroll in Google's "Advanced Protection Plan"

If you are a high-value target with a Google account, you can optionally enroll in the Advanced Protection Plan to further secure your account.

Who should enroll in this extended account security plan?

- C-Level executives
- System Administrators
- Public-Facing high-visibility employees
- Anyone who may have high-value information in their email account.

More details can be found here.

Securing a Microsoft `outlook.com` Email Address

As Microsoft Live (aka `outlook.com` or `live.com`) is a common Email provider, this module will walk you through some basic security settings you should enable and use on your account.

Most of these options and settings exist as part of the Microsoft `live.com` account.

Choosing a Passphrase

The first step of securing an online account is to have a secure password/passphrase.

A passphrase of multiple words is usually easier to remember and more secure.

Look at the "Authentication" module of this training course for details.

IMPORTANT

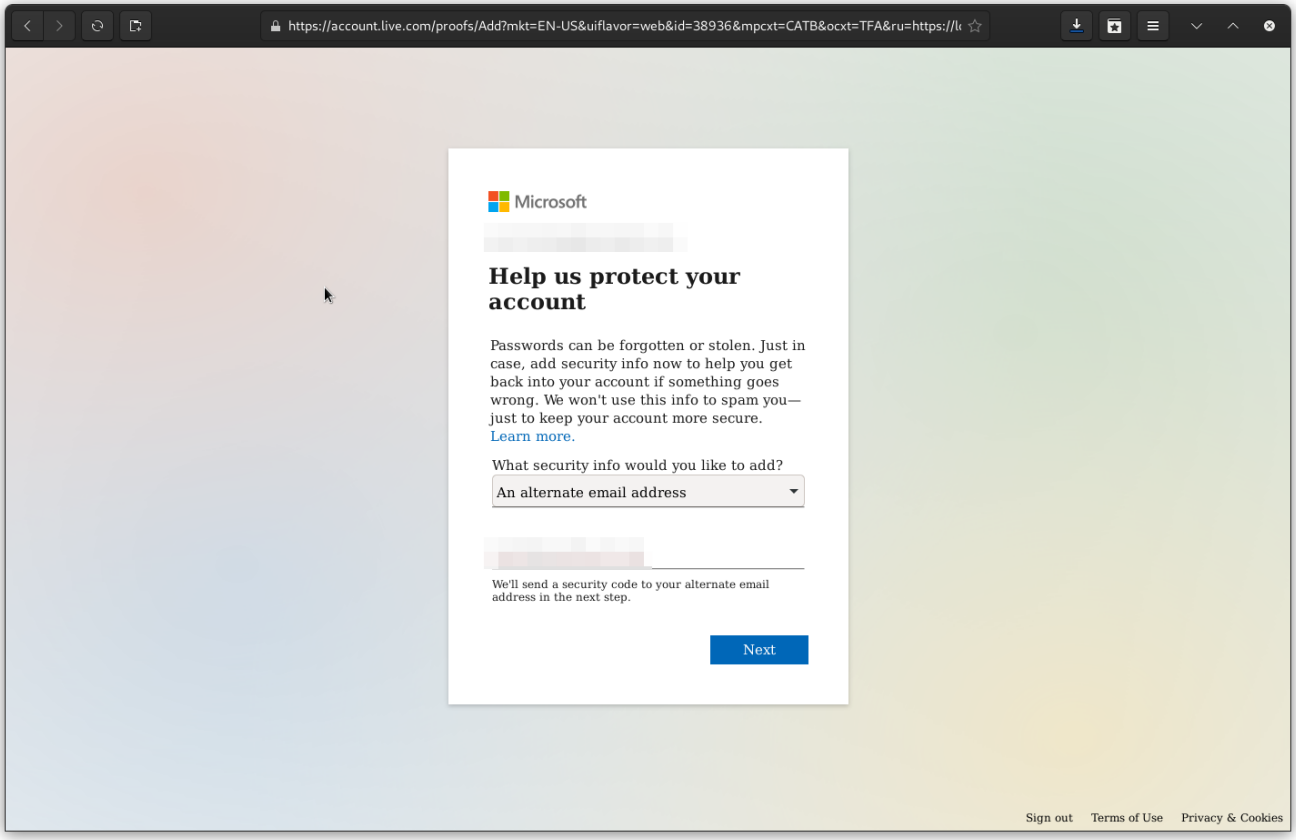
IMPORTANT: Use a Password Manager

Using a Password Manager is a more secure way to ensure you have the highest security passwords for an account.

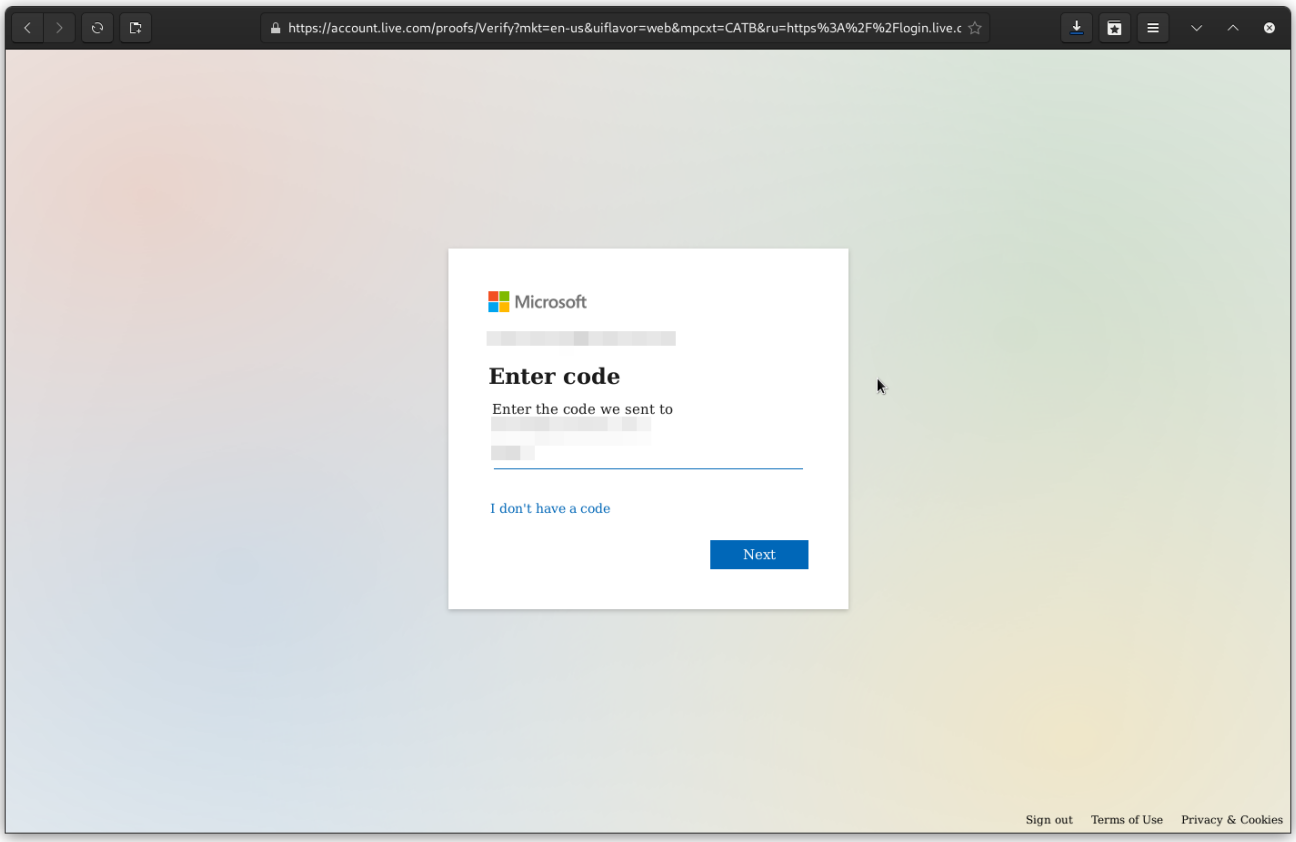
More information about password managers is in the "Password Manager" module of this training.

Setup a Secure Recovery Email Address

One of the security features of a Microsoft account is the recovery email address. Use this address if you find yourself locked out of your account and need to reset the password or verify that you are the account owner.



The recovery email address will get a code you need to enter:



You should choose an address where you have complete trust, as this is essentially a back-door into your account.

TIP

TIP

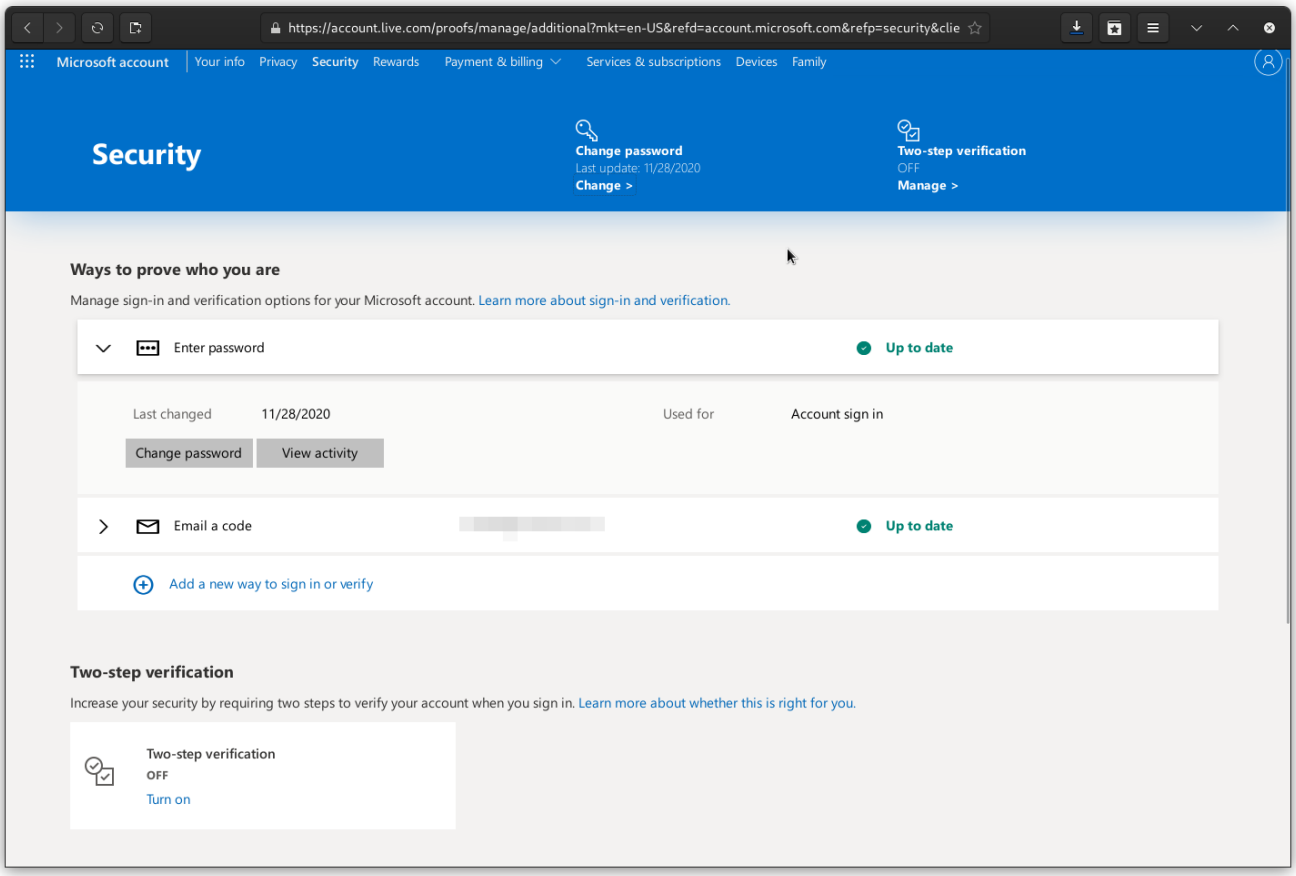
Use another personal account on a different provider for the highest level of security.

Turn on Multi-Factor Authentication (MFA)

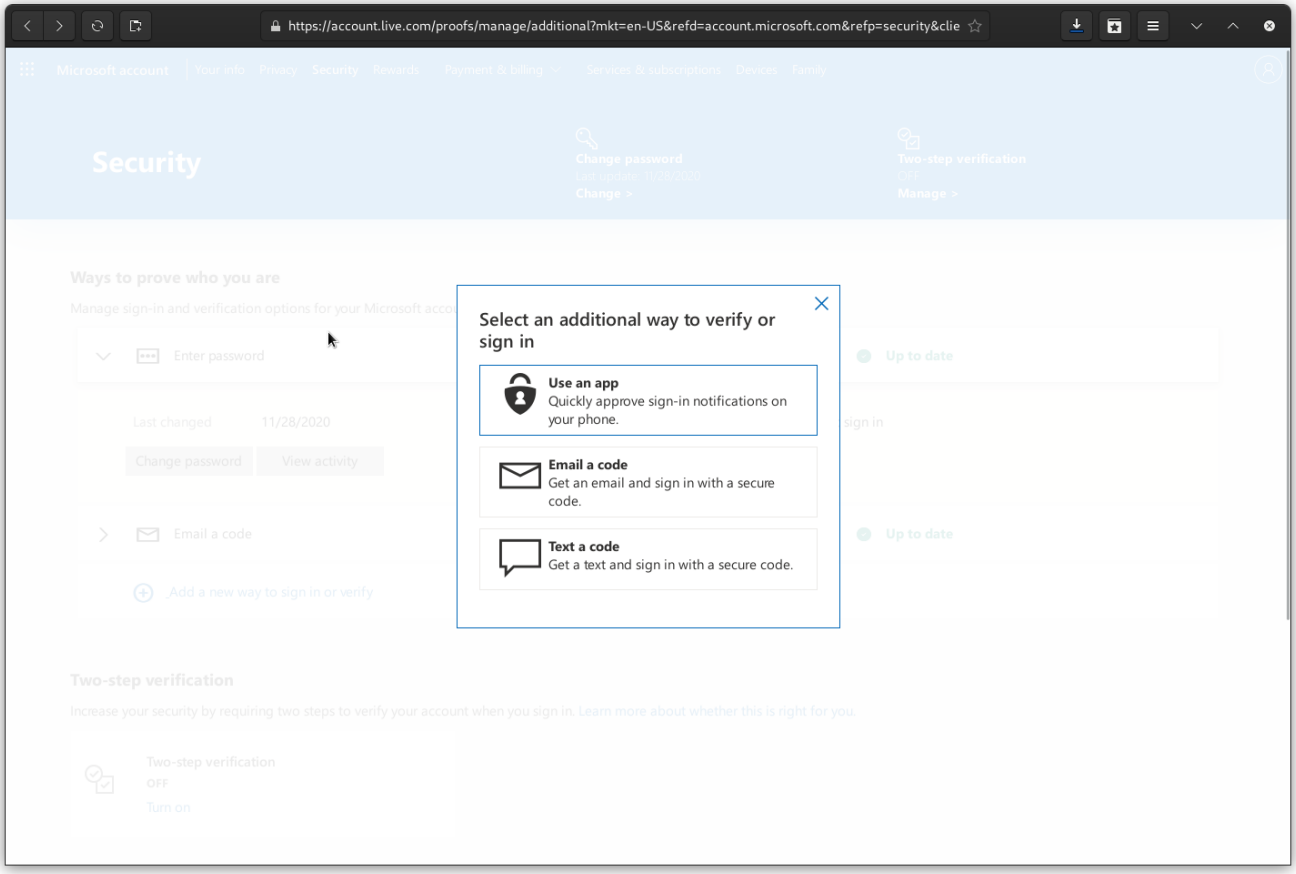
Compromised logins to your accounts are more likely if you don't have Multi-Factor Authentication(MFA) enabled. It would be best if you turned on MFA on your account.

Setup MFA

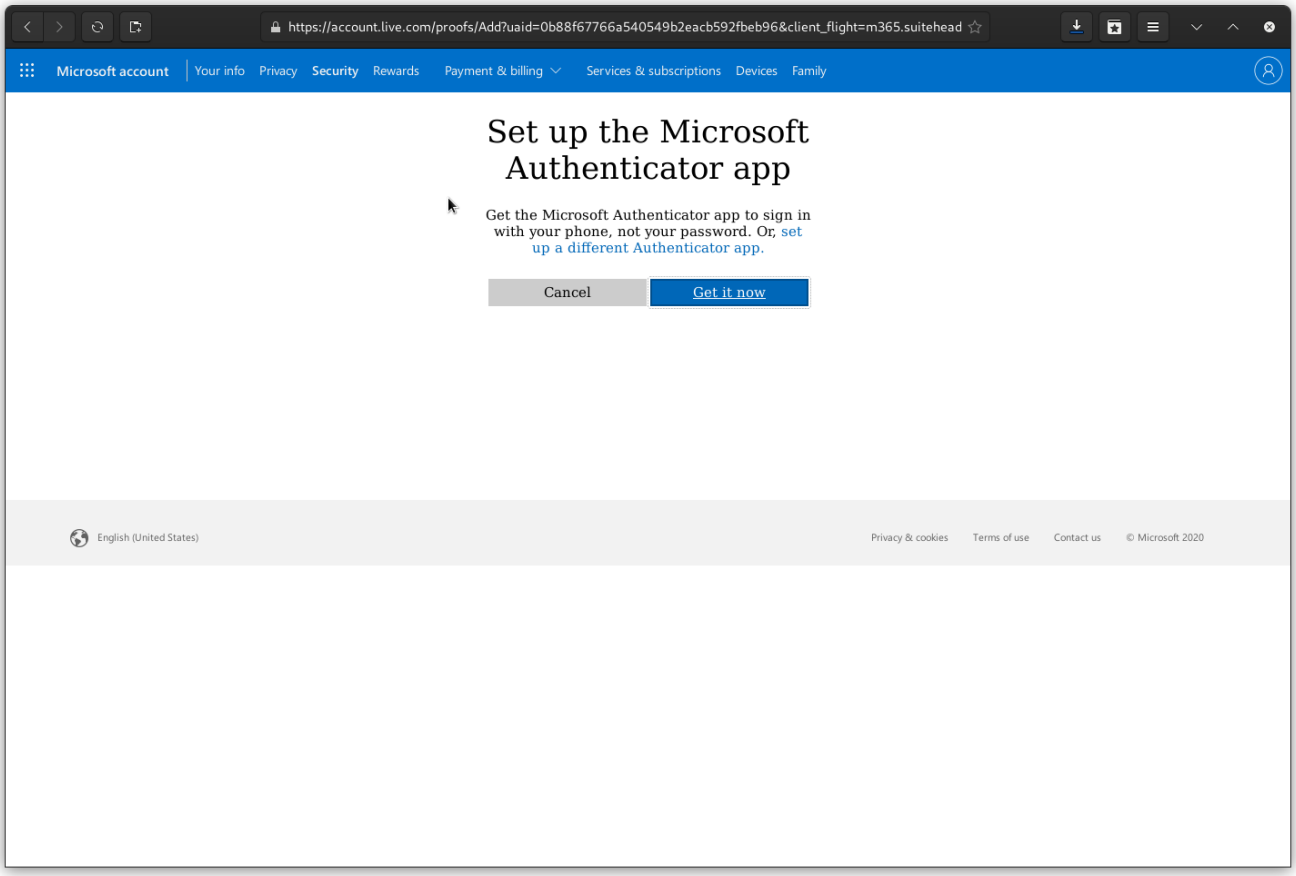
Start from the advanced security page in the account settings:



Choose "Add a new way to sign in or verify":

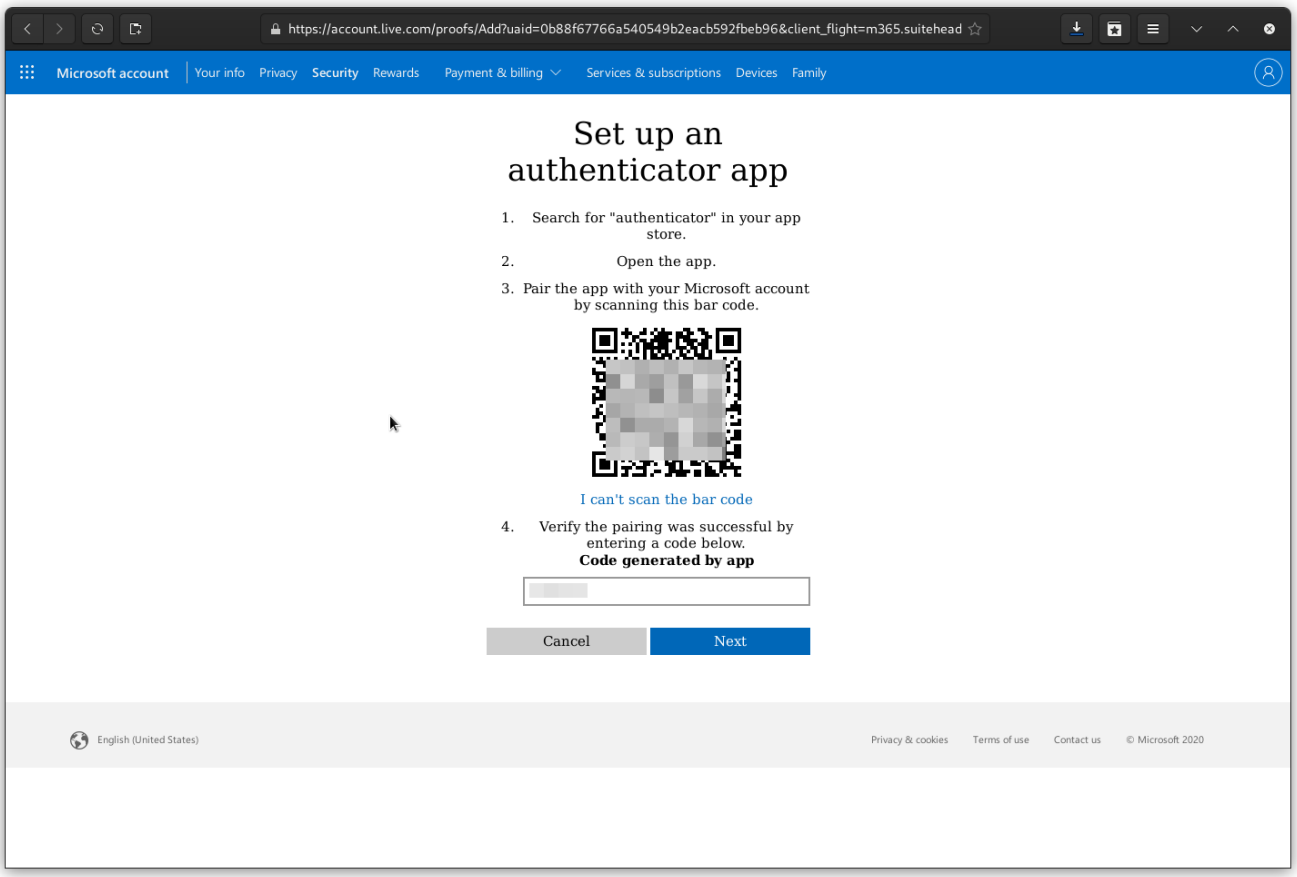


Select "Use an app."

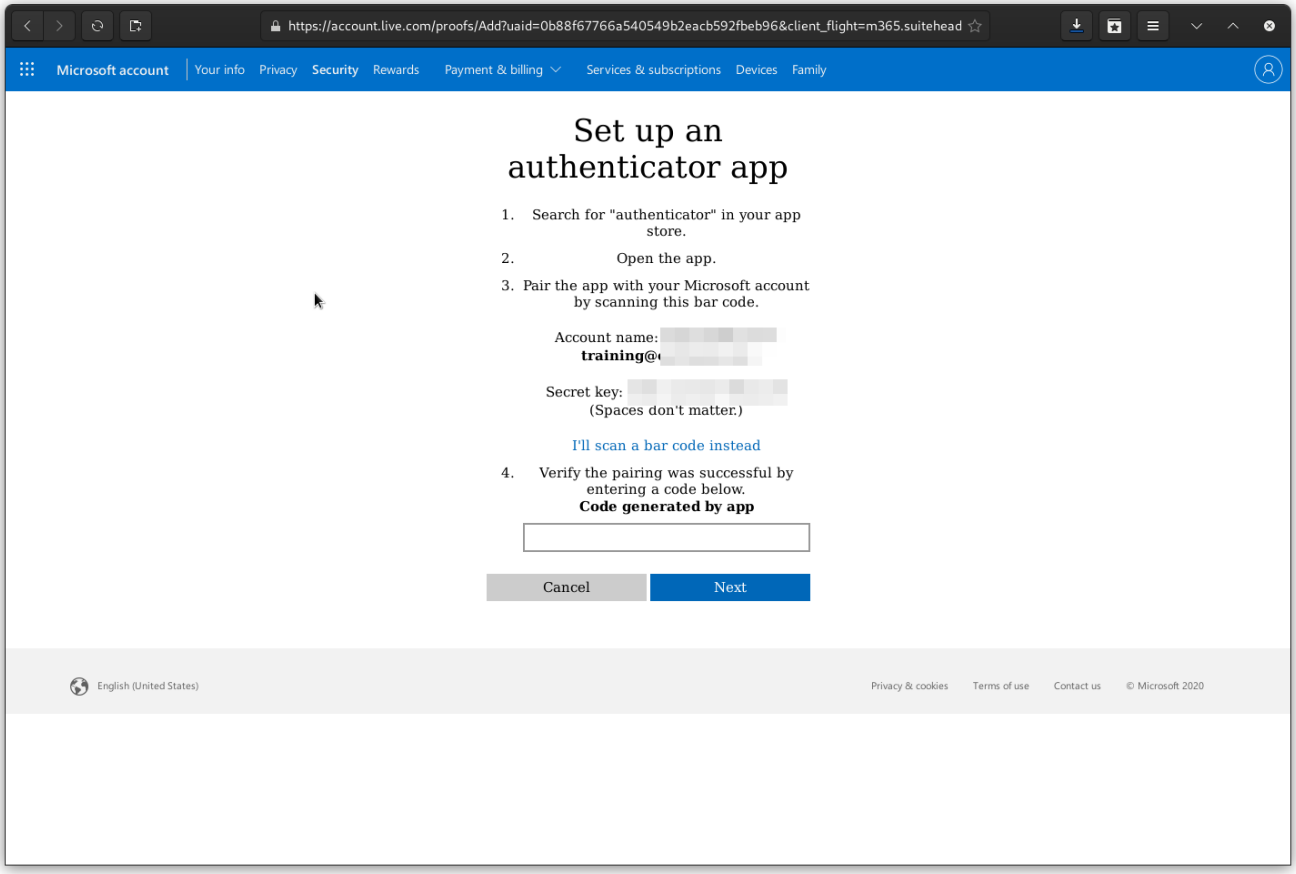


You can, at this point, download the Microsoft Authenticator app or click the link labeled "set up a

different Authenticator app" to use the TOTP-based app of your choice.

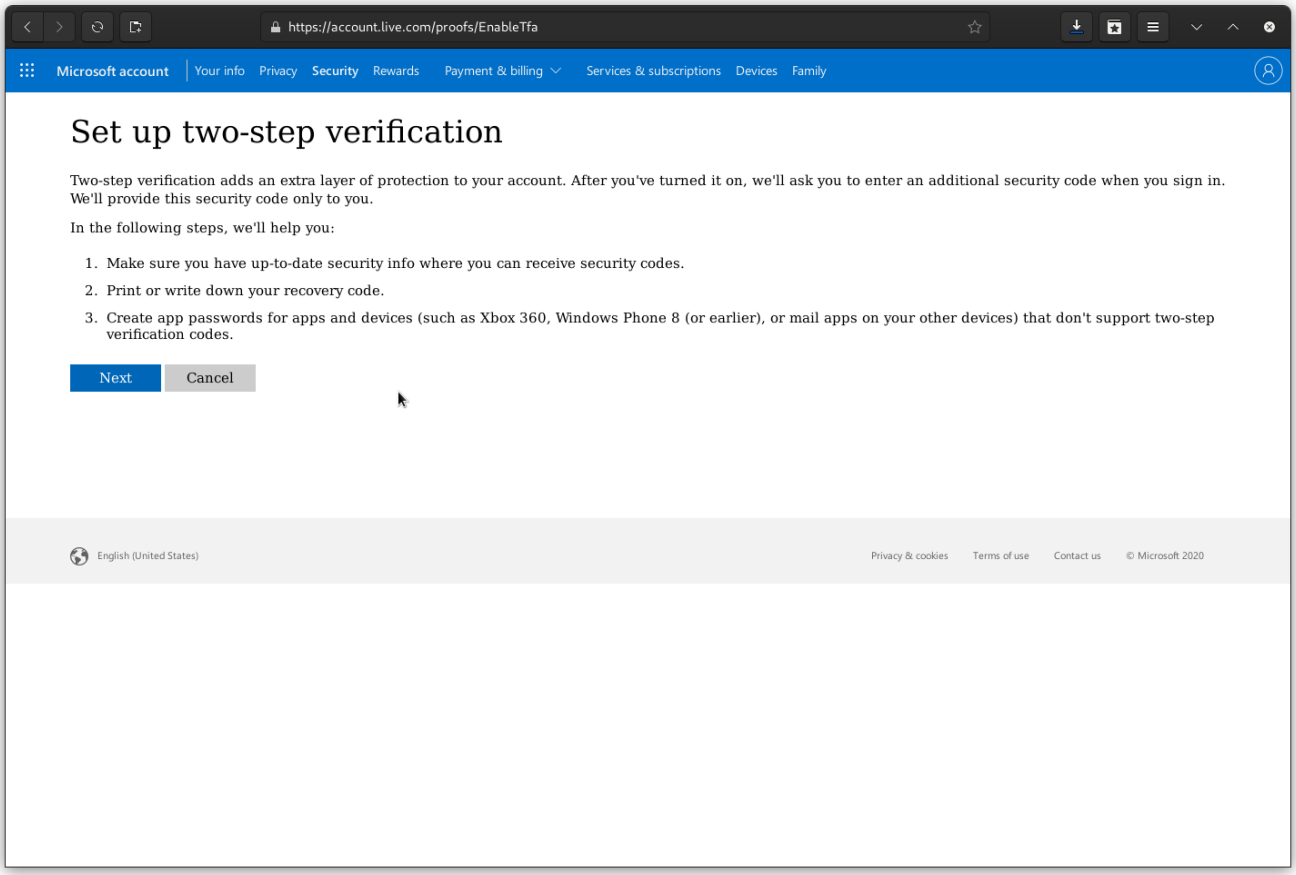


You can, at this point, scan the barcode or click the link "I can’t scan the bar code" to get a secret key to insert into your Authenticator app.



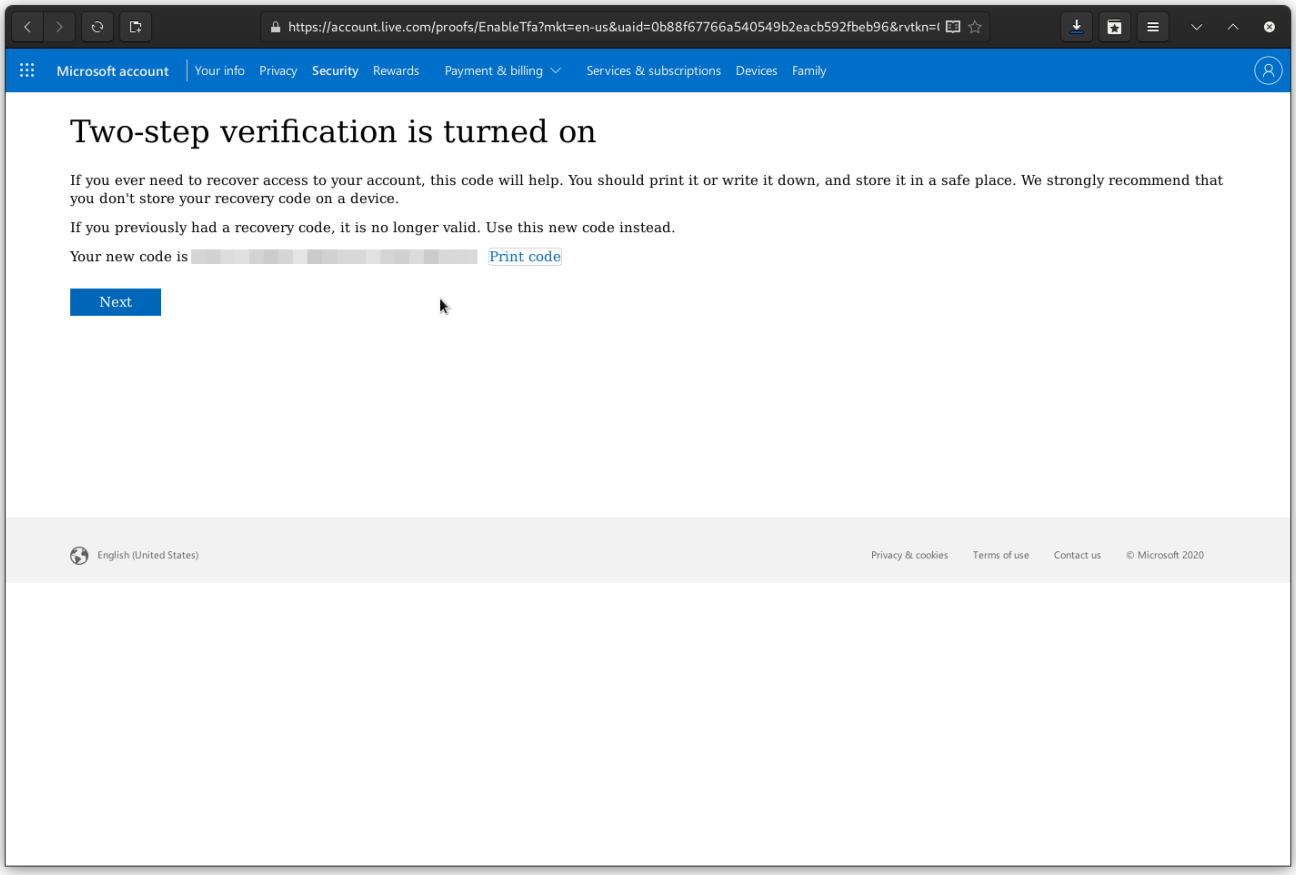
Either way, enter the code from the Authenticator app to validate it, and you're on to the next step.

You'll need to turn on the two-step (MFA) verification step manually.



Generate Recovery Code

When you turn on 2-step (MFA) on your account, you need a way to access the account if your second factor fails. With your Microsoft account, it creates a recovery code when you enable a second factor.

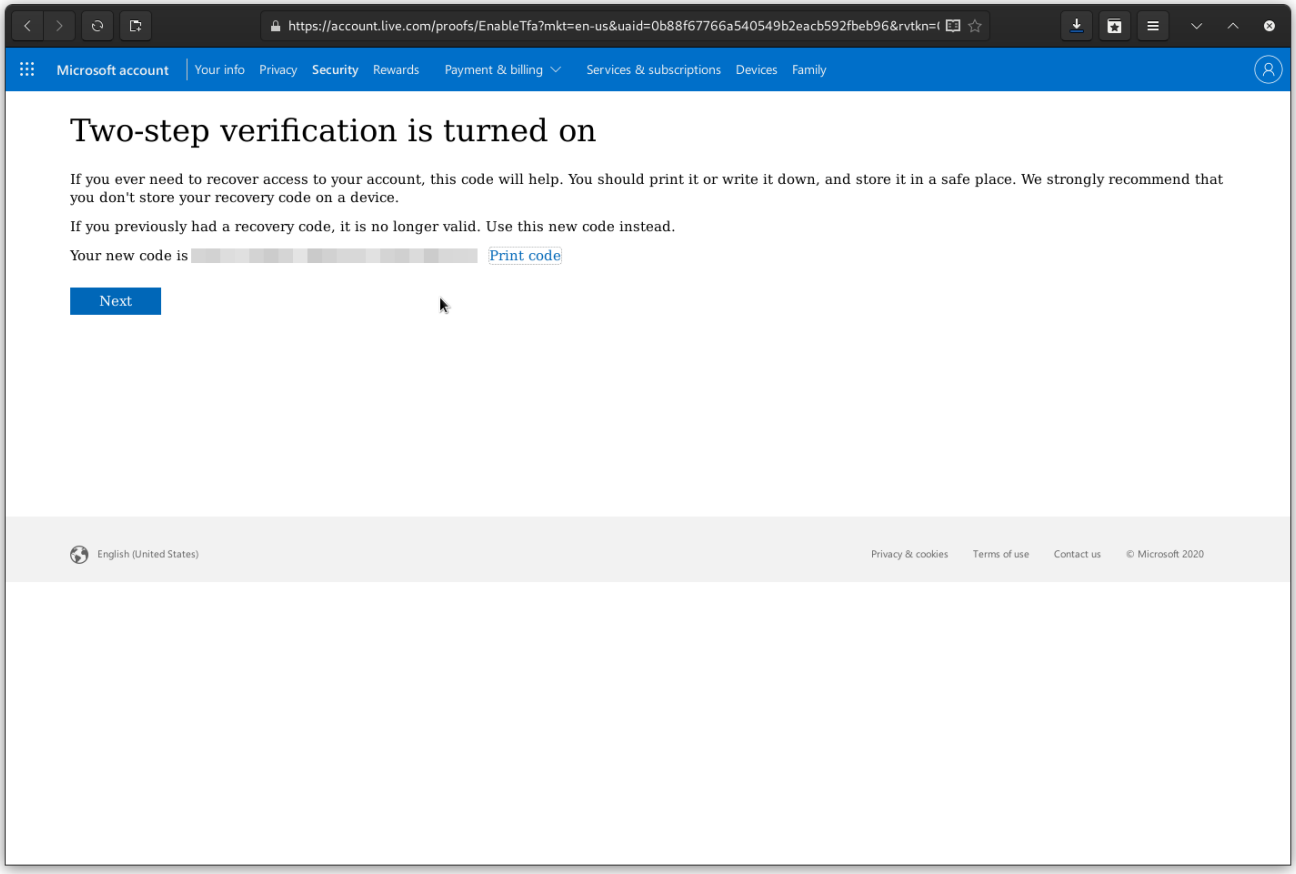


Download, print, or otherwise secure this code; once you click away, you will have to generate another, and this code will fail to work.

Microsoft Account additional access methods

Some apps or phones don’t do Microsoft account MFA properly and need an app password.

If your app/phone supports MFA properly, do not enable this.

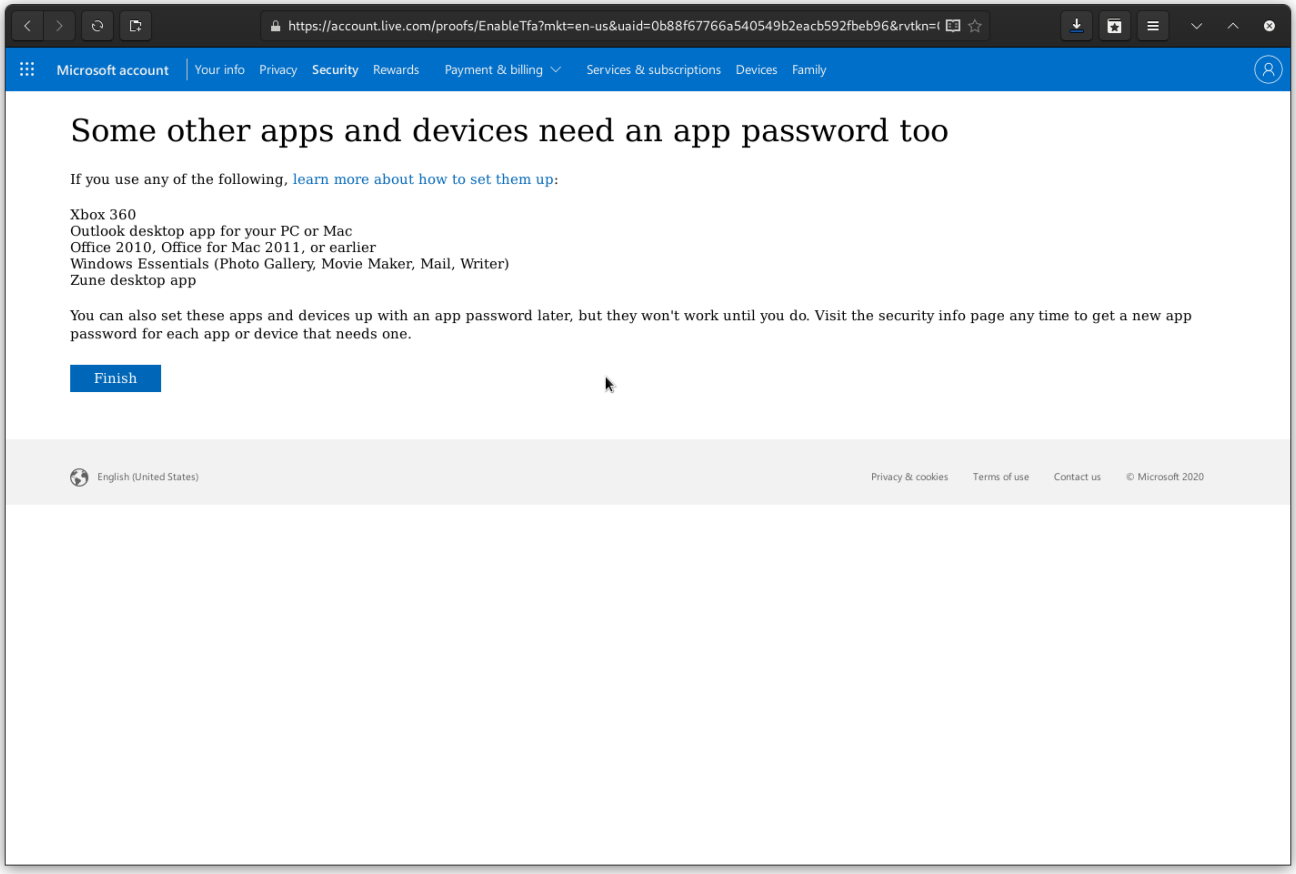


WARNING

Warning: App Passwords

Enabling app passwords reduces your account's security.

Some applications or systems **REQUIRE** that you create an app password for use with a `live.com` account.


https://account.live.com/proofs/EnableTfa?mkt=en-us&uaid=0b88f67766a540549b2eacb592fbeb96&rvtkn=
Microsoft account
Your info
Privacy
Security
Rewards
Payment & billing
Services & subscriptions
Devices
Family
Some other apps and devices need an app password too
If you use any of the following, learn more about how to set them up:
Xbox 360
Outlook desktop app for your PC or Mac
Office 2010, Office for Mac 2011, or earlier
Windows Essentials (Photo Gallery, Movie Maker, Mail, Writer)
Zune desktop app
You can also set these apps and devices up with an app password later, but they won't work until you do. Visit the security info page any time to get a new app password for each app or device that needs one.
Finish
English (United States)
Privacy & cookies
Terms of use
Contact us
© Microsoft 2020

Securing Your Mobile Computing Experience

Mobile computing has become a part of everyday life in the 21st century. Nearly all of us carry around more computing capacity than NASA used to get a man to the Moon in the 1960s. We use these devices without giving much conscious thought to the risks associated with them and what measures we can take to protect ourselves.

So the two most important questions we need to answer are:

- What could go wrong?
- What can we do to prevent it from happening, or at least minimize the impact?

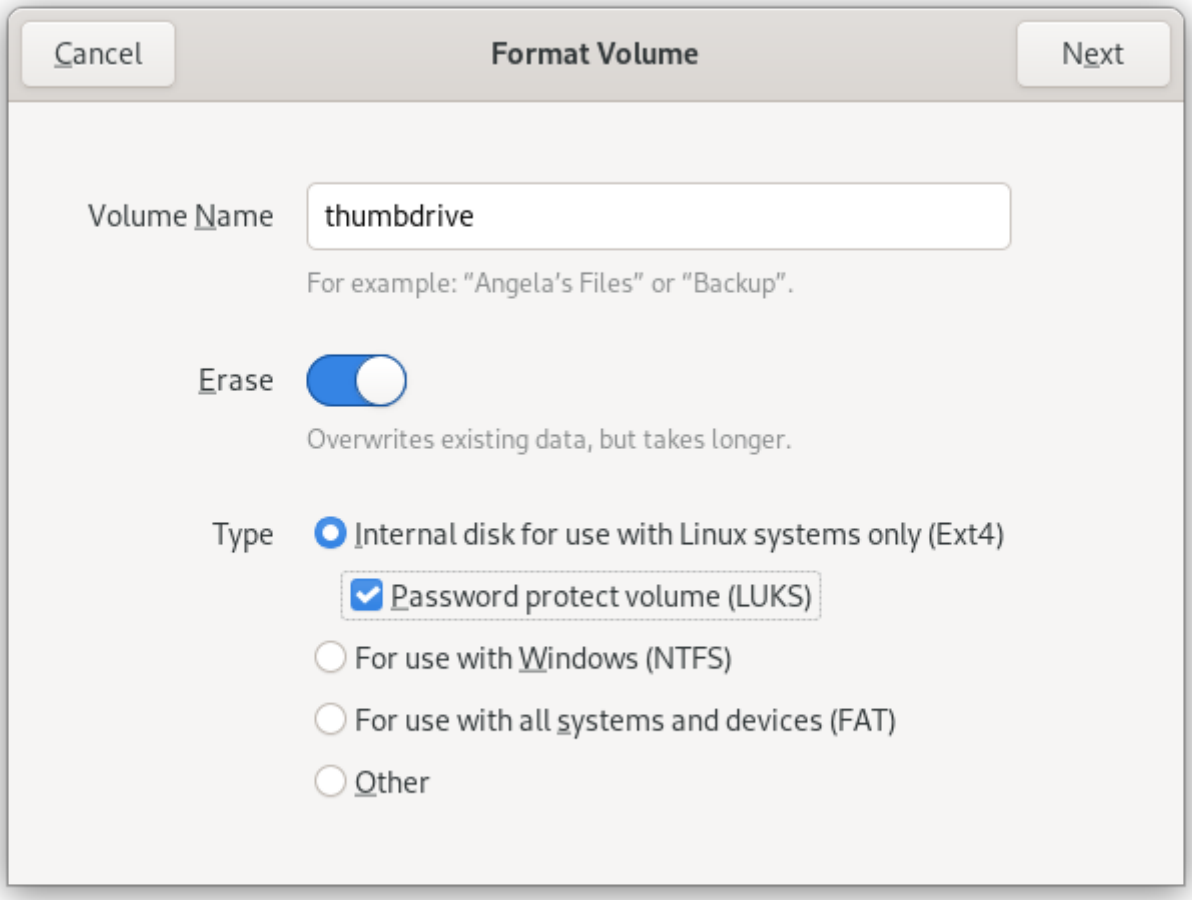
Losing Your Device

The first risk we'll discuss is the most obvious scenario; a lost (or stolen) device (almost all of us have lost a mobile device).

While the cost associated with replacing (and setting up) a replacement device is significant, it may be negligible compared with the damage associated with losing control of sensitive information (both work and personal).

What can you do to minimize the risks?

- Check for your devices frequently. At least before departing an area and upon arrival at a new area. It is better to recognize a device has been lost promptly when you are best positioned to remedy the problem.
- Encrypt your devices. If you lose a device, then encrypting it gives you the greatest assurance that those who come into possession of it won't gain access to your sensitive information. Devices to be encrypted include external storage devices (thumb drives and hard drives).
- Ensure that the device requires unlocking before accessing it; a trade-off between security and convenience. Use the most secure means to control access to your device that is practicable to you. If you know the information is particularly sensitive, then a more secure means of authentication is recommended. If possible, use multi-factor authentication.
- If you use your device to support multi-factor authentication, make sure you have alternative means of authenticating if your device is lost.
- Install or utilize device management tools to enable you to wipe the lost device remotely. Not always an option, but it can help you sleep at night if it is.

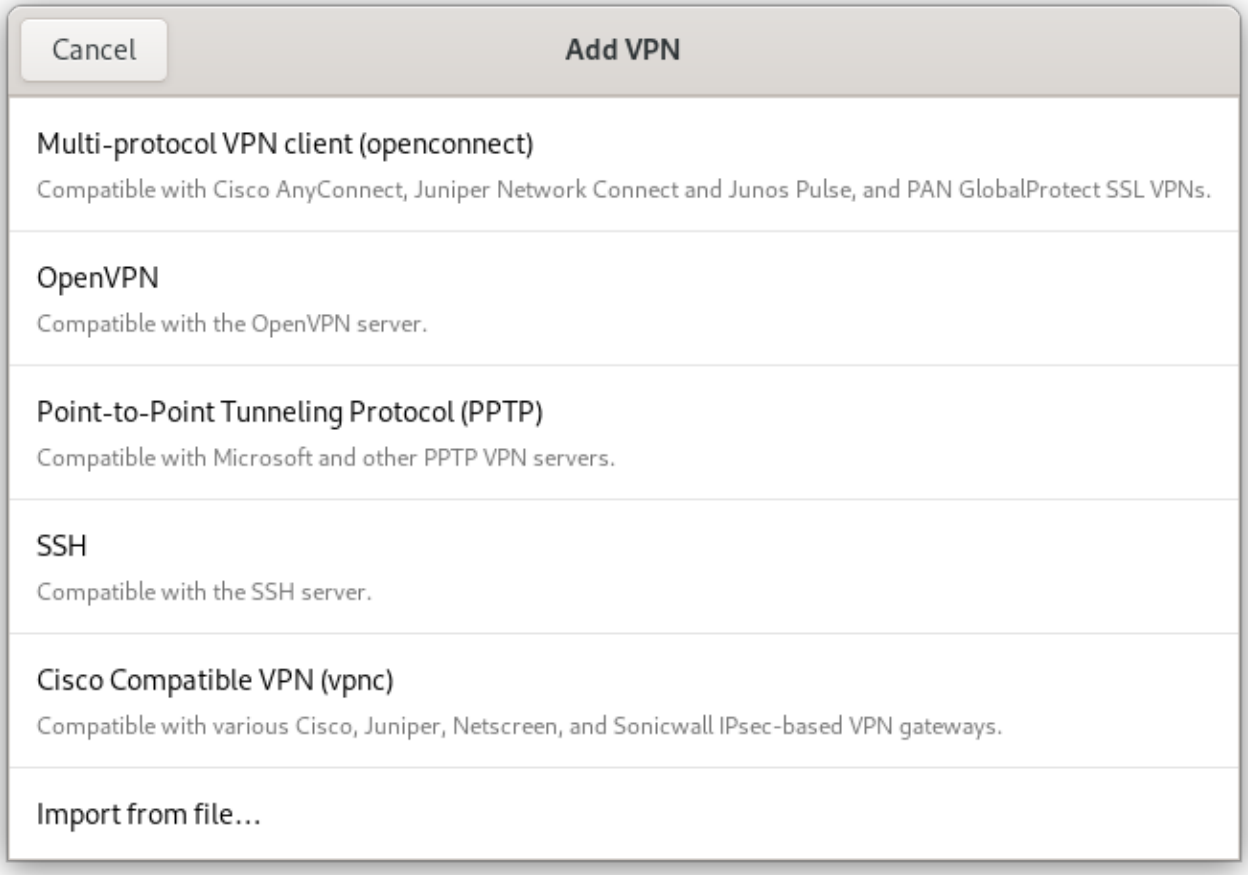


Uncontrolled/Insecure Operating Environments

You probably don't think too much about the controls in place in your home or office (for example, not just anyone has access to your home). While you are away from these environments, you are much more exposed. While not recommended, leaving your laptop unlocked and walking away from it in your home or office poses significantly less risk than doing the same thing at a corner coffee shop.

What can you do to minimize the risks?

- If your device processes or stores sensitive information, you should avoid working in insecure/uncontrolled places. If you need to do something in an insecure environment, you should seek out an isolated area, with your back to a wall, and where you can see other people approaching.
- We recommend securing your network traffic with a VPN connection. You probably have limited information about the controls of hazards present in an uncontrolled environment; therefore, you should assume that hostile actors are present and sniffing the network traffic.
- Avoid accessing any particularly sensitive information or services while you are in an uncontrolled environment. Wait until you are back inside a more controlled environment (if at all possible).



Traveling Internationally

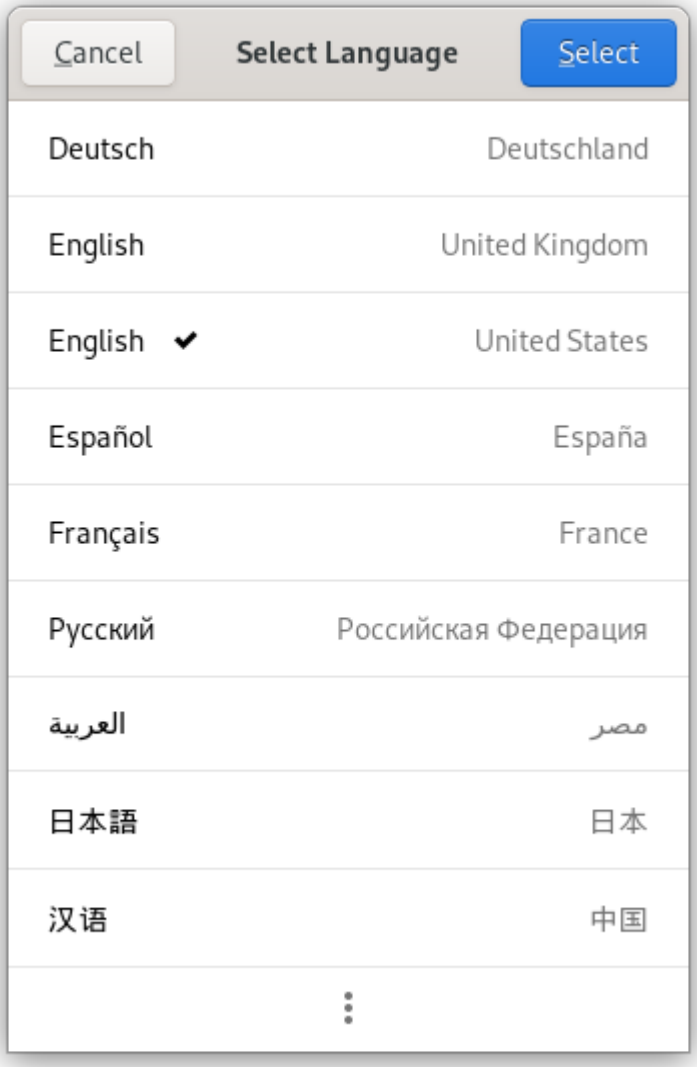
Taking and using your mobile devices when you travel internationally exposes you to particular hazards. In many countries, privacy protections (if they exist) are most often weakest at airports. To gain transit through or gain entry to a country, you probably need to submit to searches of your person and devices. While most of these searches are perfunctory, other searches can be rather intrusive. Additionally, some countries have significantly higher criminal activity than your originating country.

What can you do to minimize the risks?

- Research the countries you are traveling to (and through) to understand their privacy protections, security/inspection measures, and criminal activity concerns. The last thing you want to do is get surprised along the way.
- Consider minimizing the devices (or the sensitive data) you bring with you. If you don't need it for what you intend to do, it is probably best to avoid bringing it with you. If you need to use a phone to communicate, but you don't want to risk much of your personal information, then using an alternate phone or wiping your phone may be something you'll want to do.
- Use thin clients (if your organization allows/supports them). A thin client doesn't allow/enable storing information on them; therefore, the risk associated with losing or allowing someone to inspect the device is less than with conventional devices.
- Again, using a VPN connection to secure your network traffic. It is safe to assume that all traffic is being sniffed by countries and criminal operations while traveling abroad. Encrypting all

your communications is an essential security measure.

- Whenever possible, do not leave your devices unattended. If an adversary has physical access to your devices, they could tamper with them to compromise their security. Some attacks are at the hardware-level and are invisible to your system's security measures.
- Seek assistance from your organization's security personnel before traveling. They might be able to identify any particular threats and help you mitigate them.
- Update your devices before traveling. Two reasons for this. First, it makes sure that your devices are protected against any vulnerabilities that its vendors have fixed before your departure. Second, it will minimize your need to update while you are using potentially hostile networks. Some known attacks leverage software updates to compromise devices. While this can be attempted anywhere, updating while traveling makes you particularly vulnerable.



Summary

While mobile devices have become ubiquitous, they also open us up to significant risks. Taking the time to prepare and adjust your computing practices can mitigate (if not eliminate) most of these risks. Encrypting your mobile devices, exercising situational awareness, using a VPN to protect your network traffic, keeping your devices up-to-date are some of the things you can do to protect

yourself and your sensitive data.

Key Principles of Social Engineering

Robert Cialdini wrote a book on the 'key principles of "Influence"[influence: R. Cialdini].

These principles include:

- Reciprocity
- Commitment
- Social Proof
- Obeying Authority
- Likability
- Scarcity
- Unity

The psychology of social engineering can be wrapped in this framework.

Key Principle — Reciprocity

Reciprocity — aka "Returning the Favor".

Reciprocity is used in a social engineering attack by offering a small gift or concession to a target and asking the target to do something to reciprocate (such as change a password or open a locked door).

Another way to use reciprocity is to ask a considerable favor which the target declines to do. At this point, the attacker asks a smaller favor (their real goal) and the target can feel compelled to reciprocate on the concession of backing off the original favor.

Key Principle — Commitment

Commitment — aka "I want to sign up later".

When people commit to a future action or goal, they are more likely to follow through with that action.

Creators of web popups use this tactic "I'll sign up later" instead of "Cancel" or "No Thanks".

Key Principle — Social Proof

Social Proof — aka "Everyone is doing it".

People will conform to what they see other people doing.

Are all of the other employees shirking security training?

What kinds of behavior around security practices are challenging because of your corporate

culture?

Key Principle — Obeying Authority

Obeying Authority — aka "This authoritative person told me to".

Obedience to authority figures is ingrained in many cultures.

Often security is compromised by submitting to false authority figures.

IMPORTANT	*Verify Requests from Authority Figures* One should always verify any request purported to have come from a VIP.

Key Principle — Likability

Likability — aka "I'm more likely to help you if I like you."

Commonly security standards are overridden for attackers when asked nicely; this is doubly true with the attacker is "nice" or likable.

Key Principle — Scarcity driven

Scarcity — aka "Limited Time Offer"

A simple way to get people to lower their guard is to offer something with scarcity. Implying something is scarce leads to people taking action without fully thinking about the consequences.

Attackers can use this to make you click a link or install software which you shouldn't.

Key Principle — Unity

Unity — aka "The more alike we are, the more trusting we are".

Attackers will often prey upon our similarities: "Hey, we both have crazy bosses, I need your help, or he's gonna chew me out!"

References

Cialdini, Robert (2009). Influence: Science and Practice. Boston, MA: Pearson Education. ISBN 0-205-60999-6.

Social Engineering

Social Engineering is tricking people into revealing information they usually wouldn't.

Social Engineering is one of the more common attacks your company faces. A social engineering component often accompanies most other types of attacks and vulnerabilities.

Social Engineering Defined

> Any act that influences a person to take any action that may or may not be in their best interest .[1]
>
> — www.social-engineer.org -- Social Engineering Defined

Social Engineering — Methods

Social engineering comes through a few different vectors:

Vishing

aka "Voice Phishing" Vishing is using Social engineering over the telephone system. This method is used as an attack by purporting to be a bank or other organization that the target does business with to directly steal information such as usernames, passwords, and account info. This method is also used to reconnoiter for other information in a multi-stage attack.

Phishing

Using electronic communications such as email or websites to gather private or secure information. Phishing email scams send links to authentic-looking fraudulent sites, which then gather your personal information (usernames, passwords, accounts, Card PINs). Often phishing attacks use a request to "verify" information and use "loss aversion" principles to ensure compliance. An example of this method would be the request to provide or verify a credit card number to continue using an online service.

Smishing

Using SMS text messages in a social engineering attack.

Impersonation

Pretending to be another person to gain access; including using another person's credentials to gain access to a location or system.

Other Social Engineering Concepts

Tailgating

following someone with access into a secured location.

Pretexting

Gaining trust from the target by sharing information about the victim. An attacker uses information gained through other avenues: "I have your last statement balance; can you give me

your password?"

Baiting

Using malware-infected disks or thumb drives to gain access to systems.

Social Engineering "Red Flags."

- An organization calling, texting, or emailing you and asking for credentials.
- Someone in "distress" asking you to forgo security procedures. "If I don’t get my password reset, we’ll lose this account! You have to help me!"
  - This can be legitimate; take extra care to verify the identity of the requester.
- Urgency conveyed in a non-urgent medium
  - A common trick is to send an SMS message asking someone to do a task such as send money or buy gift cards. This attacker often claims to be in an important meeting hence the request coming from a text message.
- An offer seems "Too good to be true".
- Email attachments you are not expecting.
  - Even if they claim to be from people you know.
- A website where the security certificate does not match the domain.

[1] https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Updates

Over time, mistakes and vulnerabilities are found in every system. To stay secure, most mature vendors will provide a way to update their products.

Updates are Mostly for Security

With few exceptions, most updates are to fix vulnerabilities in products and software. Even with the most rigorous controls and processes, software developers will make mistakes. It is only a matter of time before someone will find them. Once the manufacturers become aware of these vulnerabilities, they will frequently produce an update that fixes them.

Update Promptly

After an update becomes available, attackers will learn about the vulnerabilities and develop 'exploits' (tools to attack) that target them. As time passes, it will become easier and less cumbersome to attack systems and services that have not been kept up to date.

Reasons for not Updating

Most of the reasons people don't update their devices/systems are:

- They don't know an update is available.
- They fear that an update may 'break' a device/system's functionality.
- A provider no longer supports the device/system.

We will discuss what to do in each of these situations.

Don't Know an Update is Available

Most software today will have the capacity to manually (or automatically) check for updates.

Recommend that - as a minimum - you check for updates once a month.

As much as possible, enable auto-updates on as many of your devices and systems.

Fear That an Update Will Break Functionality

Most devices/services have a way for you to backup the currently running version of their software.

Learn how to leverage the functionality to restore the system if something (like an update) renders it unusable. You can update with confidence because you know you can always fall back to something that works.

Updates No Longer Available/Unsupported

Vendors don't support their products indefinitely.

When you purchase/acquire a product, you should make a special note of its end-of-life date and plan to replace it before that date.

If you can't replace something before it's end-of-life, then you should take measures to reduce the risks associated with continuing to use it. For example: Take it off the network.

Critical Updates

Occasionally, vendors will announce a critical update. These are usually to resolve a vulnerability that is currently being attacked or is particularly easy/impactful.

Whenever you become aware of a critical update, you should immediately update it to minimize risk.