Text Scams, Email Phishing & Malware 2023

Presented Saturday, 5/27/23
Gail Weiss

Agenda

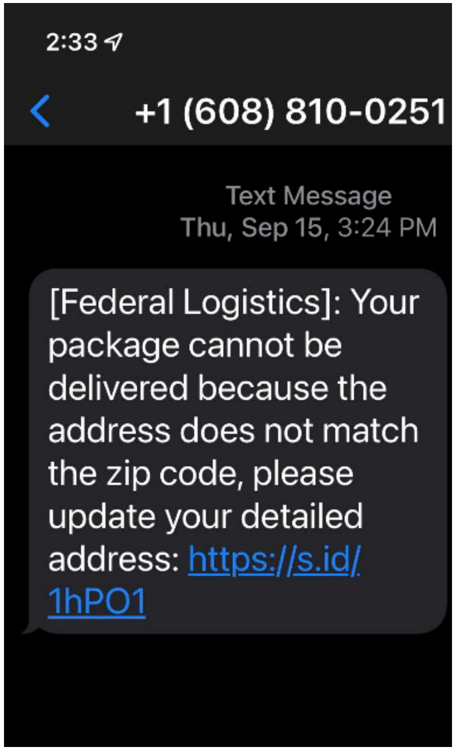
- Text Scams
- Email Phishing
- Google Email Security Settings
- iPhone & Android Security Settings
- Malware
- AntiVirus Software
- Google Chrome Security Settings
- Managing Your Passwords

Text Scams

On an Android or iPhone

Text Scams

- Samples of Text Scams

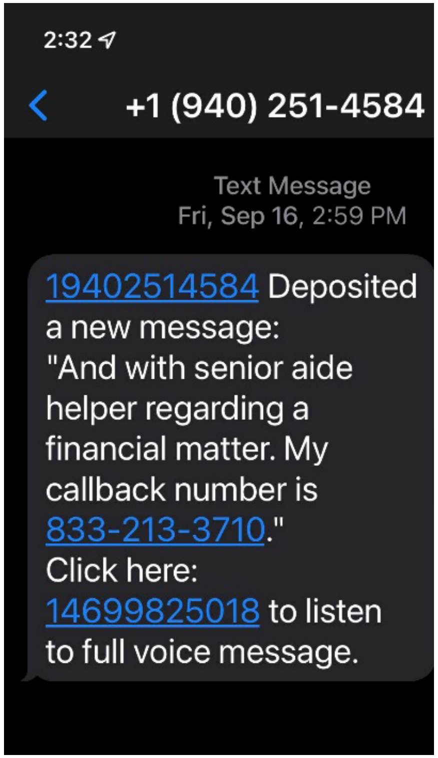


2:33

+1 (608) 810-0251

Text Message
Thu, Sep 15, 3:24 PM

[Federal Logistics]: Your package cannot be delivered because the address does not match the zip code, please update your detailed address: https://s.id/1hPO1

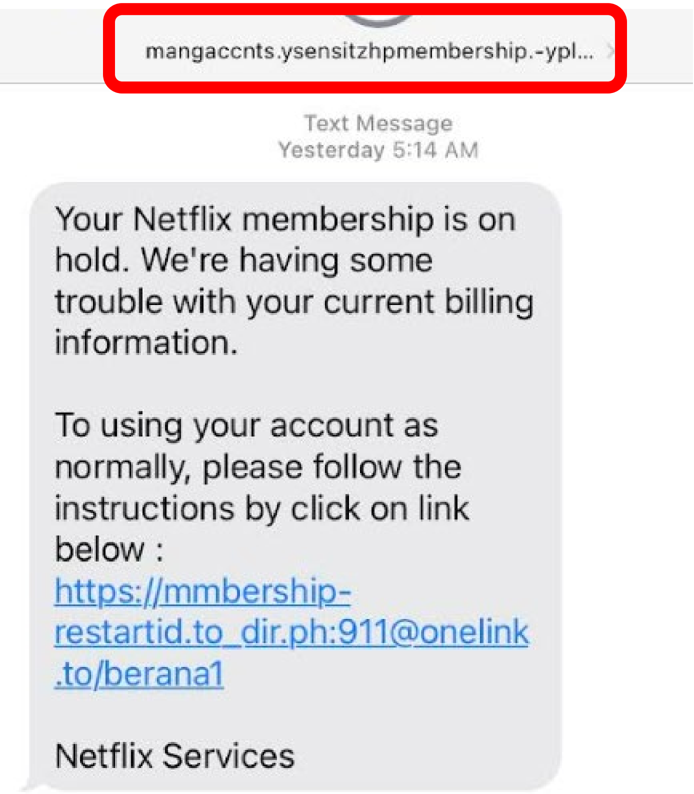


2:32

+1 (940) 251-4584

Text Message
Fri, Sep 16, 2:59 PM

19402514584 Deposited a new message: "And with senior aide helper regarding a financial matter. My callback number is 833-213-3710." Click here: 14699825018 to listen to full voice message.



mangaccnts.ysensitzhpmembership.-ypl...

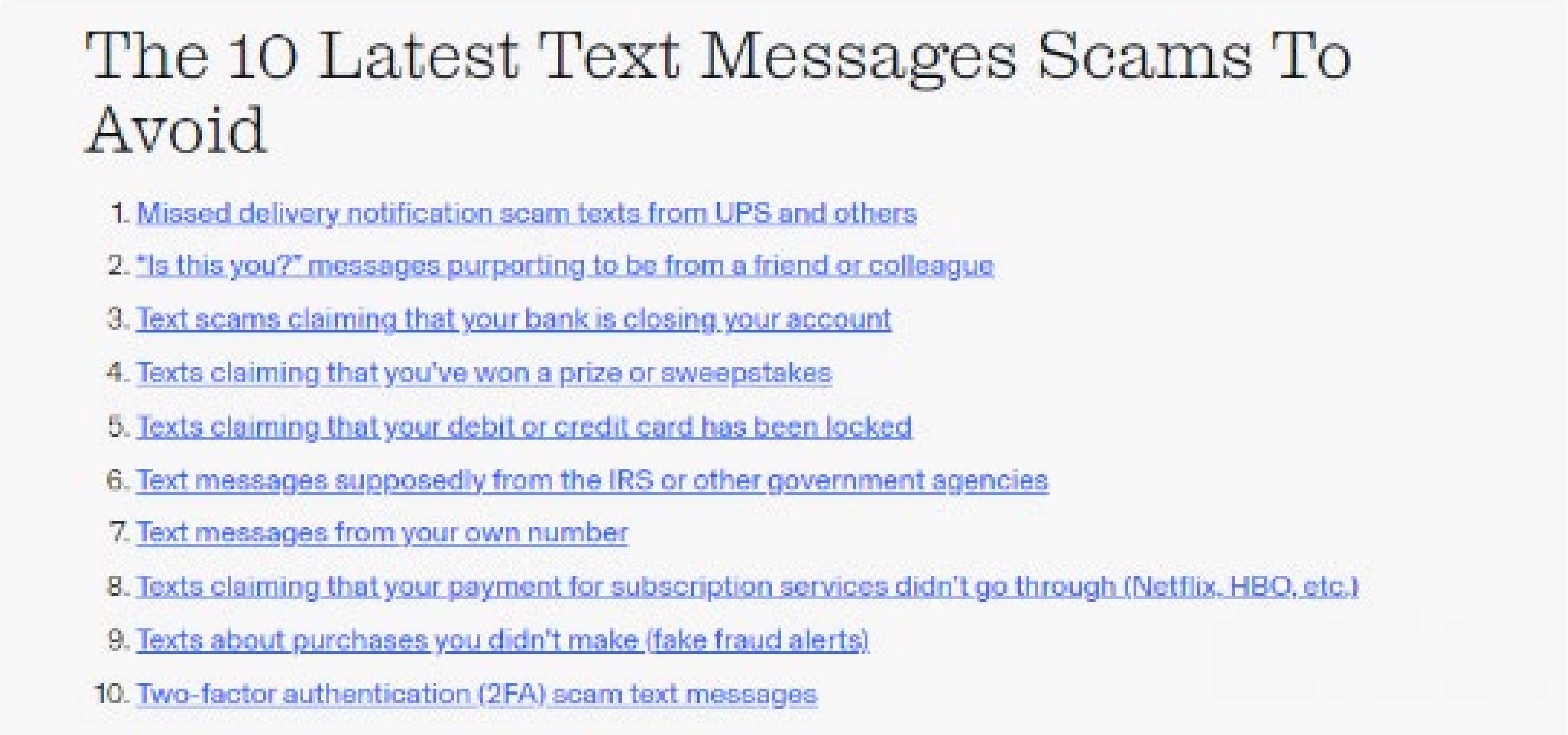
Text Message
Yesterday 5:14 AM

Your Netflix membership is on hold. We're having some trouble with your current billing information.

To using your account as normally, please follow the instructions by click on link below : https://mmbership-restartid.to_dir.ph:911@onelink.to/berana1

Netflix Services

How to Recognize & Report Spam Text Messages



The 10 Latest Text Messages Scams To Avoid

1. Missed delivery notification scam texts from UPS and others
2. "Is this you?" messages purporting to be from a friend or colleague
3. Text scams claiming that your bank is closing your account
4. Texts claiming that you've won a prize or sweepstakes
5. Texts claiming that your debit or credit card has been locked
6. Text messages supposedly from the IRS or other government agencies
7. Text messages from your own number
8. Texts claiming that your payment for subscription services didn't go through (Netflix, HBO, etc.)
9. Texts about purchases you didn't make (fake fraud alerts)
10. Two-factor authentication (2FA) scam text messages

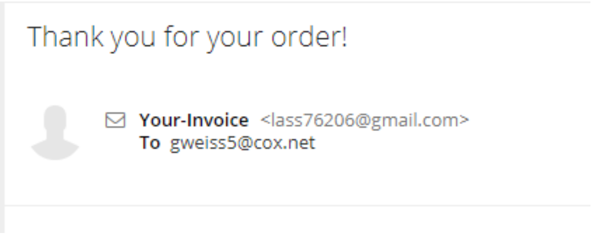
- Federal Trade Commission – Consumer Advice Article
- https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

Email Spam & Phishing

Regardless of email provider

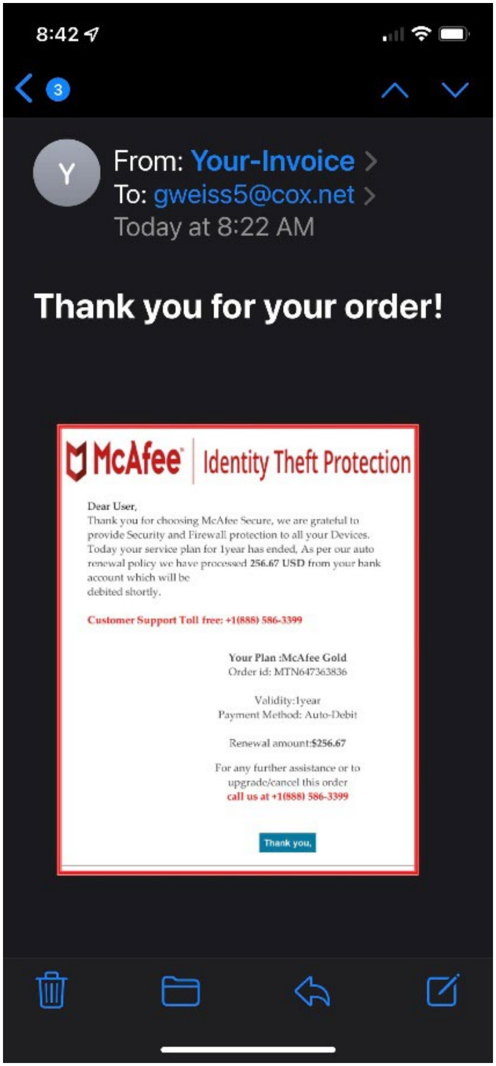
Email Spam

- Samples of Email Spam



Thank you for your order!

Your-Invoice <lass76206@gmail.com>
To gweiss5@cox.net



From: Your-Invoice
To: gweiss5@cox.net
Today at 8:22 AM

Thank you for your order!

McAfee | Identity Theft Protection

Dear User,
Thank you for choosing McAfee Secure, we are grateful to provide Security and Firewall protection to all your Devices. Today your service plan for 1year has ended, As per our auto renewal policy we have processed **256.67 USD** from your bank account which will be
debited shortly.

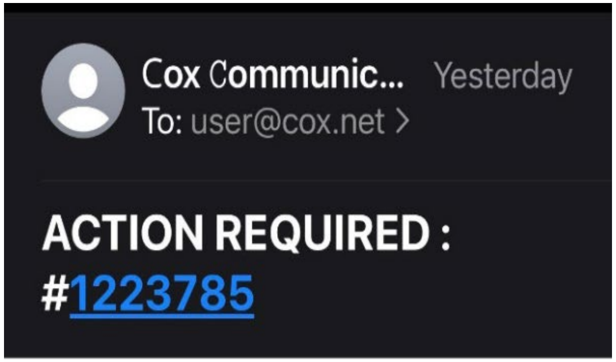
Customer Support Toll free: +1(888) 586-3399

Your Plan :McAfee Gold
Order id: MTN647363836

Validity:1year
Payment Method: Auto-Debit

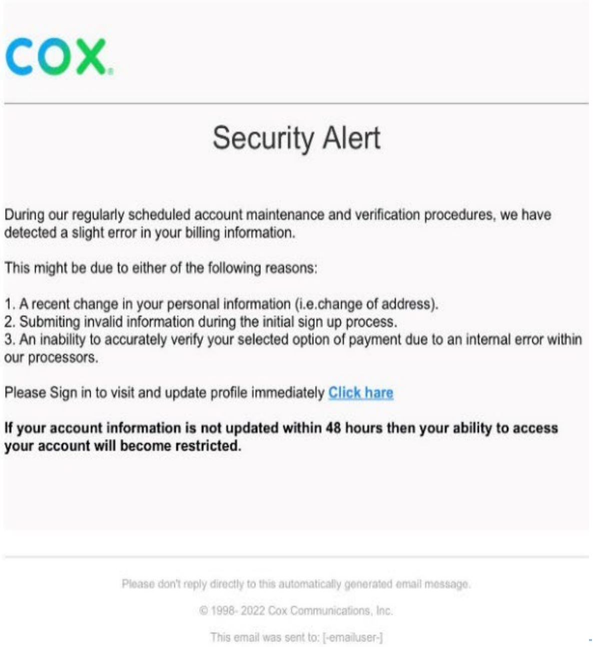
Renewal amount:**$256.67**

For any further assistance or to
upgrade/cancel this order
call us at +1(888) 586-3399



Cox Communic... Yesterday
To: user@cox.net

ACTION REQUIRED :
#1223785



COX

Security Alert

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e.change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please Sign in to visit and update profile immediately Click hare

If your account information is not updated within 48 hours then your ability to access your account will become restricted.

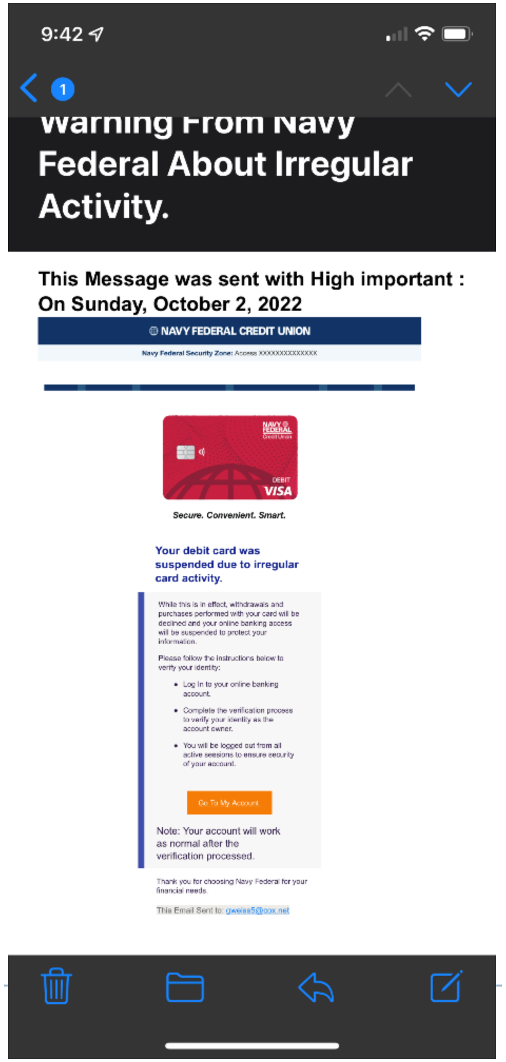
Please don't reply directly to this automatically generated email message.

© 1998- 2022 Cox Communications, Inc.

This email was sent to: [-emailuser-]

Email Spam – Phishing

- Samples of Phishing – Account Information


9:42

Warning From Navy Federal About Irregular Activity.

This Message was sent with High important :
On Sunday, October 2, 2022

NAVY FEDERAL CREDIT UNION

Navy Federal Security Zone: Access XXXXXXXXXXXXXX

Secure. Convenient. Smart.

Your debit card was suspended due to irregular card activity.

While this is in effect, withdrawals and purchases performed with your card will be declined and your online banking access will be suspended to protect your information.

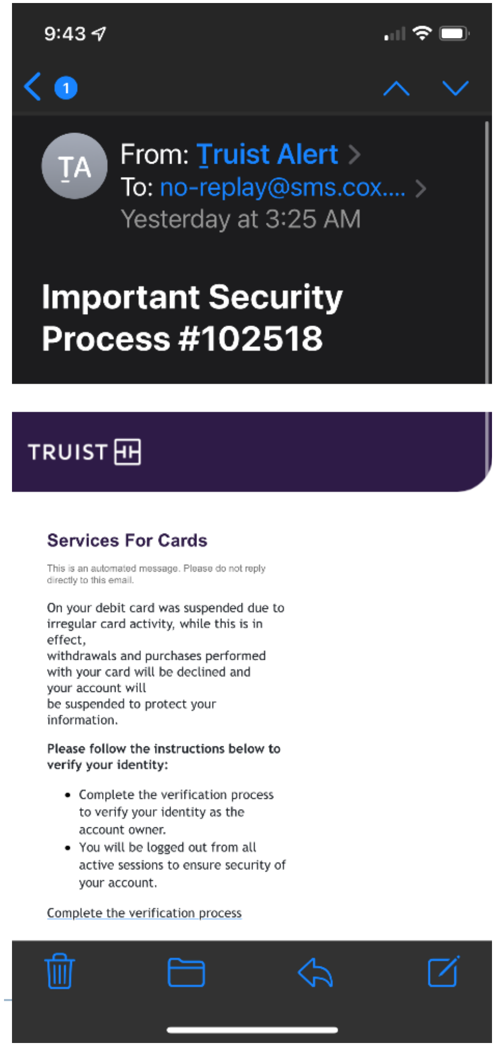
Please follow the instructions below to verify your identity:

- Log in to your online banking account.
- Complete the verification process to verify your identity as the account owner.
- You will be logged out from all active sessions to ensure security of your account.

Note: Your account will work as normal after the verification processed.

Thank you for choosing Navy Federal for your financial needs.

This Email Sent to: gweiss5@cox.net


9:43

From: Truist Alert
To: no-replay@sms.cox....
Yesterday at 3:25 AM

Important Security Process #102518

TRUIST

Services For Cards

This is an automated message. Please do not reply directly to this email.

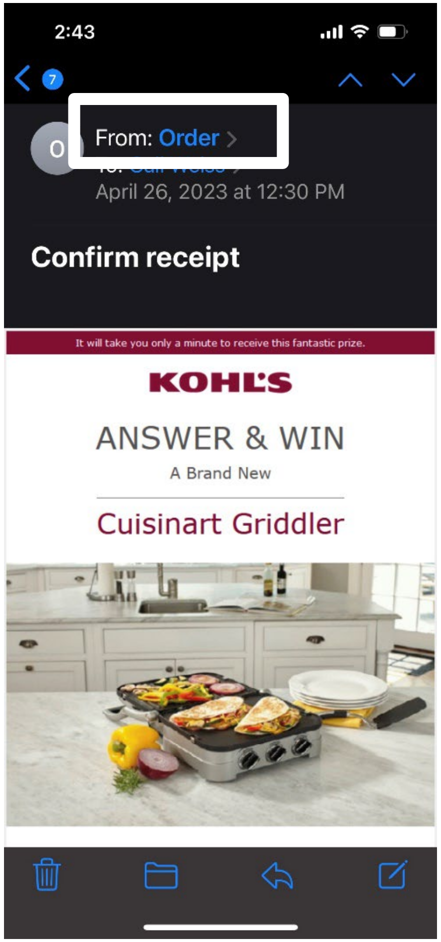
On your debit card was suspended due to irregular card activity, while this is in effect,
withdrawals and purchases performed with your card will be declined and your account will
be suspended to protect your information.

Please follow the instructions below to verify your identity:

- Complete the verification process to verify your identity as the account owner.
- You will be logged out from all active sessions to ensure security of your account.

Complete the verification process

Checking the Sender's Address



From: Order

April 26, 2023 at 12:30 PM

Confirm receipt

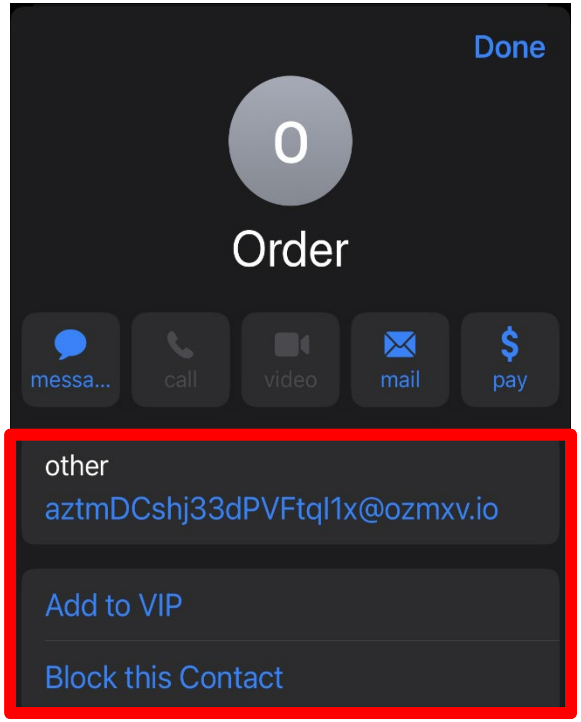
It will take you only a minute to receive this fantastic prize.

KOHL'S

ANSWER & WIN

A Brand New

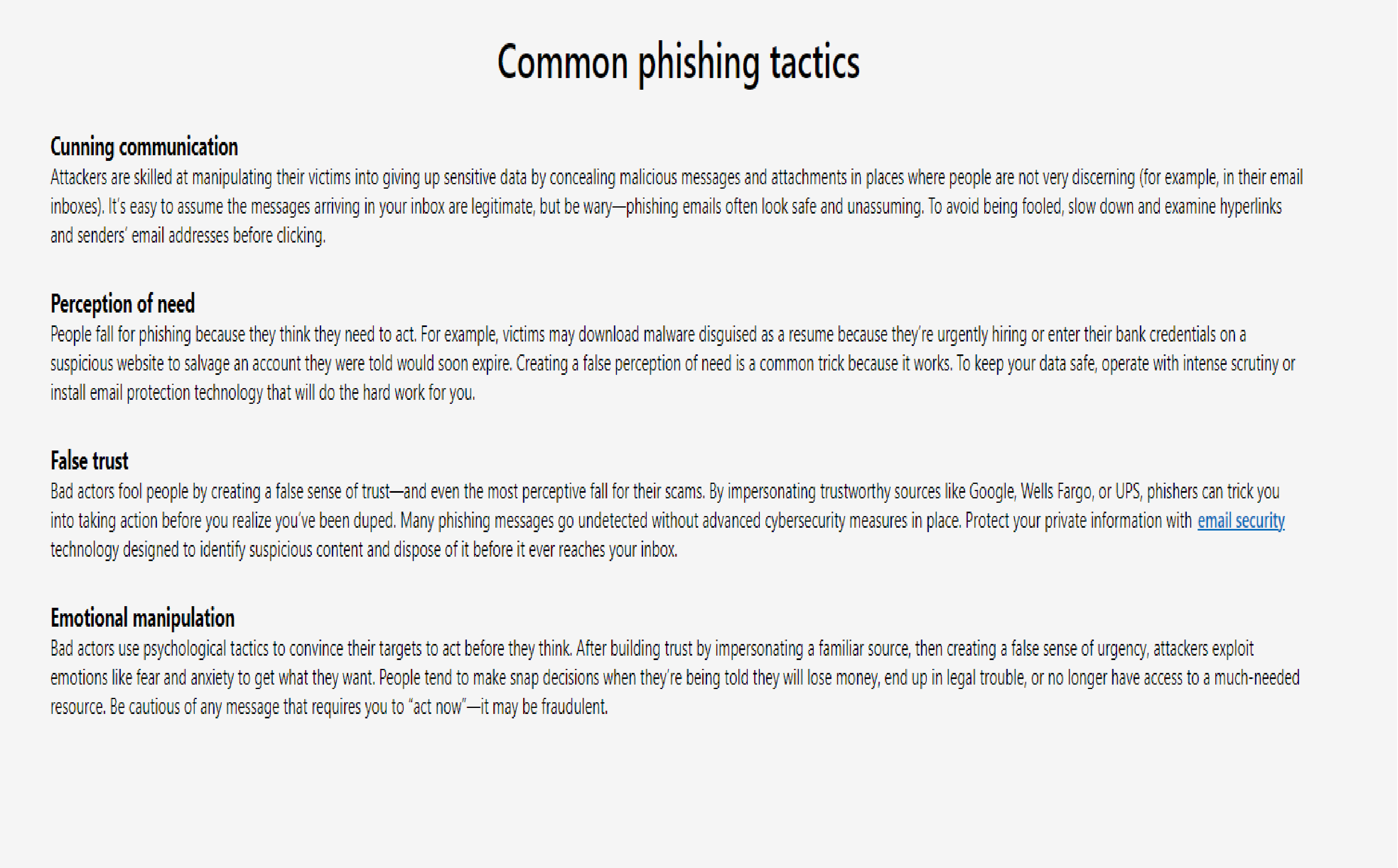
Cuisinart Griddler



other

aztmDCshj33dPVFtql1x@ozmxv.io

Common Phishing Tactics



Common phishing tactics

Cunning communication

Attackers are skilled at manipulating their victims into giving up sensitive data by concealing malicious messages and attachments in places where people are not very discerning (for example, in their email inboxes). It's easy to assume the messages arriving in your inbox are legitimate, but be wary—phishing emails often look safe and unassuming. To avoid being fooled, slow down and examine hyperlinks and senders' email addresses before clicking.

Perception of need

People fall for phishing because they think they need to act. For example, victims may download malware disguised as a resume because they're urgently hiring or enter their bank credentials on a suspicious website to salvage an account they were told would soon expire. Creating a false perception of need is a common trick because it works. To keep your data safe, operate with intense scrutiny or install email protection technology that will do the hard work for you.

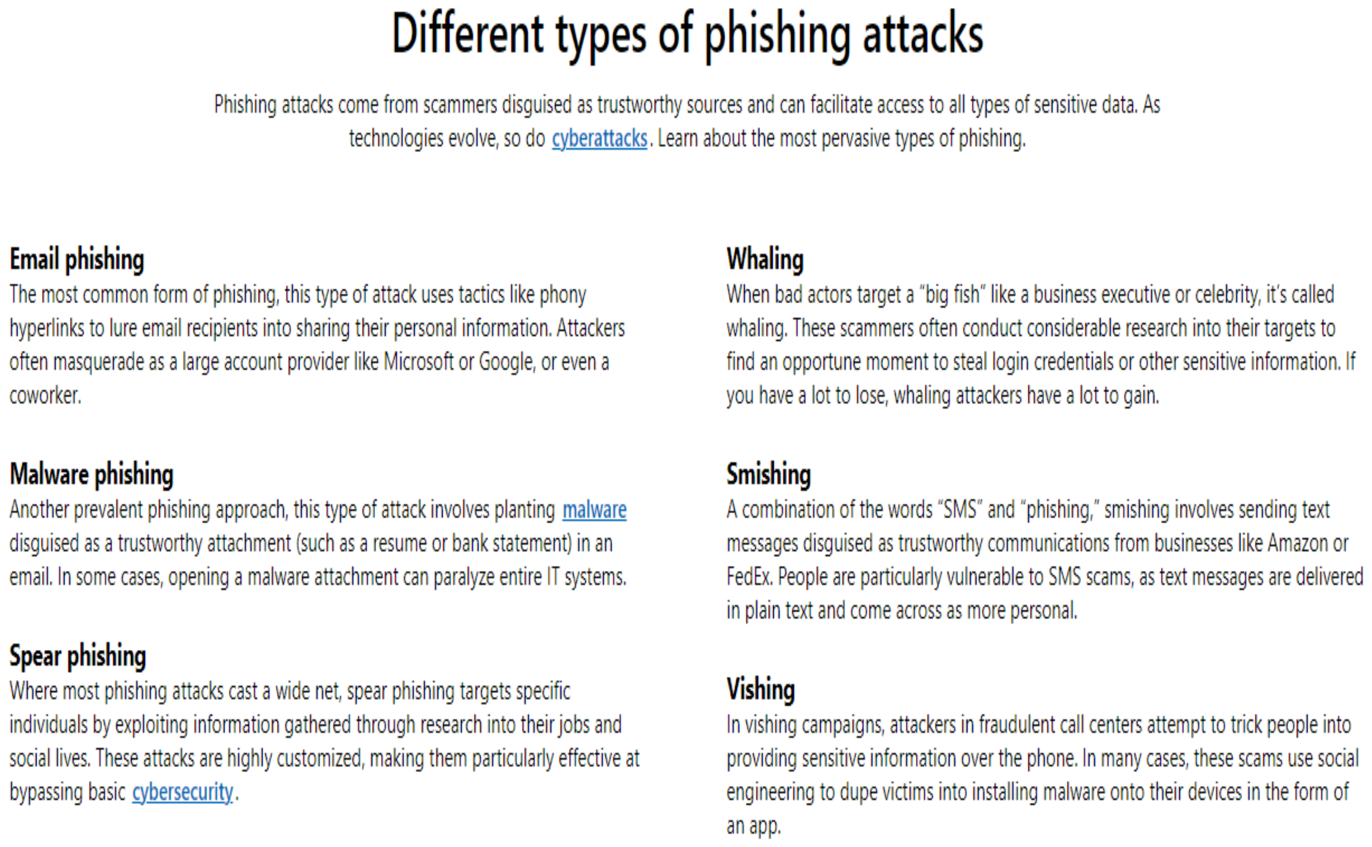
False trust

Bad actors fool people by creating a false sense of trust—and even the most perceptive fall for their scams. By impersonating trustworthy sources like Google, Wells Fargo, or UPS, phishers can trick you into taking action before you realize you've been duped. Many phishing messages go undetected without advanced cybersecurity measures in place. Protect your private information with email security technology designed to identify suspicious content and dispose of it before it ever reaches your inbox.

Emotional manipulation

Bad actors use psychological tactics to convince their targets to act before they think. After building trust by impersonating a familiar source, then creating a false sense of urgency, attackers exploit emotions like fear and anxiety to get what they want. People tend to make snap decisions when they're being told they will lose money, end up in legal trouble, or no longer have access to a much-needed resource. Be cautious of any message that requires you to "act now"—it may be fraudulent.

Different Types of Phishing Attacks



Different types of phishing attacks

Phishing attacks come from scammers disguised as trustworthy sources and can facilitate access to all types of sensitive data. As technologies evolve, so do cyberattacks. Learn about the most pervasive types of phishing.

Email phishing

The most common form of phishing, this type of attack uses tactics like phony hyperlinks to lure email recipients into sharing their personal information. Attackers often masquerade as a large account provider like Microsoft or Google, or even a coworker.

Malware phishing

Another prevalent phishing approach, this type of attack involves planting malware disguised as a trustworthy attachment (such as a resume or bank statement) in an email. In some cases, opening a malware attachment can paralyze entire IT systems.

Spear phishing

Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity.

Whaling

When bad actors target a "big fish" like a business executive or celebrity, it's called whaling. These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information. If you have a lot to lose, whaling attackers have a lot to gain.

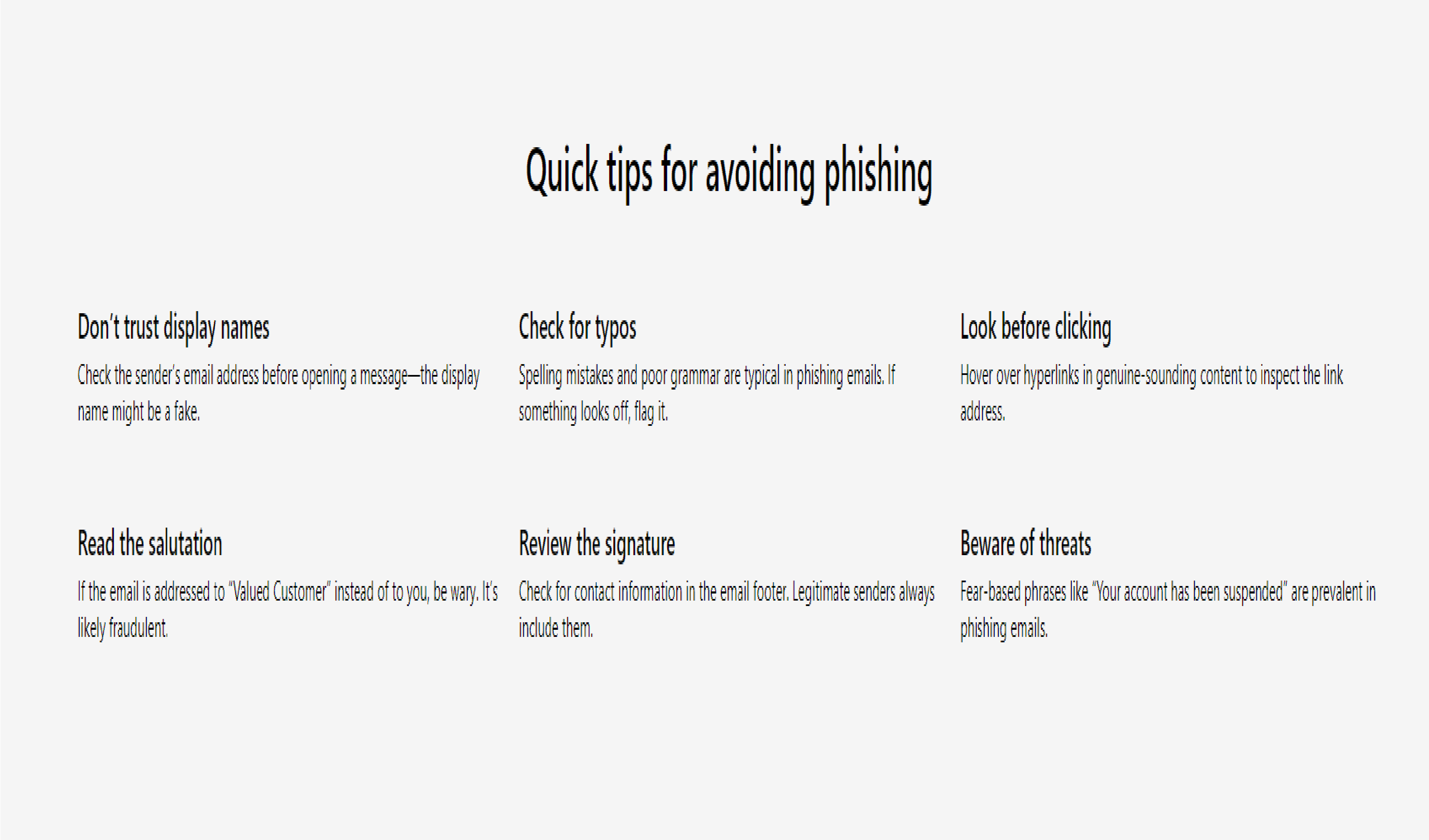
Smishing

A combination of the words "SMS" and "phishing," smishing involves sending text messages disguised as trustworthy communications from businesses like Amazon or FedEx. People are particularly vulnerable to SMS scams, as text messages are delivered in plain text and come across as more personal.

Vishing

In vishing campaigns, attackers in fraudulent call centers attempt to trick people into providing sensitive information over the phone. In many cases, these scams use social engineering to dupe victims into installing malware onto their devices in the form of an app.

Quick Tips for Avoiding Phishing



Quick tips for avoiding phishing

Don't trust display names

Check the sender's email address before opening a message—the display name might be a fake.

Check for typos

Spelling mistakes and poor grammar are typical in phishing emails. If something looks off, flag it.

Look before clicking

Hover over hyperlinks in genuine-sounding content to inspect the link address.

Read the salutation

If the email is addressed to "Valued Customer" instead of to you, be wary. It's likely fraudulent.

Review the signature

Check for contact information in the email footer. Legitimate senders always include them.

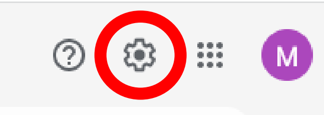
Beware of threats

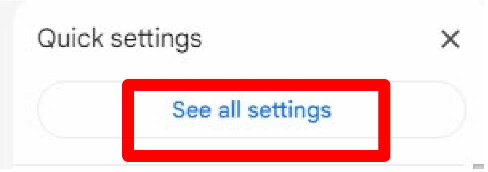
Fear-based phrases like "Your account has been suspended" are prevalent in phishing emails.

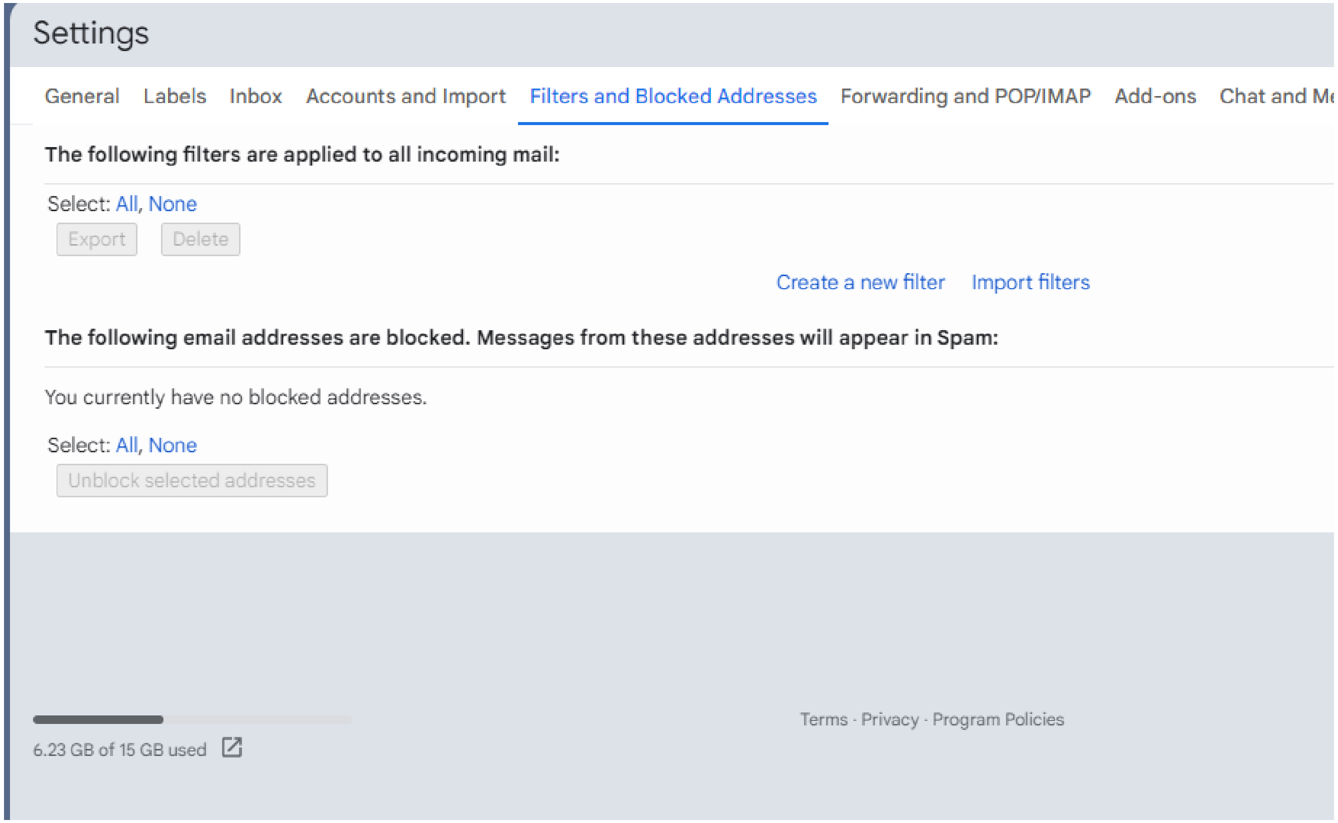
Security Settings for Gmail

Google Mail Account

Google Mail Settings – Filters & Blocked Addresses







The following filters are applied to all incoming mail:

Select: All, None

The following email addresses are blocked. Messages from these addresses will appear in Spam:

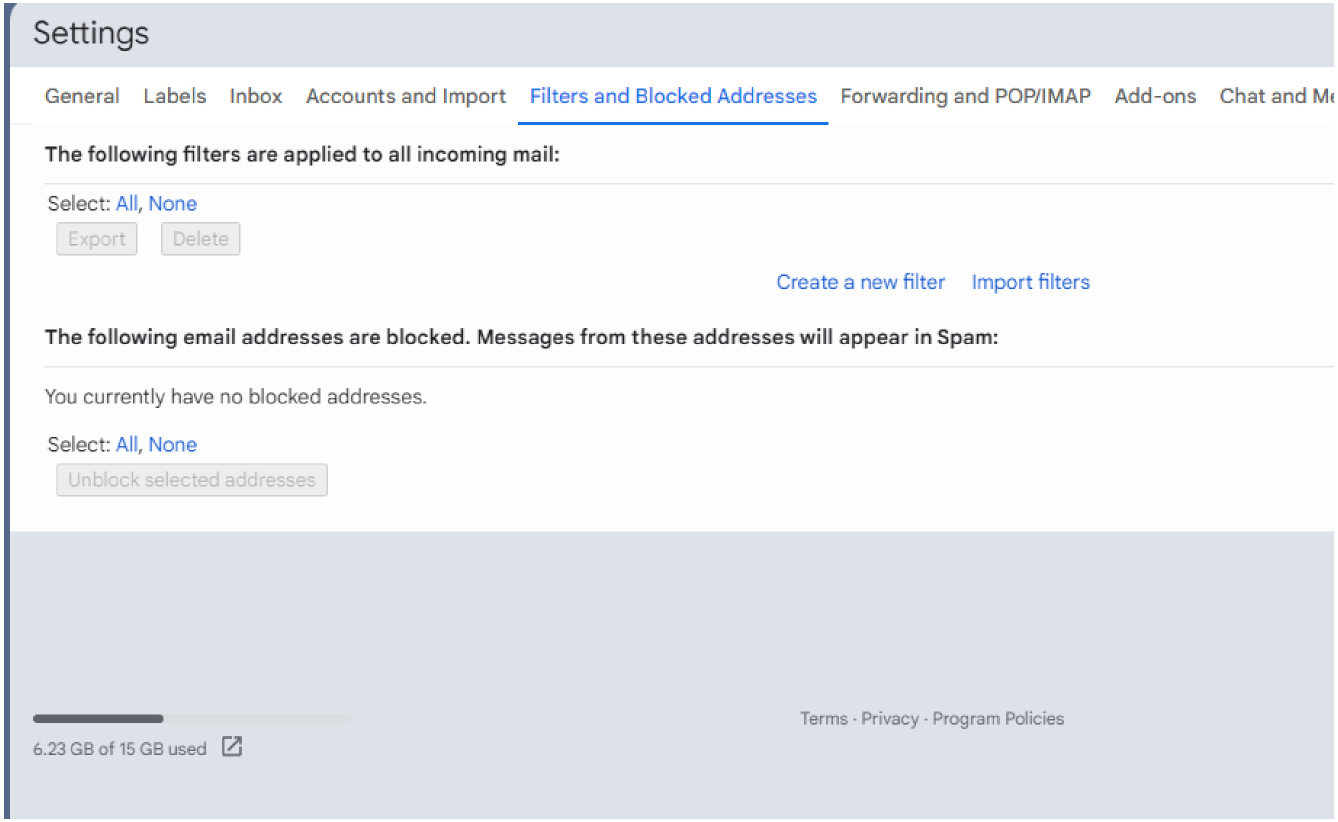
You currently have no blocked addresses.

Select: All, None

Unblock selected addresses
Terms · Privacy · Program Policies

6.23 GB of 15 GB used

Filters and Blocked Addresses



Settings
General Labels Inbox Accounts and Import Filters and Blocked Addresses Forwarding and POP/IMAP Add-ons Chat and Me

The following filters are applied to all incoming mail:

Select: All, None

Export
Delete
Create a new filter
Import filters

The following email addresses are blocked. Messages from these addresses will appear in Spam:

You currently have no blocked addresses.

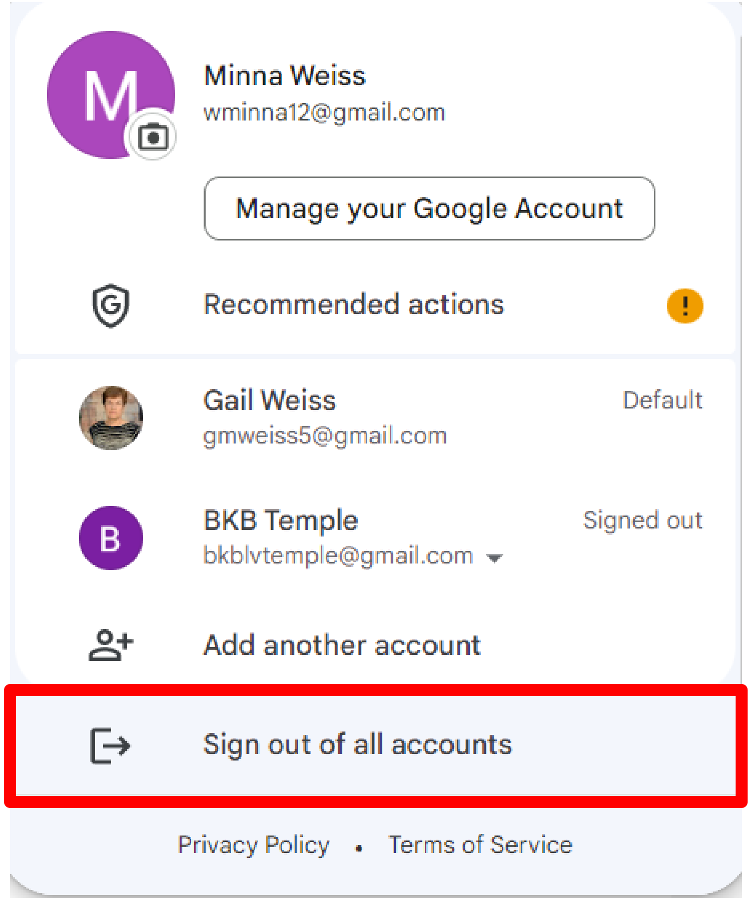
Select: All, None

Unblock selected addresses

6.23 GB of 15 GB used

Terms · Privacy · Program Policies

Always Sign Out of Gmail Account



Minna Weiss
wminna12@gmail.com

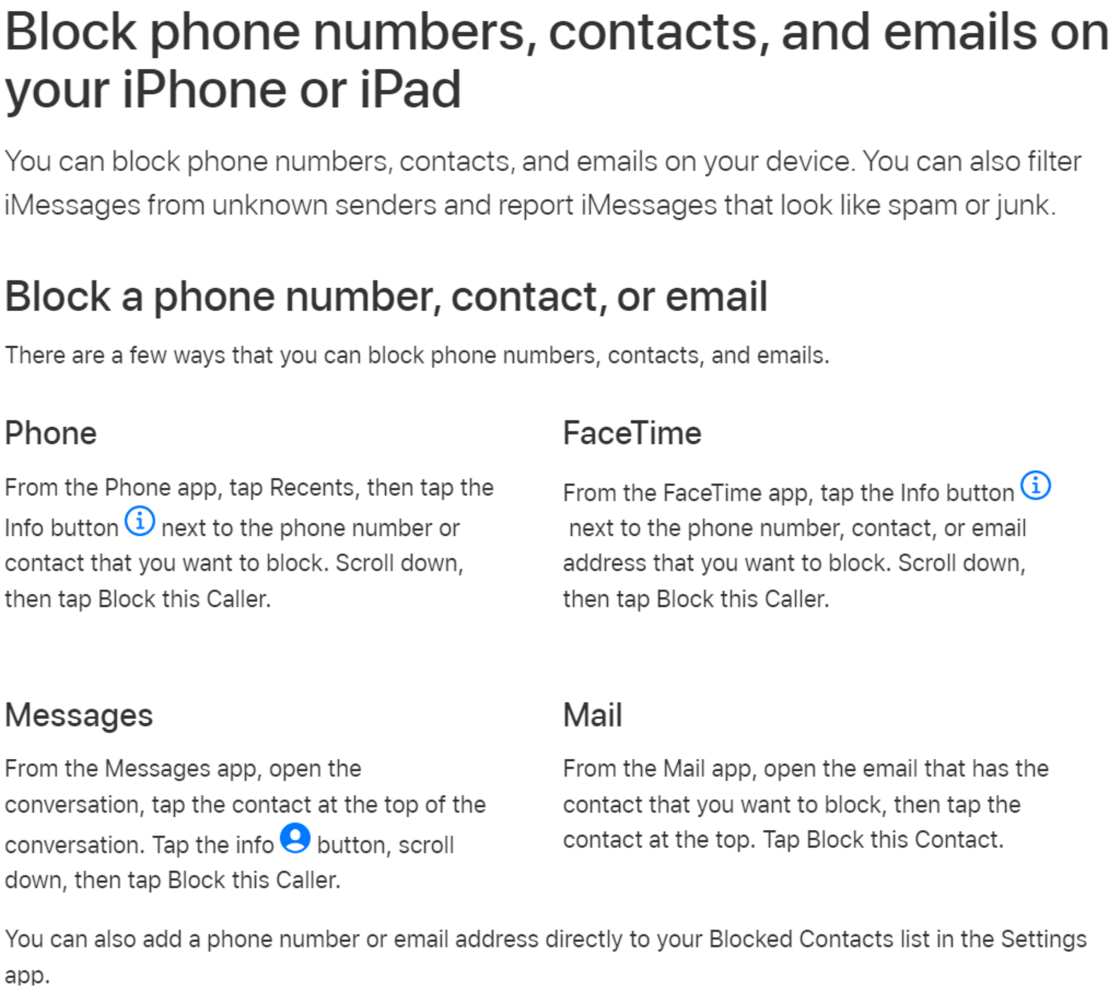
Gail Weiss Default
gmweiss5@gmail.com

BKB Temple Signed out
bkblvtemple@gmail.com

iPhone & Android Security Settings

Apple Tips

- Tips



Block phone numbers, contacts, and emails on your iPhone or iPad

You can block phone numbers, contacts, and emails on your device. You can also filter iMessages from unknown senders and report iMessages that look like spam or junk.

Block a phone number, contact, or email

There are a few ways that you can block phone numbers, contacts, and emails.

Phone

From the Phone app, tap Recents, then tap the Info button ⓘ next to the phone number or contact that you want to block. Scroll down, then tap Block this Caller.

FaceTime

From the FaceTime app, tap the Info button ⓘ next to the phone number, contact, or email address that you want to block. Scroll down, then tap Block this Caller.

Messages

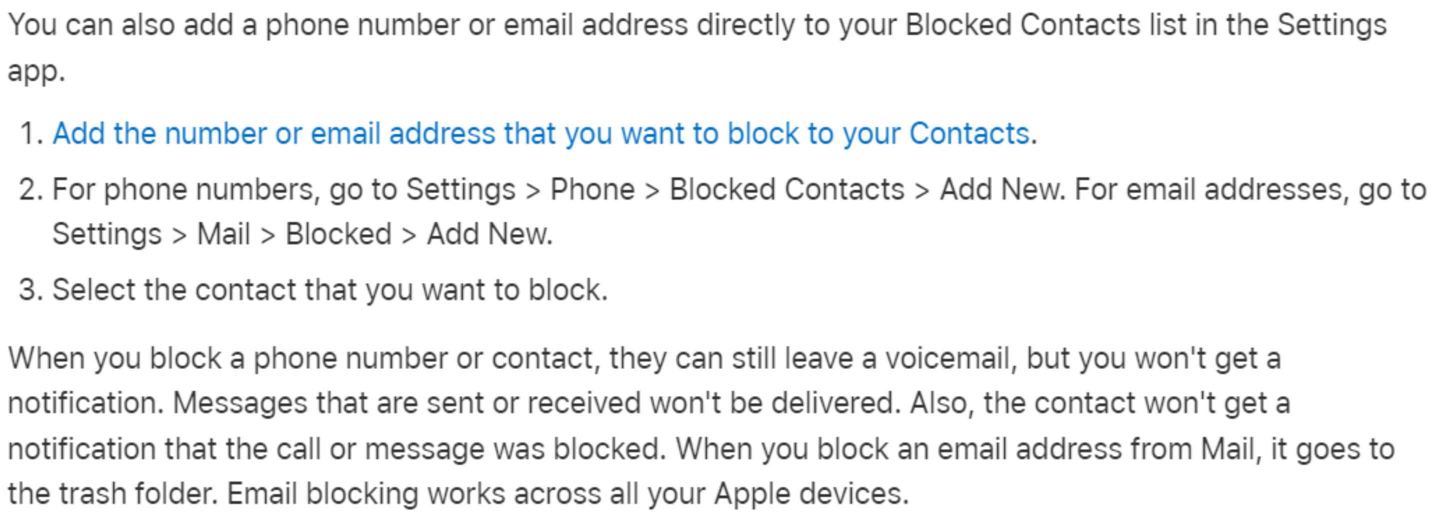
From the Messages app, open the conversation, tap the contact at the top of the conversation. Tap the info 👤 button, scroll down, then tap Block this Caller.

Mail

From the Mail app, open the email that has the contact that you want to block, then tap the contact at the top. Tap Block this Contact.

You can also add a phone number or email address directly to your Blocked Contacts list in the Settings app.

iPhone Settings – Blocking Contacts

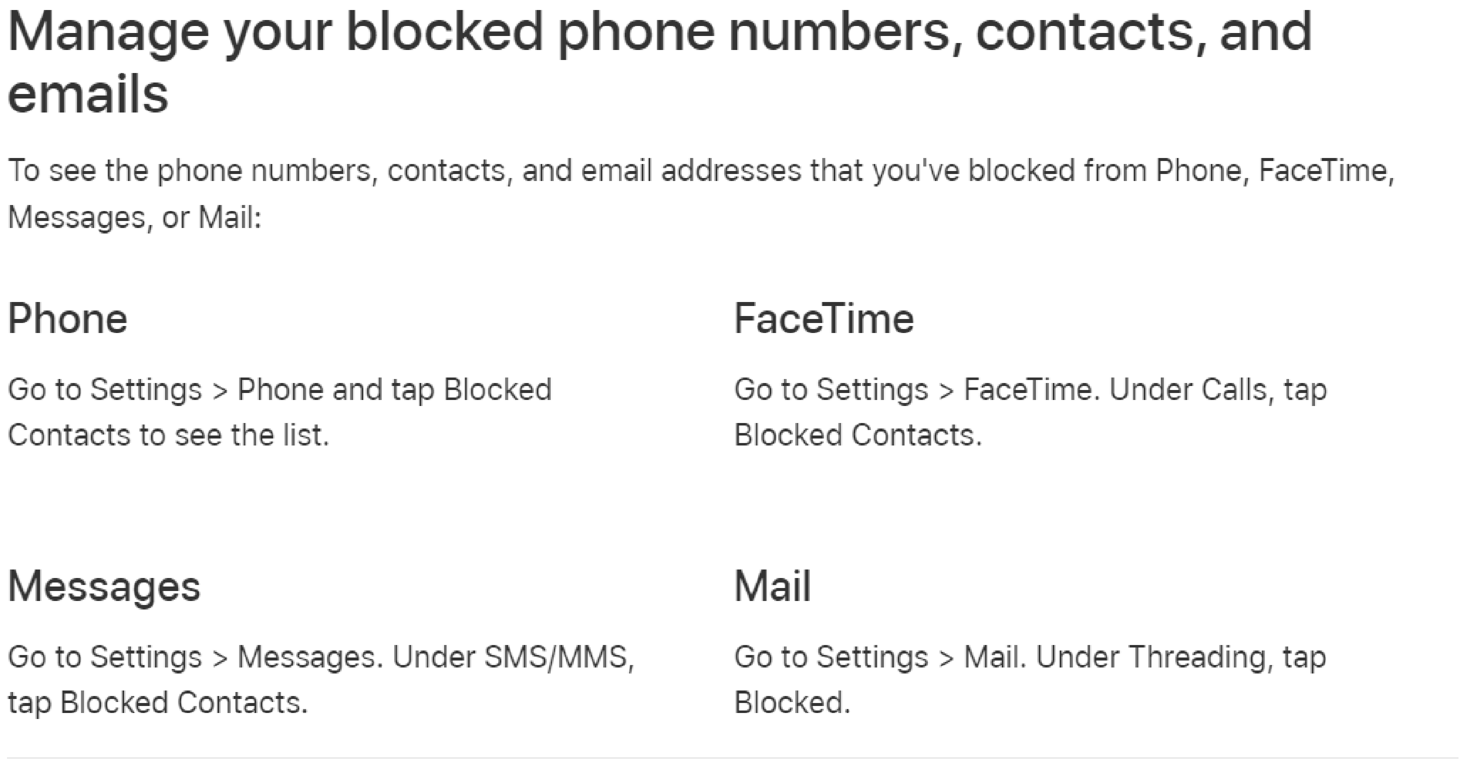


You can also add a phone number or email address directly to your Blocked Contacts list in the Settings app.

1. Add the number or email address that you want to block to your Contacts.
2. For phone numbers, go to Settings > Phone > Blocked Contacts > Add New. For email addresses, go to Settings > Mail > Blocked > Add New.
3. Select the contact that you want to block.

When you block a phone number or contact, they can still leave a voicemail, but you won't get a notification. Messages that are sent or received won't be delivered. Also, the contact won't get a notification that the call or message was blocked. When you block an email address from Mail, it goes to the trash folder. Email blocking works across all your Apple devices.

iPhone Settings – Managing Blocks



Manage your blocked phone numbers, contacts, and emails

To see the phone numbers, contacts, and email addresses that you've blocked from Phone, FaceTime, Messages, or Mail:

Phone

Go to Settings > Phone and tap Blocked Contacts to see the list.

FaceTime

Go to Settings > FaceTime. Under Calls, tap Blocked Contacts.

Messages

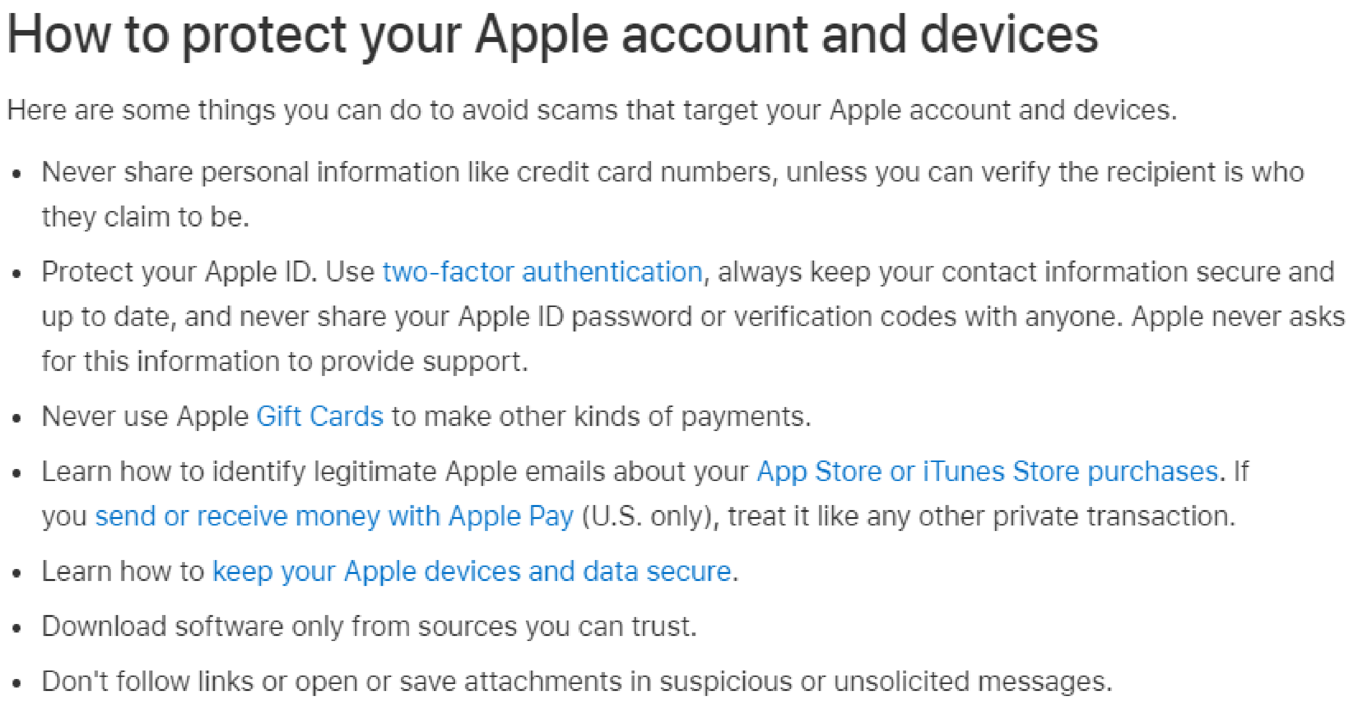
Go to Settings > Messages. Under SMS/MMS, tap Blocked Contacts.

Mail

Go to Settings > Mail. Under Threading, tap Blocked.

iPhone Security Settings

- Block phone numbers, contacts & emails on your Apple Devices
- https://support.apple.com/en-us/HT201229



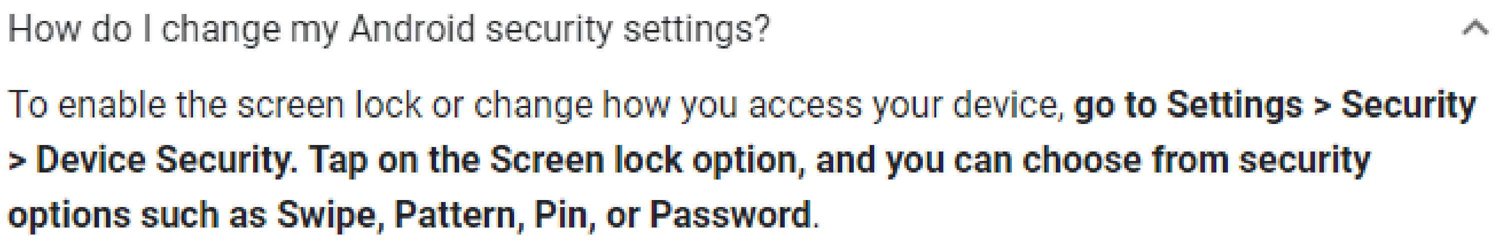
How to protect your Apple account and devices

Here are some things you can do to avoid scams that target your Apple account and devices.

- Never share personal information like credit card numbers, unless you can verify the recipient is who they claim to be.
- Protect your Apple ID. Use two-factor authentication, always keep your contact information secure and up to date, and never share your Apple ID password or verification codes with anyone. Apple never asks for this information to provide support.
- Never use Apple Gift Cards to make other kinds of payments.
- Learn how to identify legitimate Apple emails about your App Store or iTunes Store purchases. If you send or receive money with Apple Pay (U.S. only), treat it like any other private transaction.
- Learn how to keep your Apple devices and data secure.
- Download software only from sources you can trust.
- Don't follow links or open or save attachments in suspicious or unsolicited messages.

Android Security Settings

https://www.computerworld.com/article/3268079/android-settings-security.html



How do I change my Android security settings?

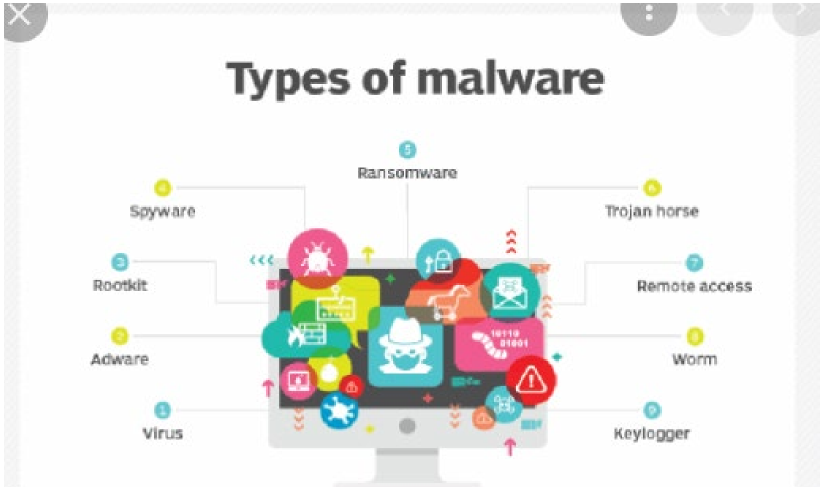
To enable the screen lock or change how you access your device, **go to Settings > Security > Device Security. Tap on the Screen lock option, and you can choose from security options such as Swipe, Pattern, Pin, or Password**.

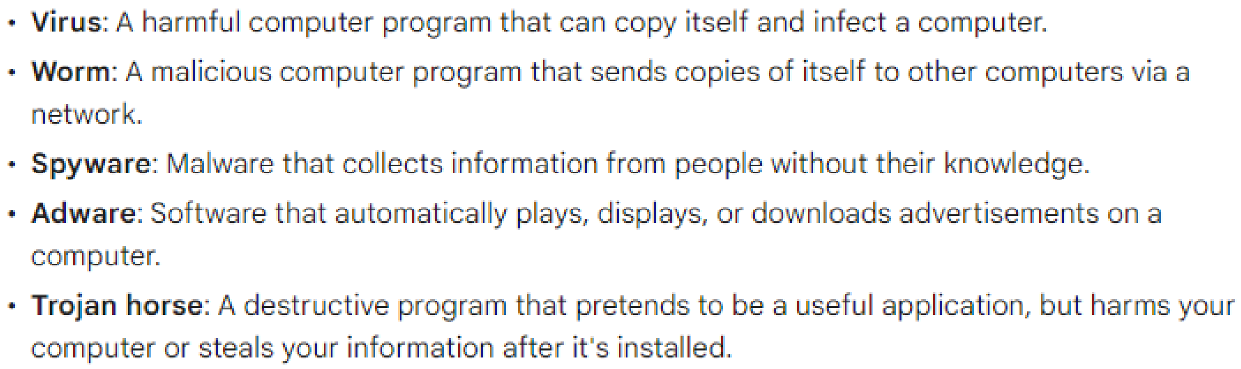
Malware

Windows Computers

Malware

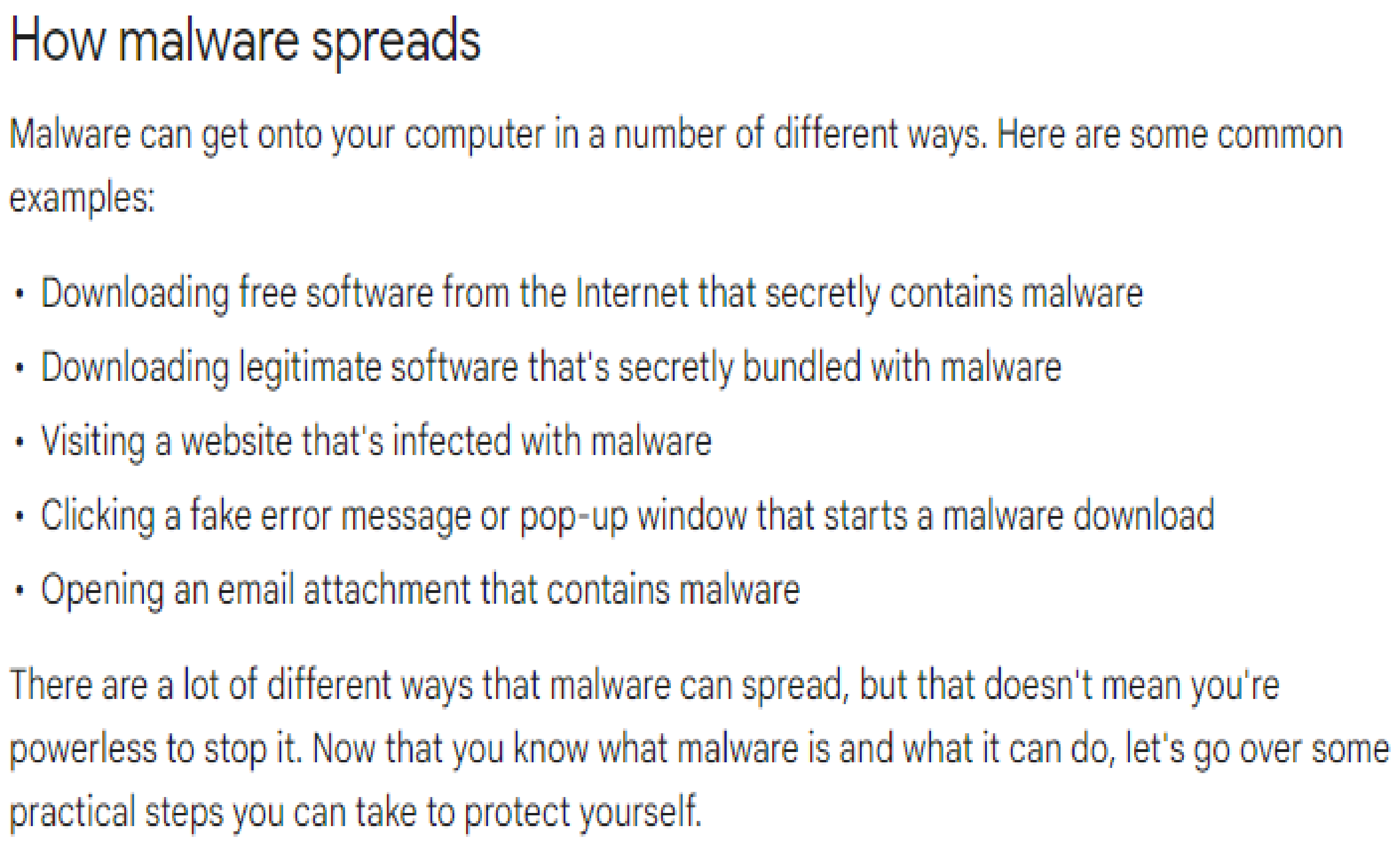
- Software that is specifically designed to disrupt, damage or gain access to a computer system.





- **Virus**: A harmful computer program that can copy itself and infect a computer.
- **Worm**: A malicious computer program that sends copies of itself to other computers via a network.
- **Spyware**: Malware that collects information from people without their knowledge.
- **Adware**: Software that automatically plays, displays, or downloads advertisements on a computer.
- **Trojan horse**: A destructive program that pretends to be a useful application, but harms your computer or steals your information after it's installed.

How Malware Spreads



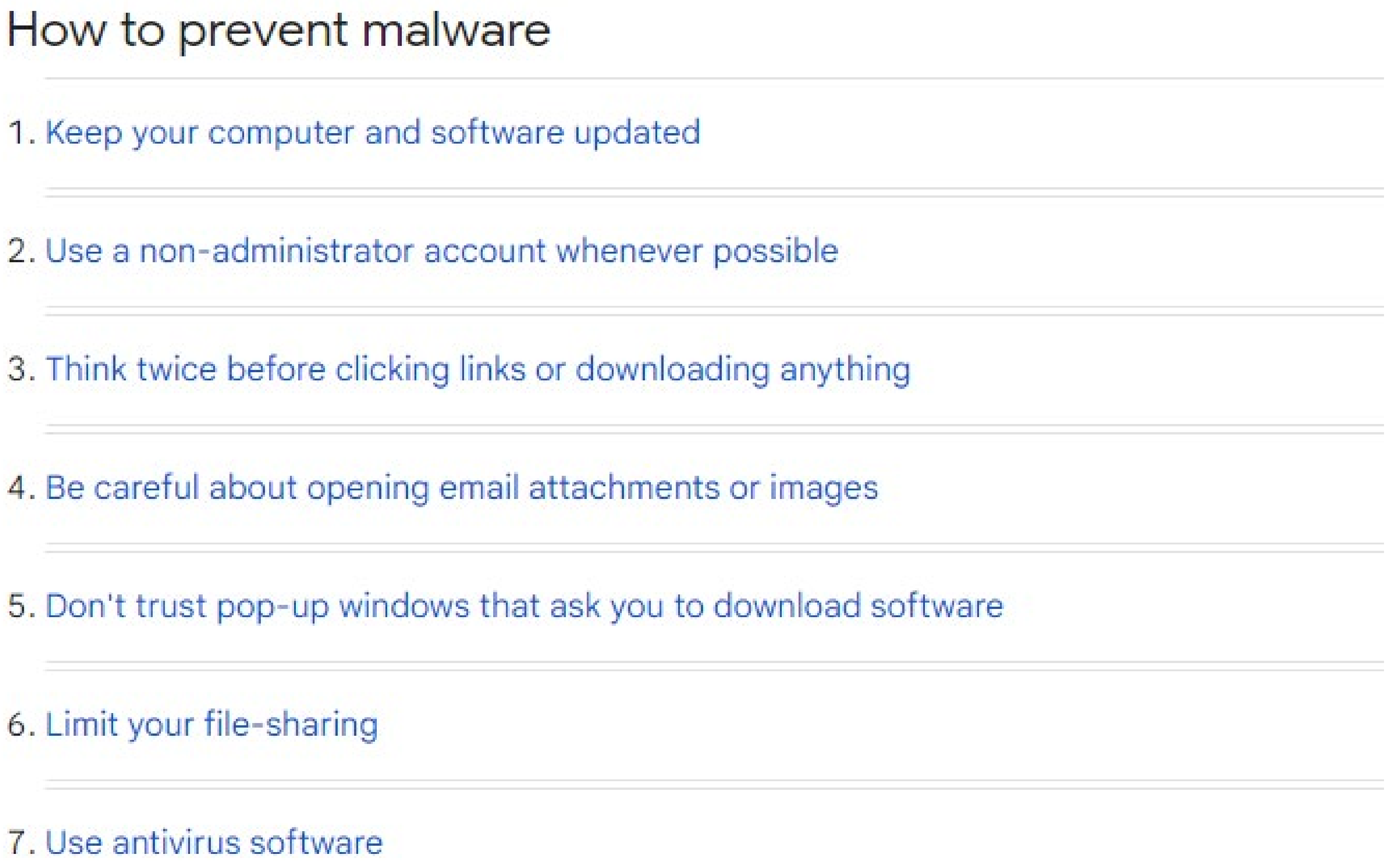
How malware spreads

Malware can get onto your computer in a number of different ways. Here are some common examples:

- Downloading free software from the Internet that secretly contains malware
- Downloading legitimate software that's secretly bundled with malware
- Visiting a website that's infected with malware
- Clicking a fake error message or pop-up window that starts a malware download
- Opening an email attachment that contains malware

There are a lot of different ways that malware can spread, but that doesn't mean you're powerless to stop it. Now that you know what malware is and what it can do, let's go over some practical steps you can take to protect yourself.

How to Prevent Malware



How to prevent malware

1. Keep your computer and software updated
2. Use a non-administrator account whenever possible
3. Think twice before clicking links or downloading anything
4. Be careful about opening email attachments or images
5. Don't trust pop-up windows that ask you to download software
6. Limit your file-sharing
7. Use antivirus software

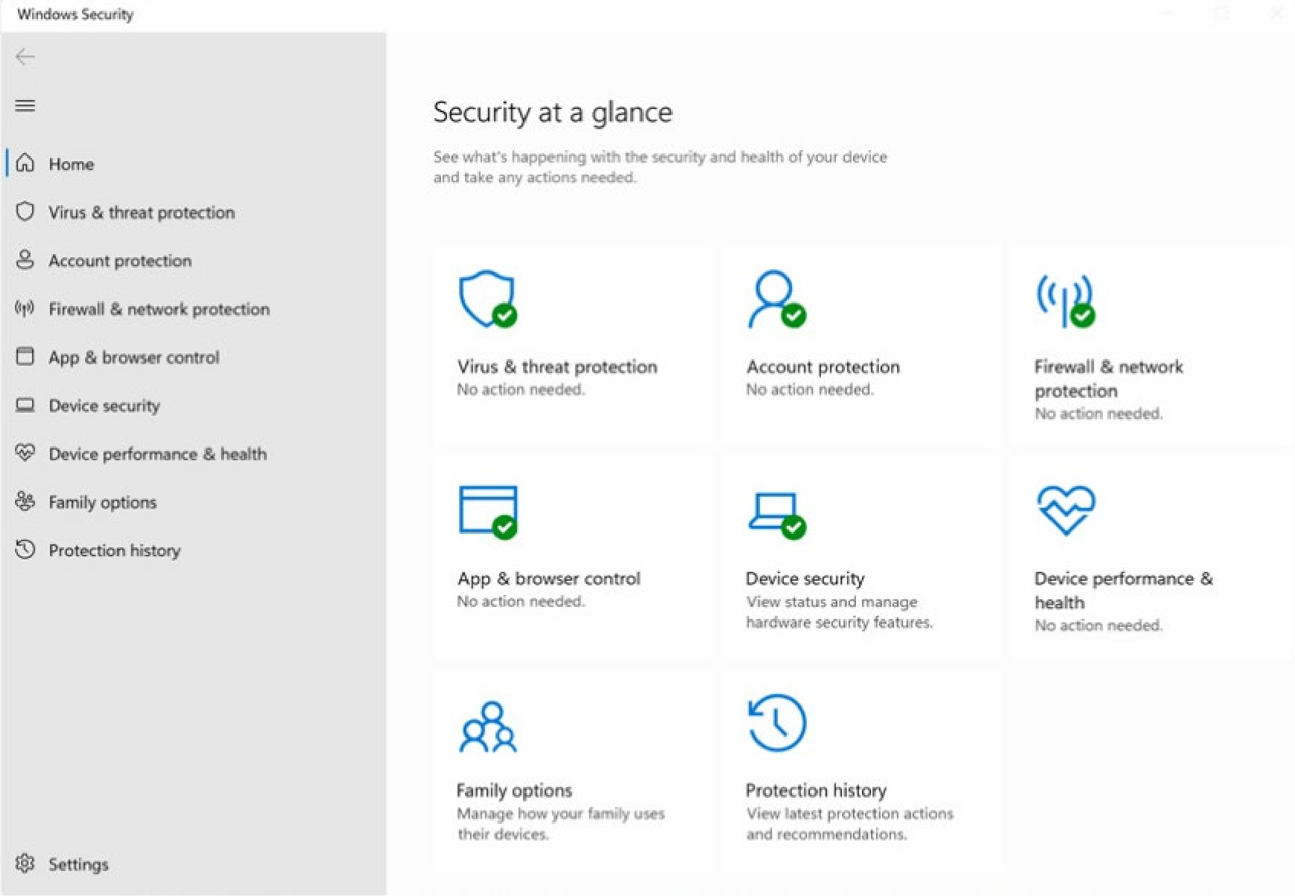
Anti-Virus Software

Anti-Virus Software

- If you need to download anything, you should use an antivirus program to scan that download for malware before opening it. Antivirus software also allows you to scan your entire computer for malware.
- Total AV
- Norton
- Bitdefender
- Webroot
- McAfee

Windows Defender – (Windows 11)

- Advanced AntiVirus Software to defend against today's cyberthreats. Built into Windows 11, routinely updated, and no extra cost to you.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

Managing Passwords

Using Different Passwords for Every Site

- One Single Strong Password Isn't Enough Anymore
- Use of Different Strong Password for Every Important On-Line Account
- Devise a Way to Manage Them All

Using Different Passwords for Every Site

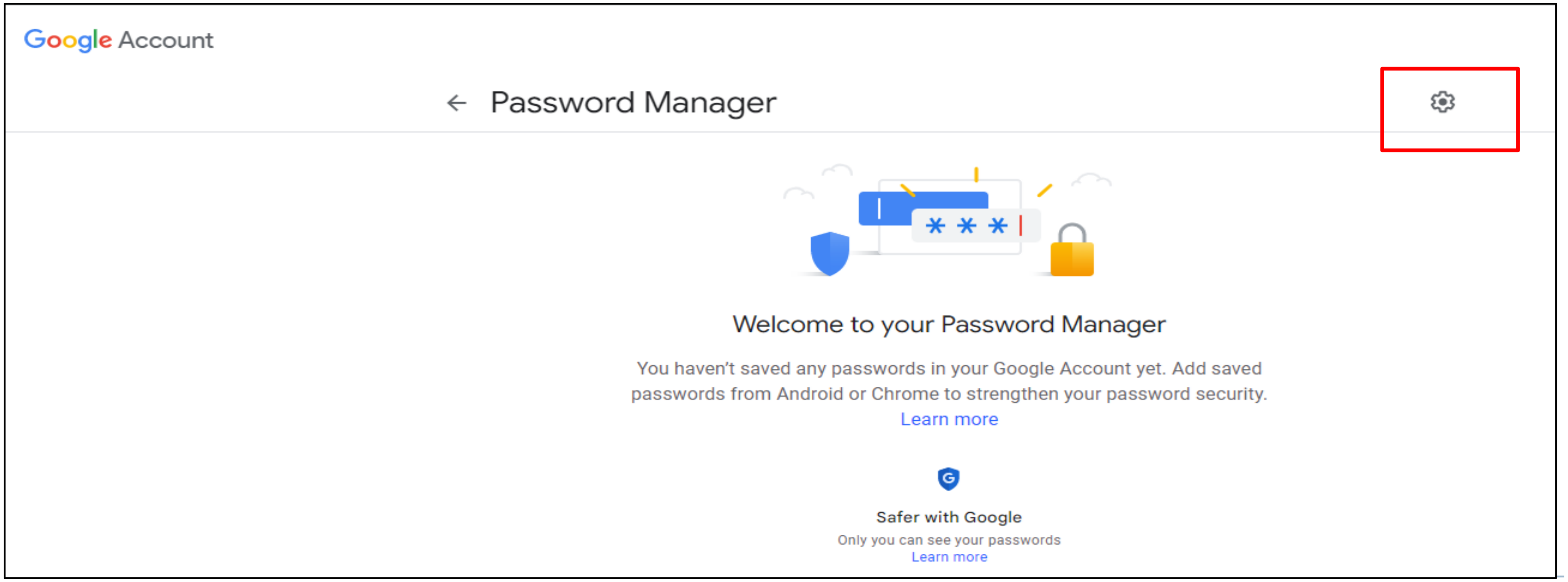
- If you use a Single Password everywhere, a single leak of that password puts all your other accounts at risk
- Hacker breaches Service A's security –
  - Gets your Login ID, Password and Security Questions
  - Now has access to Service B, C & etc.
- Phishing Email Messages Asking for Password
- Improper Use of Open Wi-Fi Hotspot

Tips for Strong Passwords

- Eight to Twelve Characters Minimally
- One Uppercase Letter, Numbers and Special Characters
- Randomly Generated (i.e. By LastPass and other Password Manager Programs)

Google Chrome – Managing Passwords

- Log into your Google Account
- Click Account Icon (upper right corner)
- Click Manage Your Google Account
- Search Passwords
- Select Password Manager - Click Settings Icon



Google Account

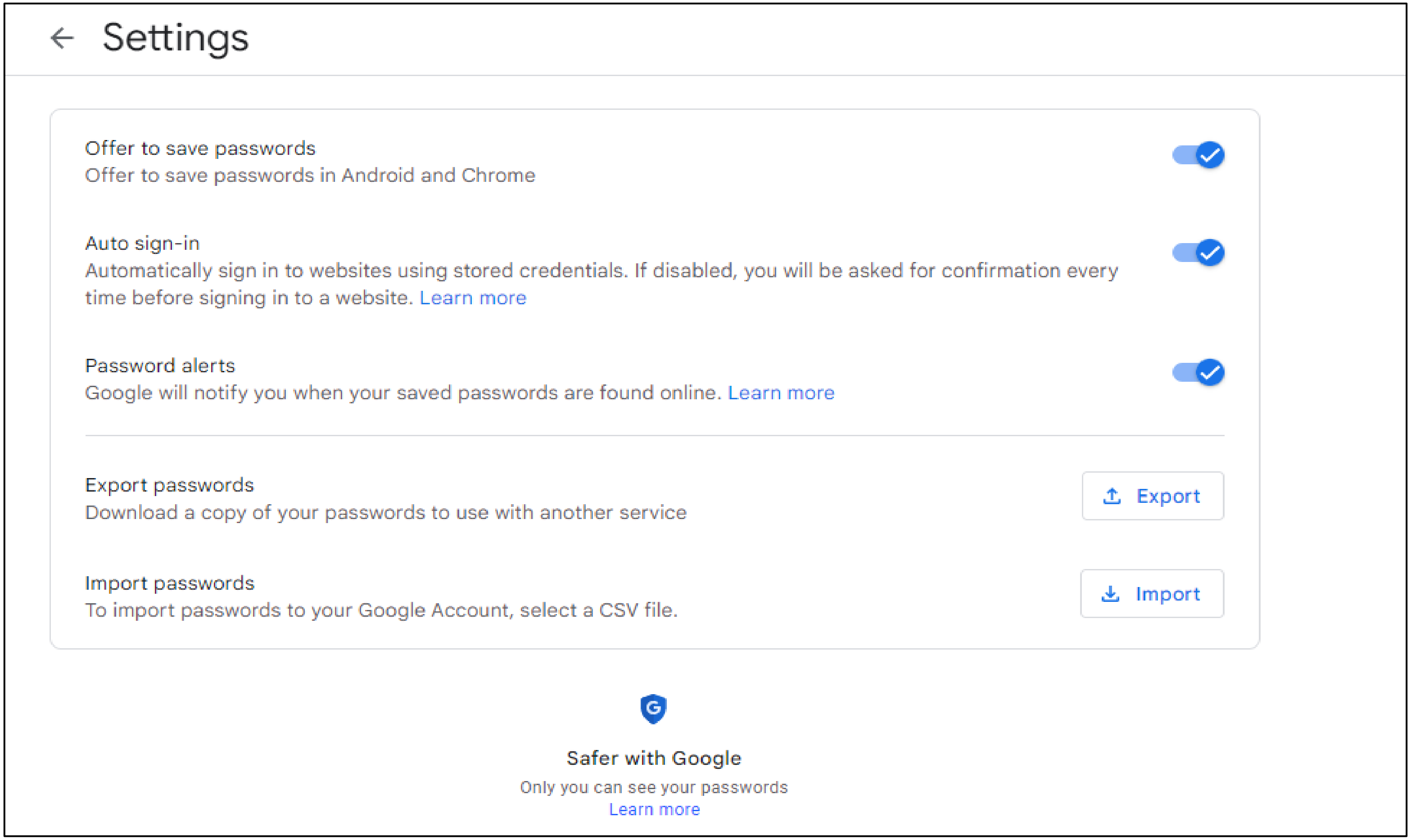
← Password Manager

Welcome to your Password Manager

You haven't saved any passwords in your Google Account yet. Add saved passwords from Android or Chrome to strengthen your password security.
Learn more

Safer with Google
Only you can see your passwords
Learn more

Google Password Manager - Settings



← Settings

Offer to save passwords
Offer to save passwords in Android and Chrome ✓

Auto sign-in
Automatically sign in to websites using stored credentials. If disabled, you will be asked for confirmation every time before signing in to a website. Learn more ✓

Password alerts
Google will notify you when your saved passwords are found online. Learn more ✓

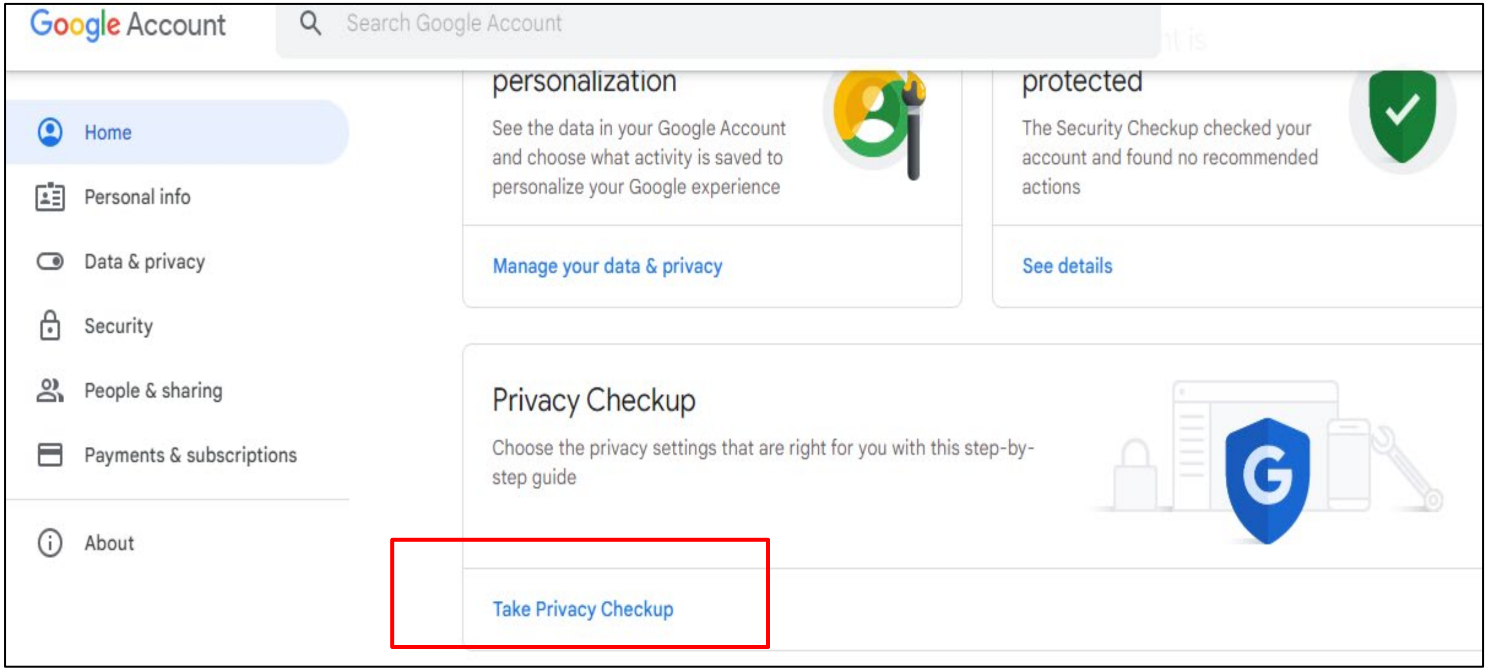
Export passwords
Download a copy of your passwords to use with another service

Import passwords
To import passwords to your Google Account, select a CSV file.

Safer with Google
Only you can see your passwords
Learn more

Google Account – Password Checkup

- Log into your Google Account
- Click Manage Your Account
- Click Take Privacy Checkup



Google Account

Search Google Account

- Home
- Personal info
- Data & privacy
- Security
- People & sharing
- Payments & subscriptions
- About

personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

protected

The Security Checkup checked your account and found no recommended actions

See details

Privacy Checkup

Choose the privacy settings that are right for you with this step-by-step guide

Take Privacy Checkup