# CYBER SAFETY

## Protect yourself and your personal information*

Cybercrime is a growing and serious threat, making it essential that fraud prevention is part of our daily activities. Put these safeguards in place as soon as possible—if you haven’t already.

### Key CYBER SAFETY Tips

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create separate email accounts for work, personal use, alert notifications and other interests</td>
</tr>
<tr>
<td>2</td>
<td>Be cautious of clicking on links or attachments sent to you in emails</td>
</tr>
<tr>
<td>3</td>
<td>Use secure messaging tools when transmitting sensitive information via email or text message</td>
</tr>
<tr>
<td>4</td>
<td>Create strong passwords and change them regularly</td>
</tr>
<tr>
<td>5</td>
<td>Do not use the same password for multiple accounts</td>
</tr>
<tr>
<td>6</td>
<td>Minimize the use of unsecured, public networks</td>
</tr>
<tr>
<td>7</td>
<td>At work, limit web usage to core, business-related sites</td>
</tr>
<tr>
<td>8</td>
<td>At home, set up a primary network and a separate one for guests and children</td>
</tr>
<tr>
<td>9</td>
<td>Install anti-virus software on all your devices and keep it up-to-date</td>
</tr>
<tr>
<td>10</td>
<td>Be prudent in what you share about yourself and your job via social media</td>
</tr>
</tbody>
</table>

### Email

- Use separate email accounts: one each for work, personal use, user IDs, alerts, notifications, other interests
- Choose a reputable email provider that offers spam filtering and multi-factor authentication
- Use secure messaging tools when replying to verified requests for financial or personal information
- Encrypt important files before emailing them
- Do not open emails from unknown senders

### Passwords

- Create complex passwords that are at least 10 characters; use a mix of numbers, upper- and lowercase letters and special characters
- Change passwords at least four times a year
- Consider utilizing a password management tool
- Do not use the same password for multiple accounts
- Do not click “Remember my password” or “Remember me” on websites you visit

### Mobile

- Keep screen lock on; choose strong passwords and use biometric tools when available
- Select a device with anti-theft features
- Turn off Bluetooth when it’s not needed
- Regularly update apps (e.g., security patches)
- Securely back up your data
- Review your privacy, location and password settings
- Pay attention to the information an app can access and regularly review permissions
- Enable remote automatic wipe in settings to ensure your personal information is erased automatically if you report your device as lost
- Do not click on ads when surfing the internet

### Public Wi-Fi/hotspots

- Minimize the use of unsecured, public networks
- Turn off auto connect to non-preferred networks
- Turn off file sharing
- When public Wi-Fi cannot be avoided, use a virtual private network (VPN) to help secure your session
- Disable ad hoc networking, which allows direct computer-to-computer transmissions
- Never use public Wi-Fi to enter personal credentials on a website; hackers can capture your keystrokes

### Home networks

- Create one network for you, another for guests and children
- Change the default password to your wireless network
- Turn on router’s WPA2 encryption and firewall
- Enable “Do not broadcast” on your primary network’s name (SSID) via the router software
- Do not use default router names/passwords

### Virus and malware protection

- Install anti-virus and ad-blocking software and keep it up-to-date
- Keep software, browser and operating systems up-to-date
- Regularly back up your data
- Do not install or use pirated software
- Do not install file-sharing programs
- Do not set email to auto-open attachments

### Social engineering

- Confirm the identity of anyone requesting information or access to your data or devices via an alternate, verified method
- Limit the amount of personal information you post online
- Review privacy settings on social media accounts
- Do not open an attachment from someone you know if you are not expecting it; call to confirm before clicking
- Do not assume a request is genuine just because the requester knows information about you or your company
- Do not use personal information widely available on social media (pet’s name, child’s birthdate) to protect online accounts

---

*Cybercrime is a growing and serious threat, making it essential that fraud prevention is part of our daily activities. Put these safeguards in place as soon as possible—if you haven’t already.*
When selecting services, software and equipment, consider the following:

<table>
<thead>
<tr>
<th>Email providers</th>
<th>FEATURES TO LOOK FOR</th>
</tr>
</thead>
</table>
| Email is one of the most essential online services used today. If your email is compromised, your personal information (accounts, communications, phone numbers, addresses, etc.) can be stolen. The best email providers surround your information with several layers of security. | AUTHENTICATION  
Provides secure authentication to help prevent spam and spoofing.  
VIRUS SCANNING  
Email is scanned for malicious content by the provider.  
Look for a provider that offers multi-factor authentication and an intuitive interface. |

<table>
<thead>
<tr>
<th>Password managers</th>
<th>FEATURES TO LOOK FOR</th>
</tr>
</thead>
</table>
| Weaknesses stem from how individuals choose and manage passwords, which can make it very easy for hackers to access them and break into individual accounts. Password management tools help users store and organize passwords, and can even provide additional features, such as form filling and password generation. | Synchronization  
A password manager should allow secure access from anywhere and synchronize across devices.  
Password Generator  
Can automatically generate strong, complex passwords.  
Look for a password management tool that supports the types of browsers, operating systems and mobile devices you use. |

<table>
<thead>
<tr>
<th>Virus and malware protection</th>
<th>FEATURES TO LOOK FOR</th>
</tr>
</thead>
</table>
| If you use a computer or mobile device for web surfing, shopping, banking, email and instant messaging and do not have adequate protection, you are a higher risk for becoming a victim. Running real-time anti-virus products and keeping them up-to-date is an essential step to reduce risks from malware. | Detection  
Should detect existing and new variations of malicious software.  
Cleaning  
Effectively quarantines or removes malicious software from an infected device.  
Protection  
Helps maintain a healthy system by proactively preventing malicious infection.  
Consider the number of devices that each vendor will allow the software to be installed on per license subscription purchase. |

<table>
<thead>
<tr>
<th>Wireless routers</th>
<th>FEATURES TO LOOK FOR</th>
</tr>
</thead>
</table>
| A wireless router allows you to connect devices to the internet and communicate with other devices on your network. Routers are like computers, with their own operating systems, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log key strokes, access your accounts and can infect devices on your network. | Auto-update  
Choose a router that automatically updates its software, also known as firmware.  
Firewall  
Secures your network from intruders.  
Look for a router with a range that fits the size of your home and supports the number of devices you want to connect to it. |

*This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect itself against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.*
Securing your mobile devices*

Your mobile device, which has made life so much more convenient, can track who you are, where you have been, and information about your friends, family and contacts. This can make you and your device a prime target for hackers. Here are some easy steps to keep your information more secure.

*Note: Menu navigation in this guide may vary based on your mobile carrier and software version.*

### Mobile device safety guidelines

- Set a passcode on your mobile device as one of your first lines of defense. Use a 6-digit lock code and enable biometrics (fingerprint or facial recognition) on your mobile device. Avoid using a swipe pattern that can be easily guessed or shoulder surfed. Guard your mobile device code as you would a bank or credit card PIN code.
- Review the apps on your phone and what type of data they collect and share with others. Stop your phone and apps from tracking your location when they are not in use.
- Install anti-virus from a reputable provider on your mobile devices.
- Enable tracking, controlling and wiping of your mobile device when not in your possession, so you can remotely erase all data on your device if it is lost or stolen.

### Instructions for popular mobile devices on:

- Locking your device
- Limiting information appearing on your screen
- Protecting your data

- iPhone and iPad .......................... page 3
- iPhone X and 11 .......................... page 5
- Samsung Galaxy S9 ........................ page 7
- Android Google Pixel and Pixel X ....... page 9
- Android BlackBerry Key2 LE ............. page 11
This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect itself against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.
Limit your potential exposure

1. Lock your device
Setting a passcode on your mobile device is one of your first lines of defense in keeping your information private, particularly in the event your device is lost or stolen.

   • Navigate to Settings > Touch ID & Passcode > Turn Passcode ON > Enter a 6-digit passcode

   Use Touch ID if you prefer to unlock your iOS device with your fingerprint:

   • Navigate to Settings > Touch ID & Passcode > Add a fingerprint > Switch ON: iPhone Unlock

2. Limit information appearing on your lock screen and access to your device
Prevent information about you and/or your contacts from appearing on your locked device:

   • Navigate to Settings > Touch ID & Passcode > Enter Passcode > Allow Access When Locked > Switch OFF: Today View, Notification Center, Control Center, Siri, Reply with Message, Home Control, Wallet, Return Missed Calls, and USB Accessories

   Disable wireless technologies when not in use:

   • Wi-Fi and Bluetooth:
   Settings > Switch OFF: Wi-Fi and Bluetooth

   • AirDrop:
   Settings > General > AirDrop > Suggestion: Switch to “Receiving Off” or “Contacts Only”

3. Protect your data if your phone is lost or stolen
Set your phone to automatically erase all of your data after 10 incorrect password attempts:

   • Navigate to Settings > Touch ID & Passcode > Enter Passcode > Switch ON: Erase Data

   Note: Regularly back up your device to iCloud or your computer, via USB with iTunes, to ensure you can reinstall your data, apps and settings upon recovery.
4. Disable tracking of your device
By default, iOS tracks your device’s most frequently visited locations. Disabling this feature ensures that information could never end up in the wrong hands:

- Navigate to Settings > Privacy > Location Services > System Services > Significant Locations > Clear History > Switch OFF: Significant Locations

Your device will ask you to use TouchID or the passcode to see Significant Locations.

5. Limit data and location tracking
Application tracking
Some applications need your current location in order to function. Stop them from tracking your location when you’re not using them:

- Navigate to Settings > Privacy > Location Services > Change access for each app from Always to either Never or While Using

Advertising
Limit advertisers from building a personal profile about you:

- Navigate to Settings > Privacy > Advertising > Switch ON: Limit Ad Tracking > Reset Advertising Identifier

Browser controls
Safari can save the personal information you use on websites, such as usernames, passwords and addresses. To opt for security over convenience, disable this feature:

- Navigate to Settings > Safari > Autofill > Switch OFF: Use Contact Info and Credit Cards

6. Find your device if it’s misplaced, lost or stolen
Locate and maintain control of your iPhone or iPad, even if it’s not in your possession, by:
- Changing your passcode
- Preventing it from being reactivated with another phone number
- Erasing all of your data

- Navigate to Settings > Apple ID profile > Find My iPhone (or iPad) > Switch ON: Find My iPhone | iPad

Strongly consider installing the app Lookout: Security and Identity Theft Protection from the App Store. It can provide advanced theft alerts and monitor your device for potentially malicious activity.

7. Password protect app purchases
Control what’s downloaded or purchased on your device through the App Store by requiring your password to be entered before a transaction can be completed:

- Navigate to Settings > Screen Time > Content & Privacy Restrictions > iTunes & App Store Purchases > Select Always Require
Limit your potential exposure

1. Lock your device

Setting a passcode on your mobile device is one of your first lines of defense in keeping your information private, particularly in the event your device is lost or stolen.

   - Navigate to Settings > Face ID & Passcode > Turn Passcode ON > Enter a 6-digit passcode
   
   Use Face ID if you prefer to unlock your iOS device with your face:

   - Navigate to Settings > Face ID & Passcode > Set Up Face ID > Switch ON: iPhone Unlock

2. Limit information appearing on your lock screen and access to your device

Prevent important information about you and/or your contacts from appearing on your locked device:

   - Navigate to Settings > Face ID & Passcode > Use Face ID or enter passcode > Allow Access When Locked > Switch OFF: Today View, Notification Center, Control Center, Siri, Reply with Message, Home Control, Wallet, Return Missed Calls, and USB Accessories

   - Navigate to Settings > Face ID & Passcode > Use Face ID or enter passcode > Siri & Search > Switch OFF: Listen for “Hey Siri” and “Press Side button for Siri”

Disable wireless technologies when not in use:

   - Wi-Fi and Bluetooth: Settings > Switch OFF: Wi-Fi and Bluetooth

   - AirDrop: Settings > General > AirDrop > Suggestion: Switch to “Receiving Off” or “Contacts Only”

3. Protect your data if your phone is lost or stolen

Set your phone to automatically erase all of your data after 10 incorrect password attempts:

   - Navigate to Settings > Face ID & Passcode > Use Face or enter passcode > Switch ON: Erase Data

Note: Regularly back up your device to iCloud or your computer, via USB with iTunes, to ensure you can reinstall your data, apps and settings upon recovery.
4. Disable tracking of your device
By default, iOS tracks your device’s most frequently visited locations. Disabling this feature ensures that information could never end up in the wrong hands:

- Navigate to Settings > Privacy > Location Services > System Services > Significant Locations > Clear History > Switch OFF: Significant Locations

Your device will ask you to use Face ID or the passcode to see Significant Locations.

5. Limit data and location tracking

Application tracking
Some applications need your current location in order to function. Stop them from tracking your location when you’re not using them:

- Navigate to Settings > Privacy > Location Services > Change access for each app from Always to either Never or While Using

Advertising
Limit advertisers from building a personal profile about you:

- Navigate to Settings > Privacy > Advertising > Switch ON: Limit Ad Tracking and select Reset Advertising Identifier > Reset Identifier

Browser controls
Safari can save the personal information you use on websites, such as usernames, passwords and addresses. To opt for security over convenience, disable this feature:

- Navigate to Settings > Safari > Autofill > Switch OFF: Use Contact Info and Credit Cards

6. Find your device if it’s misplaced, lost or stolen
Locate and maintain control of your iPhone, even if it’s not in your possession, by:
- Changing your passcode
- Preventing it from being reactivated with another phone number
- Erasing all of your data

- Navigate to Settings > Apple ID profile > iCloud > Find My iPhone > Switch ON: Find My iPhone

Strongly consider installing the app Lookout: Security and Identity Theft Protection from the App Store. It can provide advanced theft alerts and monitor your device for potentially malicious activity.

7. Password protect app purchases
Control what’s downloaded or purchased on your device through the App Store by requiring your password to be entered before a transaction can be completed:

- Navigate to Settings > Screen Time > Content & Privacy Restrictions > iTunes & App Store Purchases > Select Always Require
Limit your potential exposure

1. Lock your device
   Enable a lock screen password to prevent unauthorized use of your device:
   • Navigate to Settings > Lock screen and security > Screen lock type > Enter password (if prompted) > Pin > Enter a 6-digit passcode and confirm
   Set your device to lock itself when it’s not in use:
   • Navigate to Settings > Lock screen and security > Secure lock settings > Lock automatically > Immediately > Switch ON: Lock instantly with power key, Auto factory reset and Lock network and security
   Additionally, use Fingerprint Scanner if you prefer to unlock your Galaxy with your fingerprint:
   • Navigate to Settings > Lock screen and security > Screen lock type > Switch ON: Fingerprints > Follow activation steps

2. Limit information appearing on your lock screen
   Android allows you to select the type of notification displayed on your locked Android device. “Hide content” will limit the information about the sender and message contents:
   • Navigate to Settings > Lock screen and security > Notifications > Switch ON: Hide Content

3. Disable tracking of your device
   By default, Android tracks where you have taken your device. Disabling this feature will help protect you.
   Disable Google Location History:
   • Navigate to Settings > Connections > Location > Google Location History > Switch OFF > Then select Manage Activities > Menu > Settings > Delete all Location History
4. Limit data tracking on your device

Your browser may save information about you and the websites you visit, such as usernames, passwords and addresses. To opt for security over convenience, disable this feature:

- Navigate to Chrome > Menu > Settings > Autofill and payments > Switch OFF: Autofill forms
- Navigate to Chrome > Menu > Settings > Passwords > Switch OFF: Save passwords

5. Find your device if it’s misplaced, lost, or stolen

Android Device Manager allows you to locate the physical location of your device and also:
- Lock and reset device password
- Make device ring
- Remotely erase all data on your device

- Navigate to Settings > Google > Security > Find My Device > Switch ON: Find My Device

Find My Device can be accessed via a web browser at: https://www.android.com/find

6. Password protect app purchases

Before making a purchase through the Google Play Store, ensure the transaction is password protected:

- Navigate to Play Store > Menu > Settings > Require authentication for purchases > For all purchases through Google Play on this device

7. Manage the amount of personal information your apps can access

Many Google Play Store apps access your personal information. Consider not installing the ones that access your Device & App History, Device ID & Call Information Identity (profile data), Contacts, Wi-Fi Connections Information (including your Wi-Fi passwords), Bluetooth Connection Information and SMS Messages. To learn what information your apps can already access:

- Navigate to Settings > Apps > App Manager > Select an app > Permissions

As a general rule, be wary of free apps, as they are often a source of malware and/or viruses. It’s best to download apps only from a trusted source.

Strongly consider installing the app Lookout Security & Antivirus from the Google Play Store. It can help you monitor the information accessed and shared by your apps, as well as provide anti-virus protection.
SECURING YOUR ANDROID GOOGLE PIXEL AND PIXEL XL

**Limit your potential exposure**

1. **Lock your device**
   Enable a lock screen passcode to prevent unauthorized use of your device:
   - Navigate to **Settings > Security & location > Screen lock** > Enter passcode (if prompted) > **PIN** > Enter a 6-digit passcode and confirm
   Additionally, use Pixel Imprint if you prefer to unlock your Pixel with your fingerprint:
   - Navigate to **Settings > Security & location > Pixel Imprint** > Follow activation steps

2. **Limit information appearing on your lock screen**
   Android allows you to select the type of notification displayed on your locked Android device. “Hide sensitive notification content” will limit the information about the sender and message contents:
   - Navigate to **Settings > Apps & notifications > Notifications > On lock screen > Hide sensitive content**

3. **Disable tracking of your device**
   By default, Android tracks where you have taken your device. Disabling this feature will help protect you.
   Disable Google Location History:
   - Navigate to **Settings > Security & location > Location > Advanced > Google Location History** > Switch OFF: **Use Location History** > then select **Manage Timeline > Menu > Settings > Delete all Location History**
4. Limit data tracking on your device

Your browser may save information about you and the websites you visit, such as usernames, passwords and addresses. To opt for security over convenience, disable these features. For example:

- Navigate to Chrome > Menu > Settings > Autofill and payments > Switch OFF: Autofill forms
- Navigate to Chrome > Menu > Settings > Passwords > Switch OFF: Save passwords

5. Find your device if it’s misplaced, lost, or stolen

Find My Device allows you to locate the physical location of your device and also:
- Lock and reset device password
- Make device ring
- Remotely erase all data on your device

- Navigate to Settings > Google > Security > Find My Device > Switch ON: Find My Device

Find My Device can be accessed via a web browser at: https://www.android.com/find

6. Password protect app purchases

Before making a purchase through the Google Play Store, ensure the transaction is password protected:

- Navigate to Play Store > Menu > Settings > Require authentication for purchases > For all purchases through Google Play on this device

7. Manage the amount of personal information your apps can access

Many Google Play Store apps access your personal information. Consider not installing the ones that access your Device & App History, Device ID & Call Information Identity (profile data), Contacts, Wi-Fi Connections Information (including your Wi-Fi passwords), Bluetooth Connection Information and SMS Messages. To learn what information your apps can already access:

- Navigate to Settings > Apps & notifications > Select an app > Permissions

As a general rule, be wary of free apps, as they are often a source of malware and/or viruses. It’s best to download apps only from a trusted source.

Strongly consider installing the app Lookout Security & Antivirus from the Google Play Store. It can help you monitor the information accessed and shared by your apps, as well as provide anti-virus protection.
Limit your potential exposure

1. Lock your device
   Enable a lock screen passcode to prevent unauthorized use of your device:
   - Navigate to Settings > Security & location > Screen lock > Enter passcode (if prompted) > PIN > Enter a 6-digit passcode and confirm
   Additionally, if you prefer to unlock your Key2 LE with your fingerprint:
   - Navigate to Settings > Security & location > Fingerprint > Follow activation steps

2. Limit information appearing on your lock screen
   Android allows you to select the type of notification displayed on your locked Android device. “Hide sensitive notification content” will limit the information about the sender and message contents:
   - Navigate to Settings > Apps & notifications > Notifications > On lock screen > Hide sensitive notification content

3. Disable tracking of your device
   By default, Android tracks where you have taken your device. Disabling this feature will help protect you.
   Disable Google Location History:
   - Navigate to Settings > Google > Location > Google Location History > Switch OFF: Use Location History > then select Google Maps > Settings > Delete all Location History
4. Limit data tracking on your device
Your browser may save information about you and the websites you visit, such as usernames, passwords and addresses. To opt for security over convenience, disable these features. For example:
- Navigate to Chrome > Menu > Settings > Passwords > Switch OFF: Save passwords
- Navigate to Chrome > Menu > Settings > Payment methods > Switch OFF: Save and fill payment methods

5. Find your device if it’s misplaced, lost, or stolen
Find My Device allows you to locate the physical location of your device and also:
- Lock and reset device password
- Make device ring
- Remotely erase all data on your device
- Navigate to Settings > Google > Security > Find My Device > Switch ON: Find My Device
Find My Device can be accessed via a web browser at: https://www.android.com/find

6. Password protect app purchases
Before making a purchase through the Google Play Store, ensure the transaction is password protected:
- Navigate to Play Store > Menu > Settings > Require authentication for purchases > For all purchases through Google Play on this device

7. Manage the amount of personal information your apps can access
Many Google Play Store apps access your personal information. Consider not installing the ones that access your Device & App History, Device ID & Call Information Identity (profile data), Contacts, Wi-Fi Connections Information (including your Wi-Fi passwords), Bluetooth Connection Information and SMS Messages. To learn what information your apps can already access:
- Navigate to Settings > Apps & permissions > Select an app > Permissions
As a general rule, be wary of free apps, as they are often a source of malware and/or viruses. It’s best to download apps only from a trusted source. Strongly consider installing the app Lookout Security & Antivirus from the Google Play Store. It can help you monitor the information accessed and shared by your apps, as well as provide anti-virus protection.
Securing your email accounts*

Email is an integral tool used every day to communicate and interact online, and can be used as a user ID when signing into websites. Hackers can attempt to gain access to your accounts by attacking email providers or employing social engineering techniques and malware to target you. It is important to utilize your email provider’s security features and to take the appropriate steps if you believe your account has been compromised.

Email security best practices

• Maintain separate accounts for business and personal use, and don’t use them interchangeably

• Create passwords of at least 10 characters, using a mix of upper- and lower-case letters, numbers and special characters. Change your passwords three or four times a year

• Be alert to social engineering attempts — cyber criminals may use emails that contact links, malware or viruses to gain confidential information

• Safeguard your information — use an email encryption tool when transmitting sensitive information

• Create “disposable” email addresses for websites that require an email as a user ID

• When accessing email accounts, ensure software on devices are up-to-date and consider using a Virtual Private Network (VPN) when using public Wi-Fi

If you believe your account has been compromised, some best practices to mitigate the risk of future fraud occurring:

• Change your password on your various online accounts, using a different password for each account

• Enable two-factor authentication (two-step verification) wherever possible, including on your email, banking and shopping accounts

• Install anti-virus and anti-malware software, with auto-updates

• Ensure your operating system is up-to-date

• Contact your J.P. Morgan representative immediately

Instructions for popular email providers on:

• Enabling account security features
• Identifying account compromise
• Closing your account

Gmail ......................................................... page 3
Yahoo ....................................................... page 5
Hotmail/Outlook ................................. page 7
AOL ......................................................... page 9
iCloud Mail ............................................. page 11
In addition to the listed email security best practices above, consider the taking advantage of your provider’s specific account security features and tools.

Account security features

Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

- Navigate to myaccount.google.com and log in > Select Security > Select Password > Enter your new complex password and confirm it > Select Change Password

Enable 2-step verification
2-step verification is one of the strongest cybersecurity measures available and adds an extra layer of protection from cyber criminals. After you’ve enabled 2-step verification, you will enter your password and an additional security code upon logging in.

- Navigate to myaccount.google.com and log in > Select Security > In the “2-Step Verification” box, select Get started > Follow activation steps

Enable recovery contact information
In the event that you lose access to your email account, enabling recovery contact information can help expedite the account recovery process.

- Navigate to myaccount.google.com and log in > Select Security > Ensure the Recovery email and Recovery phone are up to date

Filter suspicious emails
If you receive a suspicious or unwanted email, reporting it to Gmail can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account’s spam filters.

Report spam:
- Select the message you’d like to report > in the toolbar above your emails, select the Spam button

Report phishing:
- Select the message you’d like to report > At the top right of the message next to the Reply button, select the icon > Select Report phishing

Assign an account trustee
Google offers a unique feature called Inactive Account Manager. Choose a family member or a close friend to take care of your account in case of an emergency or if something happens to you.

- Navigate to myaccount.google.com and log in > Select Data & personalization > Select Make a plan for your account > Select Start > Follow steps to set up

Security checkup
Reviewing and updating account security settings on a regular basis can ensure your account is better secured from hackers.

- Navigate to myaccount.google.com and log in > Under Security issues found, select Secure account > Follow steps

Privacy checkup
Privacy checkup helps you understand and control what information is saved and shared to your Google account.

- Navigate to myaccount.google.com and log in > Under the Take the Privacy Checkup section, select Get started > Follow steps
Tools to identify if your account has been compromised

Check email forwarding and filter settings
After compromising your account, hackers can modify email settings to forward, delete or even send emails on your behalf without your knowledge. Periodically check email forwarding and filter settings to verify that there have not been changes made to your account.

• Navigate to mail.google.com > In the top right, select ✉️ > Settings > Review each of the following sections
• Select the Accounts and Import tab
  – Ensure all email addresses in the “Send mail as” section belong to you
  – Ensure all email addresses in the “Check mail from other accounts” section belong to you
  – Check “Grant access to your account” section to ensure no unknown people have access to your account
• Select the Filters and Blocked Addresses tab
  – Make sure mail isn’t being automatically forwarded to an unknown account using a “Forward to” filter
  – Ensure there are no filters enabled that automatically delete messages (known as a “Delete it” filter

Review recent activity
Regularly review recent activity, including recently connected devices and account changes for suspicious activity.

• Navigate to myaccount.google.com and log in > Select Security > Review Recent security events for any suspicious activity

Account recovery
Hackers will often attempt to change your email account password during a compromise. If you find you can no longer sign in to your account, it may need to be recovered.

• Navigate to accounts.google.com/signin/recovery > Follow steps to begin recovering your account

Closing your account
In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings.

• Navigate to myaccount.google.com and log in > Select Data & personalization > Delete a service or your account > Choose whether you would like to delete just a service (e.g., Gmail) or your Google account and its data > Follow steps
SECURING YOUR YAHOO ACCOUNT

In addition to the listed email security best practices above, consider the taking advantage of your provider’s specific account security features and tools.

Account security features

**Strengthen your password**
A strong password is your front line of defense against unauthorized access to your accounts.

- Navigate to Your name > Account Info > Account security > Change Password > Enter and confirm your new password > Continue (a confirmation appears) > Continue to finish

**Two-step verification**
Two-step verification is one of the strongest cybersecurity measures available and adds an extra layer of protection from cyber criminals. After you’ve enabled two-step verification, you will enter your password and an additional security code upon logging in.

- Navigate to Your name > Account Info > Account security > Switch ON: Two-step Verification > Enter your mobile number > Send SMS to verify your mobile number via text message > Enter the verification code > Verify

**Enable recovery contact information**
In the event that you lose access to your email account, enabling recovery contact information can help expedite the account recovery process.

- Navigate to Your name > Account Info > Account security > Select Email addresses > Add recovery email address > Send verification email > Click the verification link in the email sent to your recovery email address > Verify

**Filter suspicious emails**
If you receive a suspicious or unwanted email, reporting it to Yahoo can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account’s spam filters.

Mark an email as spam:

- Select the checkbox next to the email(s) you’re reporting > Spam > Your selected email(s) will be sent to your Spam folder

**Disposable addresses**
If you don’t want to reveal your “real” email address, you can create disposable addresses. Each disposable address consists of a base name (common to all you create) and a keyword (up to 500). You can use disposable addresses for spam control, privacy, organization, or anonymity.

- Navigate to Settings > More Settings > Mailboxes > Disposable email address > Add (ensure you’re happy with your base name before you create it. You only get one per account and it is not possible to delete a base name once you’ve created it)

**Note:** Messages sent to your disposable addresses will be delivered right to your inbox or the folder you selected when you created the address.
Tools to identify if your account has been compromised

Review recent activity
Regularly review recent activity, including recently connected devices and account changes for suspicious activity.

• Navigate to Your name > Account Info > Recent Activity > Review location and device info for any suspicious activity

Closing your account
In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings.

• Navigate to Your name > Account Info > Help > Browse to Create or Delete Account > Select Close or Reactivate your Yahoo Account > Read the information under “Before continuing, please consider the following information” > Continue to delete your Yahoo account
In addition to the listed email security best practices above, consider the taking advantage of your provider’s specific account security features and tools.

**Account security features**

**Strengthen your password**
A strong password is your front line of defense against unauthorized access to your accounts.

- Navigate to Profile > View Account > Security > Update > Password security > Enter your new complex password and confirm it > Select Change Password

**Enable two-step verification**
Two-step verification is one of the strongest cybersecurity measures available and adds an extra layer of protection from cyber criminals. After you’ve enabled two-step verification, you will enter your password and an additional security code upon logging in.

- Navigate to Profile > View Account > Security > More Security Options > Two-step verification > Follow activation steps

You will be prompted to set up an authenticator app if you have a smartphone. (With an authenticator app, you can get security codes even if your phone isn’t connected to a cellular network). You can also create app passwords for apps and devices (such as Xbox 360, Windows Phone 8), that do not support two-step verification codes.

**Enable recovery contact information**
In the event that you lose access to your email account, enabling a recovery email address and phone number can help expedite the account recovery process.

- Navigate to Profile > View Account > Security > Security contact info > Ensure the recovery email and recovery phone number are up to date

**Filter suspicious emails and junk mail**
If you receive a suspicious or unwanted email, reporting it to Hotmail/Outlook can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account’s spam filters. Hotmail/Outlook allows you to report an email as Junk, Phishing Scam, or inform the provider that a friend’s email has been hacked. Hotmail/Outlook uses this to help prevent further unwanted emails from coming in.

- Navigate to the Inbox or Junk folder > Select Junk drop-down > Select the appropriate reporting option

Applying filters can help you reduce and avoid junk mail, and set up safe and blocked senders.

- Navigate to Settings > Mail > Junk Mail > Blocked senders and domains, Safe senders and domains, Safe mailing lists and Filters

**Alias addresses**
You can use your Hotmail/Outlook account to set up alias addresses from which you can send and receive email using the same inbox, contact list and account settings as the primary account. You can sign into your account with any alias, using the same password for all.

These aliases can help to also keep your identity protected and mitigate your cyber risk. Sign-in preferences allow you to choose which aliases can sign into your account.

To make it more difficult for someone to break into your account, turn off sign-in preferences for any email address, phone number or a Skype name you do not use.

- Navigate to Settings > Mail > Connected accounts

**Email recovery code**
In the event that your account becomes compromised by a cyber adversary, you can utilize a recovery code if you lose access to your security info. You need to print out your recovery code and keep it in a safe place in case of such an emergency.

Navigate to Profile > View Account > Security > More Security Options > Recovery Code
Tools to identify if your account has been compromised

Check email forwarding and filter settings
After compromising your account, hackers can modify email settings to forward, delete or even send emails on your behalf without your knowledge. Periodically check email forwarding and filter settings to verify that there have not been changes made to your account.

- Navigate to Settings > Mail > Verify details in each section
  - Automatic processing > Automatic replies
  - Accounts > Connected accounts and Forwarding

Additionally, monitor your Contacts for added or deleted contacts, and your Sent and Deleted mail folders for sent or deleted emails.

Review recent activity
Regularly review recent activity, including recently connected devices and account changes for suspicious activity.

Hotmail/Outlook allows you to review which devices are connected to your account and where they are located. If you do not recognize a device, its access should be removed immediately.

- Navigate to Profile > View Account > Security > See my recent activity

Email account recovery
Hackers will often attempt to change your email account password during a compromise. If you find you can no longer sign in to your account, it may need to be recovered. Use your recovery code, which you set up to recover your account.

Closing your account
In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings. Please note: an email account and the data and emails contained therein can not be reactivated.

- Navigate to Profile > View Account > Security > More Security Options > Close Your Account
SECURING YOUR AOL ACCOUNT

In addition to the listed email security best practices above, consider the taking advantage of your provider’s specific account security features and tools.

Account security features

Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

• Navigate to login.aol.com/security > Change password > Enter a new secure password > Continue

Enable two-step verification
Two-step verification is one of the strongest cyber-security measures available and adds an extra layer of protection from cyber criminals. After you’ve enabled two-step verification, you will enter your password and an additional security code upon logging in.

• Navigate to login.aol.com/security > Turn ON: Two-step verification > Follow activation steps

If you access your AOL account using any non-AOL apps or other programs (e.g. Outlook, mobile Mail apps), create application specific passwords. If you have two-step verification turned on and do not have application-specific passwords for your apps, you will receive an error that the apps cannot connect:

• After setting up two-step verification, click Generate app password > Follow activation steps

Note: Record your Disable code provided during setup for future use in case you lose or cannot access your phone

Enable recovery contact information
In the event that you lose access to your email account, enabling recovery contact information can help expedite the account recovery process. To change the contact information already provided during account set-up:

• Navigate to login.aol.com/security > Add alternate email address and mobile phone number > Follow activation steps

Filter suspicious emails
If you receive a suspicious or unwanted email, reporting it to AOL can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account’s spam filters.

• Click on the box to the left of the message > Click on Report Spam button in the toolbar above your emails

• Forward suspicious emails to aol_phish@abuse.aol.com

Premium security features
AOL provides premium security features through voluntary, subscription services. For additional information, consult the MyBenefits page:

• When logged in, select Settings > Premium Security > Select the security features you would like to turn on/off
Securing your email accounts: AOL

Tools to identify if your account has been compromised

Check email forwarding and filter settings
After compromising your account, hackers can modify email settings to forward, delete or even send emails on your behalf without your knowledge. Periodically check email forwarding and filter settings to verify that there have not been changes made to your account.

- Navigate to Options in the upper-right corner > Mail Settings > Filter Settings > Ensure only filters you created are enabled

Review recent activity
Regularly review recent activity, including recently connected devices and account changes for suspicious activity.

- Navigate to login.aol.com/account/activity > Review recent changes for suspicious activity

Closing your account
In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings.

- Navigate to myaccount.aol.com > My Services > Subscriptions > Manage > Cancel

Note: AOL automatically disables accounts that are inactive for 90 days.
CYBER SAFETY  Securing your email accounts: iCloud Mail

SECURING YOUR iCLOUD MAIL ACCOUNT

In addition to the listed email security best practices above, consider the taking advantage of your provider’s specific account security features and tools.

Account security features

Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

- Navigate to appleid.apple.com and log in > Select Change Password... > Enter your current password then your new complex password and confirm it > Select Change Password...

Enable 2-step verification
2-step verification is one of the strongest cybersecurity measures available and adds an extra layer of protection from cyber criminals. After you’ve enabled 2-step verification, you will enter your password and an additional security code upon logging in. iCloud requires 2-step verification to be activated via an iOS or MacOS device.

- iOS: Settings > Select your name > Password & Security > Select Turn On Two-Factor Authentication > Follow activation steps
- MacOS: Apple menu > System Preferences > iCloud > Account Details > Security > Turn On Two-Factor Authentication > Follow activation steps

Enable recovery contact information
In the event that you lose access to your email account, enabling recovery contact information can help expedite the account recovery process.

- Navigate to appleid.apple.com and log in > Select Edit in the Security section > Ensure the Trusted Phone Numbers and Notification Email fields are up to date

Filter suspicious emails
If you receive a suspicious or unwanted email, reporting it to Apple can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account’s spam filters.

Report spam:
- Select the message you’d like to report > Select the Flag 🚭 > Select Move to Junk

Tools to identify if your account has been compromised

Check email forwarding and filter settings
After compromising your account, hackers can modify email settings to forward, delete or even send emails on your behalf without your knowledge. Periodically check email forwarding and filter settings to verify that there have not been changes made to your account.

- Navigate to icloud.com/mail > In the bottom left, select Settings 🎉 > Rules...
  - Ensure messages aren’t being forwarded to an unknown account and are not being deleted after forwarding

Account recovery
Hackers will often attempt to change your email account password during a compromise. If you find you can no longer sign in to your account, it may need to be recovered.

- Navigate to appleid.apple.com > Select Forgot Apple ID or password? > Follow steps to begin recovering your account
Closing your account

In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings.

- Navigate to appleid.apple.com and log in > Select Manage Your Data and Privacy and log in > Request to delete your account > Follow steps
Securing your social media accounts*

You might be sharing more information about your friends, family and contacts on your social media accounts than you realize. This information could be used by fraudsters as part of social engineering efforts. Here are some easy steps to help keep your information more secure across popular social media platforms.

Social media safety guidelines

- Limit the amount of personal information you publish on social media (such as a pet’s name, school and children’s names), as key profile information can be answers to vetting questions used for authentication
- Report any suspicious activity or spam to the social media site the contact came from. Spam can come in the form of a post, message, email or friend request
- Change your password and report the suspicious activity immediately if you think someone has accessed your account
- If you believe you are being impersonated or targeted on any social media platform, immediately report it to the site(s) on which it is occurring. Facebook, LinkedIn, Twitter, Snapchat and Instagram provide specific instructions on how to do so

Instructions for popular social media sites on:

- Privacy issues
- Strengthening your passwords
- Two-step authentication and login verification

Facebook ............................................. page 3
LinkedIn ............................................. page 5
Twitter ............................................. page 6
Snapchat ............................................ page 7
Instagram .......................................... page 8
1. Privacy

Limit who can view your activity and personal information on Facebook. Modifying your privacy settings should ensure your information is only seen by those you want.

Facebook offers a feature called Privacy Checkup, which allows you to easily review your privacy settings and modify them to match your level of risk comfort.

- **iOS and Android:** Navigate to Menu > Settings & Privacy > Settings > Privacy Settings > Check a few important settings > Modify each section to your level of risk comfort
- **Desktop:** Navigate to the Help Center > Privacy Checkup > Modify each section to your level of risk comfort

Suggestion: Avoid choosing Public when possible when possible

Further limit who can view your posts and information. Modifying your privacy settings should ensure your information is only seen by those you want.

- **iOS and Android:** Navigate to Menu > Settings & Privacy > Settings > Privacy Settings > Modify each section to your level of risk comfort
- **Desktop:** Navigate to the Help Center > Privacy Setting > Modify each section to your level of risk comfort

Suggestion: Avoid choosing Public when possible

More granularly limit who can see what you have posted or what others have posted to your timeline.

- **iOS and Android:** Navigate to Menu > Settings & Privacy > Settings > Timeline and Tagging > Modify each section to limit who can view your Timeline or tag you in photos or posts to your level of risk comfort, and avoid choosing Public where applicable
- **Desktop:** Navigate to the Menu > Settings > Timeline and Tagging > Modify each Timeline permission to your level of risk comfort, and avoid choosing Everyone where applicable

Control the information being shared with authorized third-party applications.

- **iOS and Android:** Navigate to Menu > Settings & Privacy > Settings > Apps and Websites > Modify each section to your level of risk comfort
- **Desktop:** Navigate to the Menu > Settings > Apps and Websites > Modify each section to your level of risk comfort

Note: Completely turning off Apps, Websites and Games may affect your access to websites where you use Facebook to log in.
1. **Privacy (continued)**

Facebook offers a service called *Legacy Contact*. Choose a family member or close friend to take care of your account in case of an emergency or if something happens to you.

- **iOS and Android**: Navigate to `Menu > Settings & Privacy > Settings > Personal Information > Manage Account > Legacy Contact > Set up trusted contact and preferences`
- **Desktop**: Navigate to the `Menu ▼ > Settings > General > Edit` next to Memorialization Settings > Set up trusted contact and preferences

2. **Strengthen your password**

A strong password is your front line of defense against unauthorized access to your accounts.

- **iOS and Android**: Navigate to `Menu ▼ > Settings & Privacy > Settings > Security and Login > Change password` > Enter your current password, then enter your new secure password and confirm > **Save Changes**
- **Desktop**: Navigate to the `Menu ▼ > Settings > Security and Login > Edit` next to Change password > Enter your current password, then your new secure password and confirm > **Save Changes**

3. **Two-factor authentication**

To ensure an unauthorized person is not attempting to access your account, Facebook can provide you with a security code when you access your account from a new device.

- **iOS and Android**: Navigate to `Menu ▼ > Settings & Privacy > Settings > Security and Login > Use two-factor authentication` > Switch ON: Two-factor authentication > Follow activation steps
- **Desktop**: Navigate to the `Menu ▼ > Settings > Security and Login` > Click `Edit` next to Use two-factor authentication > Follow activation steps

4. **Login alerts**

Facebook can send notifications, emails or text messages when your account is accessed from a new computer or device.

- **iOS and Android**: Navigate to `Menu ▼ > Settings & Privacy > Settings > Security and Login > Get alerts about unrecognized logins` > Choose where you would like to receive alerts
- **Desktop**: Navigate to the `Menu ▼ > Settings > Security and Login > Edit` next to Get alerts about unrecognized logins > Choose where you would like to receive alerts
SECURING YOUR LINKEDIN ACCOUNT

1. **Privacy**
   Limit who can view your posts and personal information on LinkedIn. Modifying your privacy settings should ensure your information is only seen by those you want.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Privacy > Modify each setting to your level of risk comfort
   - **Desktop:** Navigate to Me > Settings & Privacy > Privacy > Modify each setting to your level of risk comfort

   Pay special attention to:
   - Who can see your connections
     *Suggestion: Only you*
   - Who can contact you via LinkedIn. Modifying your communication settings will limit who can send you invites and messages.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Communications > Modify each setting based on your level of risk comfort
   - **Desktop:** Navigate to Me > View Profile > Settings & Privacy > Communications > Modify each setting based on your level of risk comfort

2. **Strengthen your password**
   A strong password is your front line of defense against unauthorized access to your accounts.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Account > Permitted services > Modify access for each application to your level of risk comfort
   - **Desktop:** Navigate to Me > Account > Partners and services > Modify access for each application to your level of risk comfort

3. **Two-step verification**
   To ensure an unauthorized person is not attempting to access your account, LinkedIn can provide you with a security code when you access your account from a new device.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Privacy > Two-step verification > Set up > Follow activation steps
   - **Desktop:** Navigate to Me > Settings & Privacy > Account > Login and security > Turn on Two-step verification > Follow activation steps

   Control the information being shared with authorized third-party applications.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Account > Permitted services > Modify access for each application to your level of risk comfort
   - **Desktop:** Navigate to Me > Account > Partners and services > Modify access for each application to your level of risk comfort

   2. **Strengthen your password**
      A strong password is your front line of defense against unauthorized access to your accounts.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Account > Change password > Enter your current password, then your new secure password and confirm > Save
   - **Desktop:** Navigate to Me > Settings & Privacy > Account > Login and security > Change password > Enter your current password, then your new secure password and confirm > Save

   3. **Two-step verification**
      To ensure an unauthorized person is not attempting to access your account, LinkedIn can provide you with a security code when you access your account from a new device.

   - **iOS and Android:** Navigate to Me > View Profile > Settings > Privacy > Two-step verification > Set up > Follow activation steps
   - **Desktop:** Navigate to Me > Settings & Privacy > Account > Login and security > Turn on Two-step verification > Follow activation steps

   Control the information being shared with authorized third-party applications.
SECU RIN G YO U R TWI T T ER ACCO U NT

1. Privacy
Limit who can view your tweets and personal information on Twitter. Modifying your privacy settings should ensure your information is only seen by those you want.

- iOS: Navigate to Picture dropdown > Settings and privacy > Privacy and safety > Switch ON: Protect your Tweets
- Android: Navigate to the Picture dropdown > Settings and privacy > Privacy and safety > Switch ON: Protect your Tweets
- Desktop: Navigate to the Picture dropdown > Settings and privacy > Privacy and safety > Switch ON: Protect my Tweets > Save changes

Control the information being shared with authorized third-party applications.

- Desktop only: Navigate to the Picture dropdown > Settings and privacy > Apps and devices > Modify access for each application to your level of risk comfort

2. Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

- iOS: Navigate to Picture dropdown > Settings and privacy > Account > Change password > Enter your current password, then your new secure password and confirm
- Android: Navigate to the Picture dropdown > Settings and privacy > Account > Password > Enter your current password, then your new secure password and confirm
- Desktop: Navigate to the Picture dropdown > Settings and privacy > Password > Enter your current password, then your new secure password and confirm > Save changes

3. Login verification
To ensure an unauthorized person is not attempting to access your account, Twitter can provide you with a security code when you access your account from a new device.

- iOS: Navigate to Picture dropdown > Settings and privacy > Account > Security > Switch ON: Login verification > Confirm > Follow activation steps
- Android: Navigate to the Picture dropdown > Settings and privacy > Account > Security > Switch ON: Login Verification > Follow activation steps
- Desktop: Navigate to the Picture dropdown > Settings and privacy > Account > Set up login verification > Follow activation steps
SECURING YOUR SNAPCHAT ACCOUNT

1. Privacy
Limit who can add you and view your snaps on My Story. Modifying your privacy settings should ensure your information is only seen by those you want.

- **iOS and Android:** Navigate to the Picture dropdown ✝ > Settings ✝ > Scroll down to Who Can... > Modify each setting based on your level of risk comfort

  Pay special attention to:
  - Contact Me
    Suggestion: My Friends
  - View My Story
    Suggestion: My Friends or Custom
  - See Me in Quick Add
    Suggestion: Switch OFF: Show me in Quick Add
  - See My Location
    Suggestion: Switch ON: Ghost Mode

2. Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

- **iOS and Android:** Navigate to the Picture dropdown ✝ > Settings ✝ > Password > Enter your current password, then your new secure password > Save

- **Desktop:** Log into your account on accounts.snapchat.com > Navigate to Change my password > Enter your current password, then your new secure password > Change password

3. Two-factor authentication
To ensure an unauthorized person is not attempting to access your account, Snapchat can provide you with a security code when you access your account from a new device.

- **iOS:** Navigate to the Picture dropdown ✝ > Settings ✝ > Two-Factor Authentication > Continue > SMS > Follow activation steps

- **Android:** Navigate to the Picture dropdown ✝ > Settings ✝ > Two-Factor Authentication > Continue > SMS > Follow activation steps
1. Privacy
Limit who can view your posts and Your Story. Modifying your privacy settings should ensure your information is only seen by those you want.

- **iOS and Android:** Navigate to Your profile > Menu > Settings > Privacy > Account Privacy > Switch ON: Private Account
- **Desktop:** Navigate to Your profile > Edit Profile > Privacy and Security > Switch ON: Private Account

Control the information being shared with authorized third-party applications.

- **Desktop only:** Navigate to Your profile > Edit Profile > Authorized Applications > Modify access for each application to your level of risk comfort

2. Strengthen your password
A strong password is your front line of defense against unauthorized access to your accounts.

- **iOS and Android:** Navigate to Your profile > Menu > Settings > Security > Password > Enter your current password, then your new secure password > Save
- **Desktop:** Navigate to Your profile > Edit Profile > Change Password > Enter your current password, then your new secure password > Change password

3. Two-factor authentication
To ensure an unauthorized person is not attempting to access your account, Instagram can provide you with a security code when you access your account from a new device.

- **iOS and Android:** Navigate to Your profile > Menu > Settings > Security > Two-Factor Authentication > Get Started > Follow activation steps
- **Desktop:** Navigate to Your profile > Edit Profile > Privacy and Security > Enable Two-Factor Authentication > Switch ON: Require Security Code > Follow activation steps
Securing your credit*

In the United States, your identity and credit history can be used to secure loans and insurance policies, gain employment and open credit cards. With so much at stake, it is essential to protect your credit, beginning with your credit report. Each of the U.S. credit bureaus provides tools to help minimize the risk of your credit report being used by unauthorized parties and avoid new accounts being opened in your name.

Review your credit report

Reviewing your credit report is the single best way to spot signs of identity theft, such as errors, suspicious activity and accounts or addresses you don't recognize. The three U.S. credit bureaus are required to provide one free credit report per year upon request. Any suspicious or fraudulent credit listing should be reported to the credit bureau that is showing the activity.

The three nationwide credit bureaus have set up a central website and telephone number where you can order your free annual reports:

877.322.8228    www.annualcreditreport.com

Implement a credit freeze

A credit freeze, also known as a security freeze, restricts access to your credit report, making it more difficult for identity thieves to open accounts in your name and/or abuse your credit. A credit freeze prevents a person, merchant or institution from making an inquiry about your credit report unless you temporarily lift or remove the freeze. Your credit report will continue to be accessible to your existing creditors or to debt collectors acting on their behalf. Note: A credit freeze will not impact your credit score.

Putting a credit freeze in place must be done separately with each of the three U.S. credit bureaus.

Lift a credit freeze

A credit freeze remains in place until you direct the credit bureau to either temporarily lift it or remove it entirely. For example, you can temporarily lift the credit freeze when you are applying for credit or employment.

If possible, find out which credit bureau a merchant or prospective employer plans to use for its inquiry, and lift the freeze at that particular bureau using the pin code provided.

Protecting a family member’s credit

Fraudsters can potentially misuse a minor’s social security number or other personally identifying information for years without notice. To help protect a minor from being a financial target, ensure the same credit freeze precautions are implemented. While most minors do not have an existing credit file, it is wise to proactively secure their credit and identity by working with the credit agencies to protect them.

Contact each credit bureau to institute a freeze on the credit of minors. Refer to the “Child Identity Theft” page on the Federal Trade Commission’s Consumer Information site for more information (www.consumer.ftc.gov).

Additionally, the same precautionary measures should be considered for elderly and vulnerable family members as they can be especially susceptible to fraud.

In the United States, contact each of the three credit bureaus if you wish to put a freeze in place or lift a freeze:

Equifax
800.349.9960
www.freeze.equifax.com

Experian
888.397.3742
www.experian.com/冻

TransUnion
888.909.8872
www.transunion.com/freeze
Place a fraud alert

Placing a fraud alert on your credit file allows creditors to obtain a copy of your credit report—but they must take certain steps to verify your identity.

Fraud alerts may be effective at stopping someone from opening new credit accounts in your name; however, they may not prevent the misuse of your existing accounts. Fraud alerts do not freeze your credit, and they allow your credit score to change even as they mitigate the risk of unauthorized use. Please note: You only need to contact one credit bureau to have a fraud alert put in place, as that bureau is required to share the alert with the other two bureaus.

Three types of fraud alerts are available:

- **Initial Fraud Alert:** Principally designed for, but not reserved to, individuals who feel their identity has been compromised. Initial Fraud Alerts last one year from the date issued, are free of charge and can be continuously renewed.

- **Extended Fraud Alert:** Reserved exclusively for victims of identity theft and designed to protect your credit for seven years.

- **Active Duty Military Alert:** Reserved for military personnel who want to protect their credit during deployment. Alerts last for one year and can be renewed.

In the United States, contact one of the three credit bureaus if you wish to place a fraud alert:

<table>
<thead>
<tr>
<th>Bureau</th>
<th>Phone Number</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equifax</td>
<td>888.766.0008</td>
<td><a href="http://www.equifax.com/CreditReportAssistance">www.equifax.com/CreditReportAssistance</a></td>
</tr>
<tr>
<td>Experian</td>
<td>888.397.3742</td>
<td><a href="http://www.experian.com/fraudalert">www.experian.com/fraudalert</a></td>
</tr>
<tr>
<td>TransUnion</td>
<td>800.680.7289</td>
<td><a href="http://www.transunion.com/fraud">www.transunion.com/fraud</a></td>
</tr>
</tbody>
</table>