

Cyber Safety

Protect yourself and your personal information

10 KEY CYBER SAFETY TIPS

- 1 Never click on a link in an email until you validate the source
- 2 Never enter personal information in an email or text message
- 3 Use antivirus software and keep it up to date
- 4 Limit web usage in the office to core, business-related sites
- 5 Make minimal use of unsecured, public networks
- 6 Create strong passwords and change them every 2-3 months
- 7 Do not use the same password for multiple accounts
- 8 Create separate email accounts for work, personal use, alert notifications and other interests
- 9 At home, set up a primary network and another for guests
- 10 Be prudent in what you share about yourself and your job via social media

Put these safeguards in place as soon as possible—if you haven't already.

passwords

- Create passwords that are at least 10-14 characters; use a mix of numbers, upper- and lowercase letters and symbols
- Change passwords three to four times a year
- Store in a safe place or utilize a password management tool
- Do not use the same password for multiple accounts
- Do not create common passwords
- Do not select "remember my password" on websites you visit

email

- Create separate email accounts for work, personal use, alert notifications and other interests
- Turn on two-factor authentication whenever an ecommerce site offers it
- Encrypt important files before emailing them
- Use spam filtering to stop unwanted email from reaching your in-box
- Do not open emails from unknown senders
- Do not reply to requests for financial/personal info

virus and malware protection

- Keep software/browser/systems up to date
- Install antivirus software and keep it up to date
- Turn on firewall to highest level
- Regularly back up your data
- Do not install or use pirated software
- Do not install P2P file-sharing programs
- Do not set email to auto-open attachments

internet usage

- Download software only from trusted sources
- Log out of sites instead of simply closing the window
- Look for https:// for secure session validation
- Do not click on links from unknown/untrustworthy sources
- Do not allow ecommerce sites to store your credit card information
- Do not click on pop-up windows to close them; instead use the "X" in the upper right hand corner of the screen

mobile

- Keep screen lock on; choose strong passwords
- 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
- Do not click on ads when surfing the internet

public Wi-Fi/hot spots

- Disable ad hoc networking
- Turn off auto connect to non-preferred networks
- Turn off file sharing
- Consider using your phone's mobile network instead
- Do not use/avoid public Wi-Fi
- Do not use public Wi-Fi to enter personal credentials; your keystrokes can be captured by hackers

home networks

- Create one network for you, another for guests
- Change your router's name and password
- Change the password to your wireless network
- Turn on your router's WPA2 encryption and firewall
- Do not use default user names/passwords
- Do not broadcast your home network

social engineering

- Telephone the person who sent the email to confirm its authenticity if you suspect it may be fraudulent
- Limit the amount of personal information you give out
- Use privacy settings online wherever possible
- Do not respond to requests for personal or financial information in an email
- Do not open an attachment from someone you know if you are not expecting it; call to confirm before clicking
- Do not assume that every email you receive is authentic

Cyber Safety

Choosing services, software and equipment

email providers

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.

FEATURES TO LOOK FOR

Authentication

A high-quality email service will provide secure authentication to prevent spam and spoofing.

Virus scanning

Email is scanned for malicious content by the provider.

Look for a provider that offers enough storage, good IMAP and POP sync options for your mobile device and an intuitive interface.

Anti-spam

Reputable email service providers filter spam messages from your in-box.

Phishing protection

Some service providers will identify potential phishing emails.

password protection

Weaknesses stem from how users 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.

FEATURES TO LOOK FOR

Synchronization

A good password manager will allow access from anywhere and synchronize across devices.

Password generator

Automatically generates strong, complex passwords.

Look for a password management tool that supports the types of browsers, operating systems and mobile devices you use.

Encryption

Passwords are stored encrypted, and the master password is not retrievable.

Multi-factor support

Better management tools will support complex multi-factor passwords.

virus and malware protection

If you use a computer for web surfing, shopping, banking, email and instant messaging and do not have proper protection, you are at high risk of being victimized.

Running real-time antivirus products and keeping them up to date is an essential step to reduce risks from malware and can reduce infection by more than 80%.

FEATURES TO LOOK FOR

Detection

High-quality software detects 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 installed on per license subscription purchase.

Performance

Good antivirus software will not slow down your system.

Parental controls

Optional feature that will secure your systems when used by children.

Backups

Many applications provide optional back-up protection in case of system failure.

wireless routers

A wireless router allows you to connect devices to the internet and communicate with other devices on your network.

Routers are computers, with their own operating systems, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log keystrokes and access your accounts.

FEATURES TO LOOK FOR

Distributed Denial of Service (DDoS) protection

Prevents high-volume malicious attacks to your home network.

Firewall

Secures your network from intrusion.

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.

Guest network

Allows for separate network and credentials for temporary access.

JPMorgan Distribution Services, Inc., member FINRA / SIPC.

J.P. Morgan Asset Management is the marketing name for the asset management business of JPMorgan Chase & Co., and its affiliates worldwide.

© JPMorgan Chase & Co., June 2015

SA-CYBSEC

CYBER SAFETY

Securing your iPhone and iPad*

Operating System: iOS 10

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.

Limit your potential exposure

1. Lock your device

Enable a passcode to prevent unauthorized use of your device:

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

Or, use **Touch ID Security** 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

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

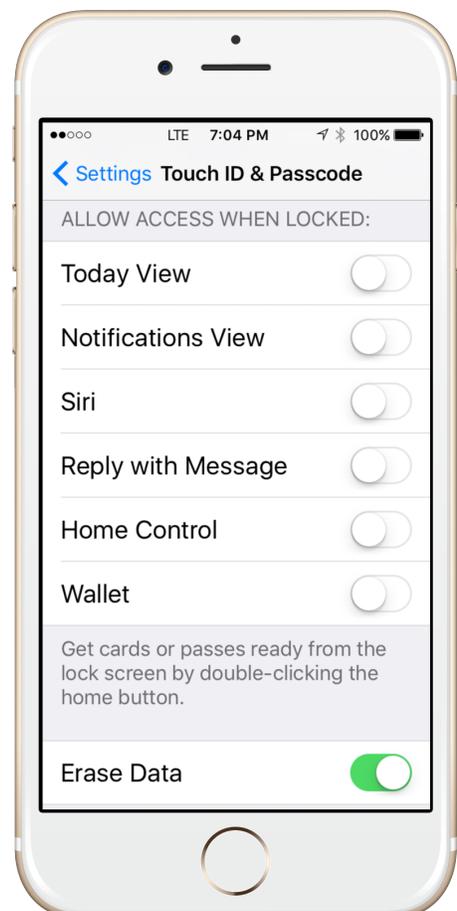
- Navigate to **Settings > Touch ID & Passcode > Enter Passcode > Allow Access When Locked** > Switch OFF: **Today View, Notifications View, Siri, Reply with Message, Home Control** and **Wallet**

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 > Frequent Locations > Clear History > Switch OFF: Frequent Locations**

5. Limit data and location tracking

Maps and weather

Some applications, such as these, 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, Names and Passwords 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 > iCloud > Find My iPhone (or iPad) > Switch ON: Find My iPhone**

Strongly consider installing *Lookout Security, Backup and Missing Device* 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 > General > Restrictions > Password Settings > Switch ON: Always Require and Require Password**

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Apple, Inc., Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your Android BlackBerry Priv*

Operating System: Android 6 Marshmallow

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.

Limit your potential exposure

1. Lock your device

Enable a lock screen password to prevent unauthorized use of your device:

- Navigate to **Settings** ⚙️ > **Security** > **Screen lock** > Enter password (if prompted) > **Password** > [Enter your new secure password and confirm]

Set your device to lock itself when it's not in use:

- Navigate to **Settings** > **Security** > Switch ON: **Power button instantly locks** > Then select **Automatically lock** > **Immediately**

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 sending and message contents:

- Navigate to **Settings** ⚙️ > **Sound & notification** > **When device is locked** > **Hide Sensitive Notification Content**

3. Disable tracking of your device

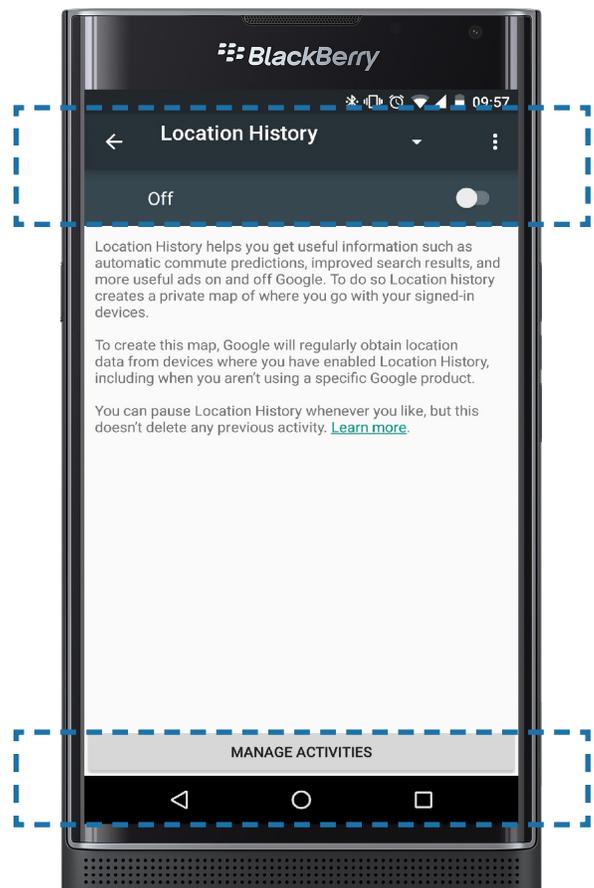
By default, Android tracks where you have taken your device. Disabling this feature will help protect you. Disable Google Location History:

- Navigate to **Settings** ⚙️ > **Location** > **Google Location History** > Switch OFF > Then select **Manage Activities** > **Menu** ⋮ > **Settings** > **Delete all Location History**

4. 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** ⚙️ > **Security** > Switch ON: **Automatically wipe device after 10 failed unlock attempts**



5. 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 > Switch OFF: Autofill forms and Save passwords**

6. 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 > Switch ON: Remotely locate this device and Allow remote lock and erase**

Android Device Manager can be accessed via a web browser at:

<https://www.google.com/android/devicemanager>

7. Password protect app purchases

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

- Navigate to **Play Store > Menu ☰ [on left side of screen] > Settings ⚙ > Require authentication for purchases > Select For all purchases through Google Play on this device**

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

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

Many Google Play Store apps can access your personal information. Consider not installing the one 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 > Select an app > Scroll down to 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 *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 antivirus protection.

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by BlackBerry Ltd., Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your Android HTC One M8 and M9*

Operating System: Android 5.0 Lollipop

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.

Limit your potential exposure

1. Lock your device

Enable a lock screen password to prevent unauthorized use of your device:

- Navigate to **Settings** ⚙️ > **Security** > **Screen lock** > Enter password (if prompted) > Select **Password** > Create a new alphanumeric password using a combination of letters, numbers and special characters

Set your device to lock itself when it's not in use:

- Navigate to **Settings** ⚙️ > **Security** > **Lock phone after** > **Immediately**

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:

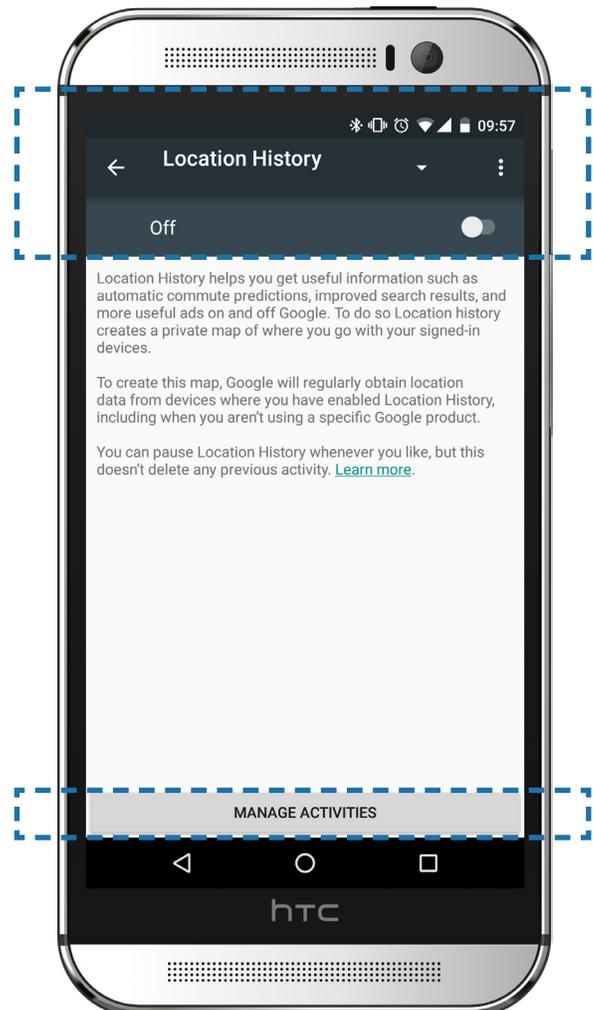
- Navigate to **Settings** ⚙️ > **Sound and notification** > **When device is locked** > and select **Hide sensitive notification content**

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** ⚙️ > **Location** > **Google Location History** > Switch OFF > Then select **Manage Activities** > **Menu** ☰ > **Settings** > **Delete all Location History** > and switch OFF



4. Limit data tracking on your device

Chrome can save information about you for websites you visit, such as usernames, passwords, and address. To secure sensitive information, disable this feature:

- Navigate to **Chrome > Menu ☰** > Switch OFF: **Autofill forms** and **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 **Apps > Google Settings > Security >** Switch ON: **Remotely locate this device** and **Allow remote lock and erase**

Android Device Manager can be accessed via a web browser at: <https://www.google.com/android/devicemanager>

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 ☰** [on left side of screen] > **Settings ⚙** > **Require authentication for purchases** > Select **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 can 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 ⚙** > **App Manager** > Select an app > Scroll down to **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 *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 antivirus protection.

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by HTC Corporation, Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your iPhone and iPad*

Operating System: iOS 10

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.

Limit your potential exposure

1. Lock your device

Enable a passcode to prevent unauthorized use of your device:

- Navigate to **Settings > Touch ID & Passcode > Turn Passcode ON** and enter a 6-digit passcode

Or, use **Touch ID Security** 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

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

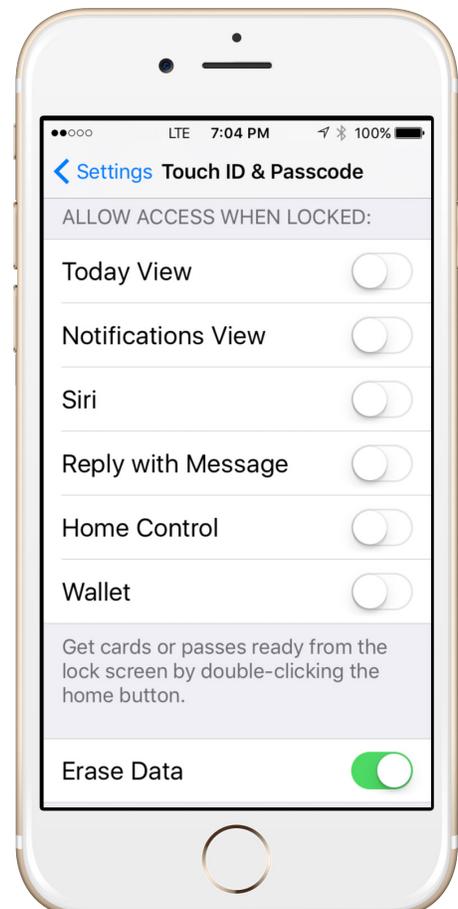
- Navigate to **Settings > Touch ID & Passcode > Enter Passcode > Allow Access When Locked > Switch OFF: Today View, Notifications View, Siri, Reply with Message, Home Control and Wallet**

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 > Frequent Locations > Clear History > Switch OFF: Frequent Locations**

5. Limit data and location tracking

Maps and weather

Some applications, such as these, 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, Names and Passwords 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 > iCloud > Find My iPhone (or iPad) > Switch ON: Find My iPhone**

Strongly consider installing *Lookout Security, Backup and Missing Device* 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 > General > Restrictions > Password Settings > Switch ON: Always Require and Require Password**

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Apple, Inc., Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your Android Samsung S6 and S6 Edge*

Operating System: Android 6 Marshmallow

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.

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) > **Password** > [Enter your new secure password 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**

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:

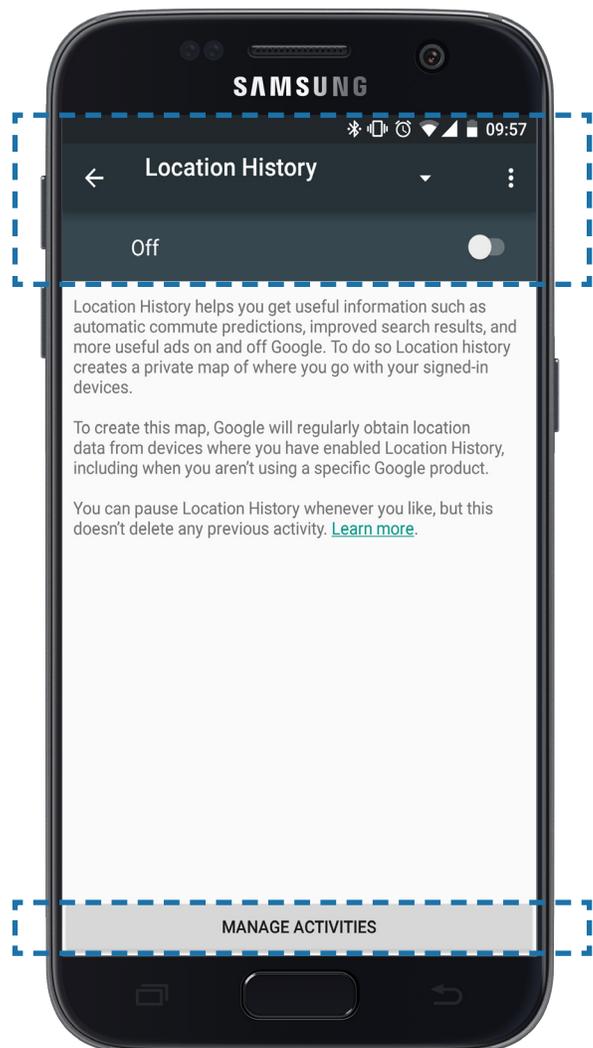
- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Notifications on lock screen** > **Hide Content**

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** ⚙️ > **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:

- For example, navigate to **Chrome > Menu ☰ > Settings > Switch OFF: Autofill forms and 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 > Switch ON: Remotely locate this device and Allow remote lock and erase**

Android Device Manager can be accessed via a web browser at: <https://www.google.com/android/devicemanager>

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 ☰ [on left side of screen] > Settings ⚙ > Require authentication for purchases > Select 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 ⚙ > Applications > Application Manager > Select an app > Scroll down to 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 *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 antivirus protection.

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Samsung Electronics Co., Ltd., Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your Android Samsung S6 Edge+*

Operating System: Android 6 Marshmallow

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.

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) > **Password** > [Enter your new secure password 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**

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:

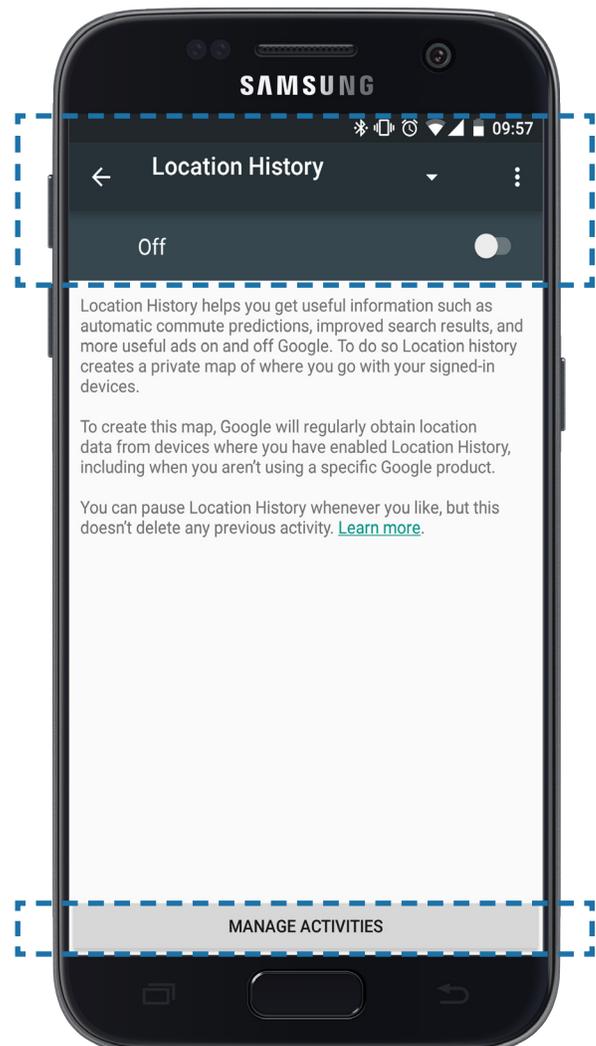
- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Notifications on lock screen** > **Hide Content**

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** ⚙️ > **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:

- For example, navigate to **Chrome** > **Menu** ☰ > **Settings** > Switch OFF: **Autofill forms** and **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** > Switch ON: **Remotely locate this device** and **Allow remote lock and erase**

Android Device Manager can be accessed via a web browser at: <https://www.google.com/android/devicemanager>

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** ☰ [on left side of screen] > **Settings** ⚙ > **Require authentication for purchases** > Select **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** ⚙ > **Applications** > **Application Manager** > Select an app > Scroll down to **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 *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 antivirus protection.

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Samsung Electronics Co., Ltd., Lookout, Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your social media accounts*

You might be sharing more information about your friends, family and contacts on your social media sites 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 three social media sites.

Social media safety guidelines

- Limit the amount of personal information you publish on social media (first dog's name, school, children's names, etc.), as key profile questions can act as answers to vetting questions trying to protect you
- Report any suspicious activity to the social media site the contact came from. Spam can come in the form of a post, message, email or even a friend request
- Monitor how your social media sites contact you; they will never ask for personal information through messages, posts or emails
- Change your password and report the suspicious activity immediately if you think someone has accessed your account

Facebook

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 most important privacy settings and modify them to match your level of risk comfort.

- Desktop only: Navigate to the **Lock** button [on the upper right corner of your screen] > **Privacy Checkup** > [Modify each of the following sections to your level of risk comfort; try to avoid choosing Public]
 - Posts
 - Apps
 - Profile

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 **More**  on the bottom right of your screen > **Settings** > **Account Settings** > **Privacy** > [Modify each section below to your level of risk comfort]

- Desktop: Navigate to the **Down arrow** [on the upper right corner of your screen] > **Settings** > **Privacy** [on the left side of your screen] > [Modify each section below to your level of risk comfort]

Sections to modify via mobile and desktop access:

- **Who can see my stuff?**
 - Who can see your future posts?
Suggestion: Friends
- **Who can contact me?**
 - Who can send you friend requests?
Suggestion: Friends of friends
- **Who can look me up?**
 - Who can look you up using the email address you provided?
Suggestion: Friends
 - Who can look you up using the phone number you provided?
Suggestion: Friends
 - Do you want search engines outside of Facebook to link to your profile?
Suggestion: No

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

*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.

- iOS and Android: Navigate to **More** ≡ on the bottom right of your screen > **Settings** > **Account 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 **Down arrow** [on the upper right corner of your screen] > **Settings** > **Timeline and Tagging** [on the left side of your screen] > [Modify each Timeline permission to your level of risk comfort, and avoid choosing Everyone where applicable]

Facebook offers a unique 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 **More** ≡ on the bottom right of your screen > **Settings** > **Account Settings** > **Security** > **Legacy Contact** > [Set up trusted contact and preferences]
- Desktop: Navigate to the **Down arrow** [on the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > **Edit** next to Legacy Contact > [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 **More** ≡ on the bottom right of your screen > **Settings** > **Account Settings** > **General** > **Password** > [Enter your current password, then enter your new secure password and confirm] > **Change Password**
- Desktop: Navigate to the **Down arrow** [on the upper right corner of your screen] > **Settings** > Click **Edit** next to 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 **More** ≡ on the bottom right of your screen > **Settings** > **Account Settings** > **Security** > Login Approvals: **On** > **Start Setup** > [Follow activation steps]
- Desktop: Navigate to the **Down arrow** [on the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > Click **Edit** next to Login Approvals > Check box to enable **Security Code** > **Get Started** > [Follow activation steps] > **Save Changes**

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 **More** ≡ on the bottom right of your screen > **Settings** > **Account Settings** > **Security** > **Login Alerts** > [Choose where you would like to receive alerts]
- Desktop: Navigate to the **Down arrow** [on the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > Click **Edit** next to Login Alerts > [Choose where you would like to receive alerts]

*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.

LinkedIn

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.

- Desktop only: Navigate to the **Photo Dropdown > Privacy & Settings > Privacy** > [Modify each setting to your level of risk comfort]

Pay special attention to:

- Who can see your connections
Suggestion: Only you

Control who can contact you via LinkedIn. Modifying your communication settings will limit who can send you invites and messages.

- Desktop only: Navigate to the **Photo Dropdown > Privacy & Settings > Communications** > [Modify each setting based on your level of risk comfort]

Pay special attention to:

- Who can send you invitations
Suggestion: Only people who know your email address or appear in your “Imported Contacts” list
- Messages from members
Suggestion: Introductions only

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** > Tap the **gear icon**  > **Change password** > [Enter your current password, then your new secure password and confirm] > **Save**
- Desktop: Navigate to the **Photo Dropdown > Privacy & Settings > Account > Change password** > [Enter your current password, then your new secure password and confirm] > **Save**

3. Two-factor authentication

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.

- Desktop only: Navigate to the **Photo Dropdown > Privacy & Settings > Privacy > Security > Two-step verification > Turn On** > [Follow activation steps]

*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.

Twitter

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.

- Desktop: Navigate to the **Picture Dropdown** > **Settings** > **Security and privacy** > Check the box next to **Protect my Tweets** > **Save changes**
- iOS: Navigate to **Me** > Tap the **gear icon** ⚙️ > **Settings** > **Privacy and safety** [on the left side of your screen] > Switch **Protect my Tweets**: **On**
- Android: Navigate to the **Picture Dropdown** [on the upper left corner of your screen] > **Settings** > **Privacy and content** > Check box next to **Protect my Tweets**

2. Strengthen your password

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

- Desktop: Navigate to the **Picture Dropdown** > **Settings** > **Password** [on the left side of your screen] > [Enter your current password, then your new secure password and confirm] > **Save changes**
- iOS: *For security reasons, changing your Twitter password is disabled on iOS devices*
- Android: Navigate to the **Picture Dropdown** [on the upper left corner of your screen] > **Settings** > **Account** > **Change password** > [Enter your current password, then your new secure password and confirm]

3. Two-factor authentication

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.

- Desktop: Navigate to the **Picture Dropdown** > **Settings** > **Security and privacy** > Check **Verify login requests** > [Follow steps to enable] > **Save changes**
- iOS: Navigate to **Me** > Tap the **gear icon** ⚙️ > **Settings** > **Account** > **Security** > Switch **Login Verification**: **On** > **Confirm**
- Android: Navigate to the **Picture Dropdown** [on the upper left corner of your screen] > **Settings** > **Account** > **Security** > Check the box next to **Login Verification** > [Follow steps to enable]

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Facebook, Inc., LinkedIn Corp. or Twitter Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

CYBER SAFETY

Securing your social media accounts – Part 2*

You might be sharing more information about your friends, family and contacts on your social media sites 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 additional social media sites.

Social media safety guidelines

- Limit the amount of personal information you publish on social media (first dog's name, school, children's names, etc.), as key profile questions can act as answers to vetting questions trying to protect you
- Report any suspicious activity to the social media site the contact came from. Spam can come in the form of a post, message, email or even a friend request
- Monitor how your social media sites contact you; they will never ask for personal information through messages, posts or emails
- Change your password and report the suspicious activity immediately if you think someone has accessed your account

Snapchat

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 **ghost icon**  > **Settings**  > Scroll to **Who can...** > [Modify each setting based on your level of risk comfort]

Pay special attention to:

- Contact Me
Suggestion: My Friends
- My Story
Suggestion: My Friends or Custom

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 **ghost icon**  > **Settings**  > **Password** > [Enter your current password, then your new secure password] > **Save**
- Desktop: 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 and Android: Navigate to the **ghost icon**  > **Settings**  > **Login Verification** > **Enable SMS Verification** > [Follow steps to enable]

*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.

Instagram

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: Navigate to **your profile**  > **Options**  > Switch Private Account: **On**
- Android: Navigate to **your profile**  > **Options**  > Switch Private Account: **On**

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: Navigate to **your profile**  > **Options**  > **Change Password** > [Enter your current password, then your new secure password] > **Done**
- Android: Navigate to **your profile**  > **Options**  > **Change Password** > [Enter your current password, then your new secure password] > **Done**
- Desktop: Navigate to **your profile**  > **Edit Profile** > **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, Instagram can provide you with a security code when you access your account from a new device.

- iOS: Navigate to **your profile**  > **Options**  > **Two-Factor Authentication** > Switch Require Security Code: **On** > [Follow activation steps]
- Android: Navigate to **your profile**  > **Options**  > **Two-Factor Authentication** > Switch Require Security Code: **On** > [Follow activation steps]

*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.

The listed merchants are in no way affiliated with JPMorgan Chase Bank, N.A., nor are the listed merchants considered as sponsors or co-sponsors of this program. The use of any third-party trademarks or brand names is for informational purposes only and does not imply an endorsement by Facebook, Inc. or Snap Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.