JPMorgan Chase & Co.

CYBER SAFETY

Cybersecurity and fraud prevention are top priorities for J.P. Morgan*

In Asset & Wealth Management, our educational programs and supporting materials about cybersecurity and fraud prevention can help you understand how to better protect yourself, your family and your office against the ever-evolving threats of cyber crime.

Cybersecurity Intelligence

GET STARTED

Speak with your J.P. Morgan representative to learn more about our cyber and fraud prevention programs, for educational information and to schedule a session with our experts. J.P. Morgan is committed to safeguarding your data, but clients remain ultimately responsible for ensuring their own cybersecurity.

PROTECT yourself and your family

Learn best practices that you and your family can implement to help mitigate cybersecurity risk

Audiences: Principals, Board members, C-suite, decision makers, family members, office staff

Key topics

- Email
- Passwords
- Wi-Fi networks
- Internet usage
- Mobile security
- Malware
- Social engineering

PROTECT your office

Understand how you can help improve your family office's, small business's or law firm's cybersecurity posture

Audiences: Office staff, Board members, C-suite

Key topics

- Working together
- Phishing
- Social engineering
- Ransomware
- Technology controls
- Operations
- Office security
- Third-party risk
- Secure communications

PROTECT yourself from fraud

Understand the latest fraud trends and fraud prevention best practices to help strengthen money movement controls

Audiences: Financial staff, authorized users, principals, decision makers

Key topics

- Money movement controls
- Common fraud schemes
- Business email compromise
- Secure communications

*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.

JPMorgan Chase & Co.

CYBER SAFETY

Cybersecurity Awareness and Education

J.P. Morgan is committed to safeguarding our client's data and addressing the ever evolving threats of cyber crime. In addition to the firm's physical, electronic and procedural safeguards, we have a robust set of cybersecurity educational materials and client programs, which include in-depth sessions for individuals, family offices and advisors.

CYBERSECURITY KIT TABLE OF CONTENTS

We are doing more than ever to protect our clients.

We have an extensive set of educational materials on a range of topics, including advanced security tips and content specific to various audiences. Clients can reach out to their J.P. Morgan team to learn more about cyber programs and additional materials we offer, and to schedule a session with our experts. Clients remain ultimately responsible for ensuring their own cybersecurity.

*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., Alphabet Inc., Yahoo Inc., Microsoft Inc., AOL Inc., Facebook, Inc., LinkedIn Corp, Twitter Inc. or Snap Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

Rohan M. Amin
Managing Director
Chief Information Security Officer &
Global Technology Control Officer

May 2018

Dear Valued Customer:

At JPMorgan Chase & Co. ("JPMC" or "Firm"), we have developed a rigorous program to safeguard our customers' data in our care. We are committed to observing the data protection laws and regulations in all the jurisdictions in which we do business.

Our Information Security Program ("Program") is designed to securely enable new business and technology initiatives while maintaining a relentless focus on protecting the Firm and its clients/customers.

How Our Information Security Program is Designed

Our IT Risk and Security Policies and Standards provide the foundation of the Program and establish the rules for safeguarding our IT environment. The Program is designed to:

- Provide for the security and confidentiality of customer, client, and employee information;
- Protect against anticipated threats or risks to the security or integrity of that information;
- Prohibit unauthorized access to, or use of, information that could harm any customer, client or employee;
- Properly store, transport and dispose of customer, client, and employee information;
- Inform employees about their responsibilities to protect customer and client information and the security of our systems;
- Require that our key third party service providers adhere to our security policies and standards, as well as applicable regulatory obligations;
- Adhere to all customer notification requirements for protecting information.

In partnership with the Firm's lines of business, the Global Cybersecurity and Technology Controls ("CTC") organization identifies information security risk issues and champions programs for the technological protection of JPMC's information resources including applications, infrastructure as well as confidential and private information related to the Firm's customers, clients and employees.

How We are Governed

The Global CTC functions are responsible for the governance and oversight of the Program.

The technology governance structure is designed to identify, escalate, and mitigate information security risks. This structure uses key governance forums to disseminate information and monitor technology efforts.

These forums are established at multiple levels throughout the Firm and include representatives from each line of business and relevant corporate functions. Compliance Measurement and Reporting for the organization is produced for these forums, and is reviewed by management at multiple levels including technology management, greater Firmwide management and the Firm's Operating Committee.

The Audit Committee of the Board of Directors reviews and approves the Program annually. Internal and external auditors continually review our IT programs and processes.

Regulators in countries where the Firm operates periodically inspect and review our Program.

How the Program is Implemented

The Firm implements the Program through the following capabilities, processes, controls and technology solutions:[1]

1. Network and Email Security

Our Network and Email Security (NES) strategy is focused on enabling enterprise security controls designed to prevent and detect unauthorized network activities, and protect against risks introduced through web and email communications. Capabilities include securing the perimeter, oversight of firewall rules, limiting access via multiple security controls, network traffic visibility and inspection, and email protection. The NES product as part of the Cyber Operating model also provides a Firmwide control framework for Network and Email Security in partnership with the lines of business, Global Technology Infrastructure, and Risk and Compliance.

2. Endpoint Security

Our Endpoint Security capabilities are designed to detect and prevent malware from infiltrating the Firm's corporate network using end point devices. We manage the security standards and Endpoint Security tools on end point computing devices, such as Workstations, Servers, ATMs and Mainframe/Large Midranges (LMRs). Capabilities include malware detection & prevention, endpoint activity monitoring, and build hardening standards & controls.

3. Data Protection

The Data Protection program identifies and implements actions to improve protection of Firm, customer and client information. The program established a framework designed to apply appropriate cybersecurity controls to business data. These controls include discovery, classification, encryption and data loss prevention. Components of the program are designed to enable the Firm to better:

- Understand the data we have, its sensitivity and ways to protect it;
- Provide standards and guidance on available tools and services;
- Identify, categorize and protect our data;
- Implement encryption and lifecycle protection of our data;
- Maintain and enhance existing data loss prevention services, processes and tools.

[1] As of 2017.

4. **Cloud Security**

The mission of the Cloud function is to ensure the appropriate cybersecurity controls are in place to protect business data and cloud services. Capabilities include logging and monitoring, encryption, access control, lifecycle management and embedding security into all cloud services.

5. **Application and Mobile Security**

Through our secure-from-the-start design processes, the Program assists software engineers and operations teams in developing, implementing and operating secure applications that deliver exceptional client and employee experiences. This is further enhanced by our comprehensive application and mobile code scanning tools and processes to improve early detection and mitigation of software security issues in JPMC and vendor applications.

6. **Vulnerability Reduction Assessments and Training**

Our Vulnerability Reduction strategy is focused on detection and remediation of vulnerabilities across JPMC infrastructure and applications, driving remediation through a standard scoring model and SLAs. Assessments capability is focused on providing visibility into the firm's security posture by demonstrating the exposure to current cyber threats, highlighting vulnerabilities and control weaknesses, by using adversary tactics, tools and procedures in order to inform and prioritize Firmwide risk reduction activities. Exercises capability leverages targeted tabletops, drills, and employee phishing tests to assess the firm's overall readiness to detect, respond to and recover from high-risk cyber scenarios targeting its most critical Business processes and assets. Training is focussed on reducing risk to the firm through enhancing technologists' knowledge, skills and abilities in CTC.

7. **Security Event and Incident Management**

Our security event and incident management capabilities enable monitoring, detection, and investigation of security-related events and incidents. These capabilities leverage threat intelligence, operational risk measures, and business referential context to continually improve early detection of threats and coordinate integrated, Firmwide responses to security-related events.

8. **Digital Forensics**

Our Digital Forensics capabilities enable the recovery, preservation and investigation of material found in digital devices and networks as part of suspected events by employing forensically sound procedures to present in investigative proceedings. Capabilities include providing technical support, evidence collection and storage for Code of Conduct investigations, and responding as Subject Matter Experts in suspected cyber-attacks.

9. **Fraud and Client Protection**

Our processes around fraud and client interaction enable us to better detect and prevent fraud activities relating to cyber security and reduce the risks introduced via client-access channels. These are accomplished by investing in authentication and other technologies to secure the online experience, increasing client awareness and implementing robust fraud prevention technologies. Our fraud program reaches across banking activities, credit/debit card related fraud, as well as our digital platforms. We also search across the web to identify potential phishing campaigns against the Firm.

10. Third Party

Corporate Third-Party Oversight (CTPO) is a dedicated function that establishes the risk management governance framework and enforces defined policies and standards for the lifecycle of third-party service providers engagements.

The framework includes identifying, assessing, managing and monitoring risk from third-party service providers, along with leveraging integrated reporting and analysis for effective risk management.

Controls are reviewed as part of the due-diligence and comprehensive risk assessment conducted of third-party service providers and third-party applications by CTPO's Supplier Assurance Services (SAS) team.

11. Identity and Access Management

The Identity and Access Management program implements access standards and controls across our infrastructure and applications, particularly those that contain customer information. These controls are designed to authenticate users, permit authorized access, enforce consistent administration procedures, maintain segregation of duties, and ensure timely changes through on-boarding/termination/transfer processes for Firmwide information systems.

12. Resiliency and Recovery

The Resiliency and Recovery program aligns an integrated Firmwide resiliency program to the Firm's business strategy and principles, as well as the requirements of the Firm's customers and clients globally. The program is designed to help the Firm recover critical business functions and supporting assets (i.e., staff, technology and facilities) in the event of a business interruption while complying with global laws and regulations relating to resiliency risk. Key elements include:

- Providing continuity of client and customer services while protecting the Firm's employees and assets;
- Engaging senior management on the program, strategy, leadership and oversight;
- Managing resiliency risks proactively to incorporate appropriate procedures and controls;
- Developing and maintaining resiliency plans based on impact analysis and criticality;
- Helping employees understand their role in recovery scenarios and conducting validation exercises across critical functions and locations.

13. Production Management

The mission of the CTC Production Management team is to oversee all Production Operations and ensure the highest degree of standards are being met for uptime, availability, hygiene and overall application health for CTC Products. The current Production Management services that provide stability to CTC are focused on delivering world class services in respect to incident, problem, change, resiliency, capacity, automation, and monitoring. Providing production coverage will ensure that we are reducing risk to the firm by ensuring our CTC toolset is consistently at peak availability.

14. Global Privacy Incident Management

The Global Privacy Office is responsible for establishing and maintaining the Firmwide framework for privacy incident and breach management. This framework drives consistency and provides guidance for Privacy Incident Response Managers and Privacy Compliance functions surrounding the minimum requirements that must be addressed in privacy incident response procedures. Cybersecurity Incident Response Teams escalate privacy incidents, in line with their procedures, to the Privacy Incident Response Team Managers for research, analysis, notification and root cause assignment.

Core responsibilities of the Global Privacy Office as it relates to Privacy Incident Management include:

- Maintaining the Potential Breaches of Information Program including the Potential Breaches of Information Policy, Global Incident Response Standards and global guidance materials;
- Developing and disseminating reporting on Firmwide potential incidents and breaches;
- Advising on high severity incidents (Sev 1) and approving approach for external notifications;
- Providing Firmwide guidance, training and reporting criteria for Incident Response Teams to include in procedures, and
- Communicating policy requirements to JPMC workforce.

Information Security is a Shared Responsibility

At JPMorgan Chase, we take the protection of our customers' data in our care seriously and have the aforementioned capabilities, processes, controls and technology solutions in place to safeguard the data. However, even the best security measures can only be effective in ensuring data security if our customers are also vigilant about employing the necessary safeguards to protect their information.

Thank you for your continued confidence in JPMorgan Chase & Co. We appreciate the partnership with you.

Rohan M. Amin
Managing Director
Chief Information Security Officer &
Chief Technology Control Officer

JPMorgan Chase & Co.

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.

10 Key CYBER SAFETY Tips

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

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

Internet usage

- ✓ Download software only from trusted sources
- ✓ Log out of sites instead of simply closing the session window
- ✓ Look for https:// for secure session validation
- ✓ Enable private browsing whenever possible
- ✓ Delete cookies regularly
- ✗ Do not click on links from unknown or 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

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

CYBER SAFETY Protect yourself and your personal information*

When selecting services, software and equipment, consider the following:

FEATURES TO LOOK FOR

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.

AUTHENTICATION
Provides secure authentication to help prevent spam and spoofing.

VIRUS SCANNING
Email is scanned for malicious content by the provider.

SPAM FILTERING
Providers should filter spam messages from your inbox.

PHISHING PROTECTION
Identifies potential phishing emails.

Look for a provider that offers multi-factor authentication and an intuitive interface.

Password managers

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.

ENCRYPTION
Passwords should be stored with at least 256-bit AES encryption.

MULTI-FACTOR AUTHENTICATION
Offers multi-factor authentication.

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

Virus and malware protection

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.

PERFORMANCE
Does not slow down your system.

PARENTAL CONTROLS
Optional feature to help limit content when devices are being used by children.

BACK-UPS
Optional back-up protection in case of system failure.

Consider the number of devices that each vendor will allow the software to be installed on per license subscription purchase.

Wireless routers

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.

GUEST NETWORK
Allows for a separate and secure network and credentials for guests and children.

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.

JPMORGAN CHASE & CO.

CYBER SAFETY

Securing your credit*

In the United States, your identity and credit history can be used to secure loans and insurance policies, to gain employment and to 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.

Monitor credit

Monitoring 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

Also known as a security freeze, a credit 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.

Putting a credit freeze in place must be done separately with each of the three U.S. credit bureaus. Encourage elderly family members to freeze their credit, as they can be especially susceptible to fraud.

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.

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	Experian	TransUnion
800.349.9960	888.397.3742	888.909.8872
www.freeze.equifax.com	**www.experian.com/freeze**	**www.transunion.com/freeze**

*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.

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:

Equifax	Experian	TransUnion
888.766.0008	888.397.3742	800.680.7289
www.equifax.com/CreditReportAssistance	**www.experian.com/fraudalert**	**www.transunion.com/fraud**

Securing a minor’s credit

Contact each credit bureau to institute a freeze on the credit of minors under the age of 16. Refer to the “Child Identity Theft” page on the Federal Trade Commission’s Consumer Information site for more information (www.consumer.ftc.gov).

In the United States, contact each major credit bureau to understand how to place a credit freeze on a minor’s credit report:

Equifax	Experian	TransUnion
www.equifax.com/personal/credit-report-services	**www.experian.com/fraud/center.html**	**www.transunion.com/freeze**

*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 Equifax, Experian Information Solutions, Inc., or TransUnion, LLC, or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.

JPMorgan Chase & Co.

CYBER SAFETY

Keep yourself safe from fraud*

At J.P. Morgan, protecting your information and assets is our top priority. While we deploy sophisticated fraud prevention strategies, you are an integral component to preventing fraudulent activity. To improve your security posture and mitigate fraud risk, it is vital for you to understand the ways fraudsters can trick you into performing actions or divulging confidential information and best practices to prevent against identity theft.

	WHAT IS IT AND HOW DOES IT HAPPEN?
Email Compromise/ Hacking	Fraudsters target individuals and businesses that regularly perform wire payments via email in a number of ways. Two popular methods are Email Compromise and Invoice Fraud. **Email Compromise:** Fraudsters go to great lengths to socially engineer you and/or your employees by researching you, your company and individuals who process wire transfers on your behalf. By mimicking you or your trusted associates, they use language specific to you and/or your company to ask for funds to be sent to accounts under their control. **Invoice Fraud:** Fraudsters target vendors because individuals and businesses trust the genuine relationship that has been established with their vendors. The fraudster hacks into the vendor's systems and then sends an email requesting a change to the banking details for the vendor. Often, individuals or businesses update the banking details without checking directly with the vendor. This causes payments for future genuine invoices to be directed to an account under the control of the fraudster.
Social Engineering	Fraudsters deceive individuals into providing confidential or sensitive information via email (**phishing**), phone (**vishing**), or text message (**smishing**) by claiming to be a trusted associate or organization. J.P. Morgan Chase will never ask you to disclose confidential information/credentials in an email or text message. We will also never ask you to move money into a new account via email, phone or text message.
Wire and ACH Fraud	**Wire fraud** occurs when a fraudster transfers funds to an account unbeknownst to the account holder, or when the account holder unintentionally sends a wire transfer to a fraudulent account. **ACH fraud** occurs when an account is accessed for unauthorized ACH payments (debits).
Online Banking Fraud	**Online banking fraud** occurs when malicious software, also known as malware, is installed on your computer. Through viruses, keystroke loggers, ransomware or other types of malware, fraudsters gather confidential account credentials and financial information.
Remote Access	Fraudsters can gain remote access to your computer through **malware** or **phishing attempts** claiming to be reputable virus protection providers. With this access, fraudsters can take over your computer and complete transactions without your knowledge.

*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.

CYBER SAFETY **Keep yourself safe from fraud***

Top 10 actions you can take to protect yourself from fraud

Money movement and online banking

1. Always validate payment instructions by calling the originator on a known number when instructions are received via email, even if the email is from a senior member of the company or a trusted vendor
2. Check your online banking accounts for unauthorized activity periodically, and set up online alerts to notify you of account changes and transactions
3. Never share banking credentials and passwords, and never log into your online banking from a public computer or Wi-Fi
4. Adopt multi-factor authentication for all online banking accounts and always log off your online banking account when not in use
5. Do not preprint or include personal information on the checks and keep your checks in a safe place

Computer, email and telephone

1. Ensure operating systems and data protection software on your computer and mobile devices, including anti-malware and anti-virus software, are up-to-date
2. Do not allow anyone to access your computer remotely
3. Be wary of the following red flags in emails:
   - Spoofed email address
   - Poor grammar or spelling
   - Urgency around payment transmission
   - Late changes of payment instructions
   - Suspicious attachments or links
   - Blurred company logo on an invoice
4. Do not assume a phone call is genuine because the person on the other end has your information; J.P. Morgan will never call to instruct you to move funds to a new account
5. Do not call or text an unknown phone number; call a known number (i.e. back of the credit card or your banking representative) to help prevent a possible fraud incident

J.P. Morgan will never:

– Ask you to log in to the same computer with more than one user's credentials

– Ask you to repeatedly submit login credentials

– Contact you about online problems, such as logging in, if you haven't contacted us first

– Request sensitive confidential information by email

If you believe you have been targeted by a fraud scheme or your login credentials have been compromised, please contact your J.P. Morgan representative.

Remember, if you receive a request to provide personal or financial information, take a step back from the situation to evaluate it. Even if the requestor claims to be your bank or other trusted organization, don't rush to action!

*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.

JPMorgan Chase & Co.

FRAUD PREVENTION

Fraud scheme: Invoice fraud*

Both individuals and organizations can fall victim to invoice fraud. Invoice fraud occurs when fraudsters exploit trusted relationships between you, your business, and vendors or third party service providers. Fraudsters often target third parties you work with in an attempt to redirect payments to their accounts. They may compromise the third party's email system and send genuine-looking invoices to deceive you or your business.

To help reduce the risk of invoice fraud, consider the best practices below:

1. **Establish a designated point of contact at the third party or vendor** to whom you, or your business, makes regular payments; raise all invoice issues and concerns with this person
   - Consider implementing an approval strategy within your organization for larger invoices
   - Verbally confirm the banking details with the third party before the payment is initiated
   - Inform the vendor or supplier after an invoice has been paid and request confirmation of payment
2. **Ensure employees responsible for processing payments remain vigilant for changes to payment instructions,** particularly banking details, invoiced amounts and sense of urgency
   - Verify all changes to standing payment instructions by implementing a call back process
   - Be vigilant for spoofed emails that appear to be from a known and trusted source. This can be done by modifying the header in a malicious email to pose as a trusted sender – for example, @**deanco**LLC.com can appear similar to a known vendor @**cleanco**LLC.com
   - Check bank statements carefully; all suspicious debits should be reported to J.P. Morgan immediately
3. **Protect your personal and business information**
   - Fraudsters often conduct extensive online and offline research to identify vendors and third parties with whom you work
     - Consider removing extraneous information from your website, social media and other publicly available materials
     - Be prudent in what you share about your role and responsibilities via social media
     - Never leave sensitive material such as invoices, account information and client data unattended

We can help

If you believe you, or your business, have been a victim of invoice fraud, speak with your J.P. Morgan representative immediately.

[1] Between October 2013 and December 2016, more than 40,000 domestic and international incidents were reported to the FBI's Internet Crime Complaint Center with a total of $5.3 billion in potential losses.

*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.

JPMorgan Chase & Co.

CYBER SAFETY

Securing your iPhone™ and iPad™*

Operating System: iOS 12

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

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**

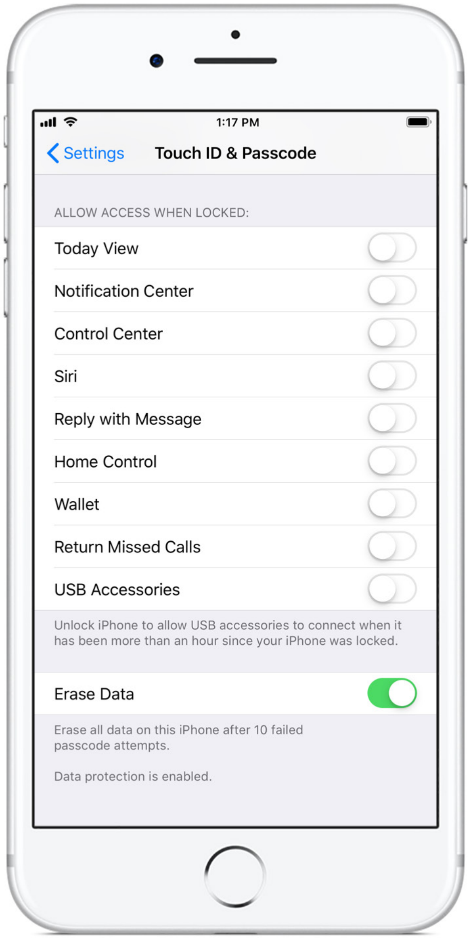
- AirDrop:
  Settings > **General** > **AirDrop** > *Suggestion: Switch to "Receiving Off" or "Contacts Only"*

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.



1:17 PM

< Settings Touch ID & Passcode

ALLOW ACCESS WHEN LOCKED:

Today View ○
Notification Center ○
Control Center ○
Siri ○
Reply with Message ○
Home Control ○
Wallet ○
Return Missed Calls ○
USB Accessories ○

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data ●

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

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** > **iCloud** > **Find My iPhone** (or iPad) > 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** > **iTunes & App Store** > **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. Apple is not a participant in or sponsor of this promotion.

JPMorgan Chase & Co.

CYBER SAFETY

Securing your iPhone X™*

Operating System: iOS 12

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

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** > **Enter Passcode** > **Allow Access When Locked** > Switch OFF: **Today View, Notification Center, Control Center, Siri, Reply with Message, Home Control, 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"*

Disable access to Wallet on your locked device:

- Navigate to **Settings** > **Wallet & Apple Pay** > Switch OFF: **Double-Click Side Button**

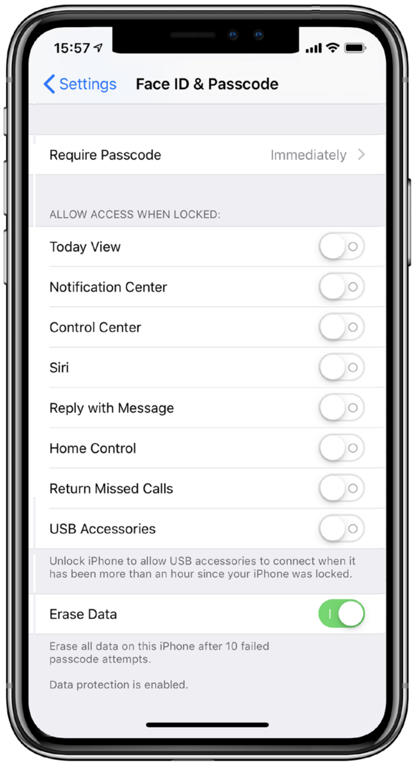
Note: Wallet will still be accessible via "Control Center" and the "Wallet" Home Screen icon.

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** > **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.



15:57

< Settings Face ID & Passcode

Require Passcode Immediately >

ALLOW ACCESS WHEN LOCKED:

Today View	○
Notification Center	○
Control Center	○
Siri	○
Reply with Message	○
Home Control	○
Return Missed Calls	○
USB Accessories	○

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data	●

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

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** > **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, 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** > 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** below **Request 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. Apple is not a participant in or sponsor of this promotion.

Securing your Samsung Galaxy S9*

Operating System: Android 8 Oreo

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) > **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:

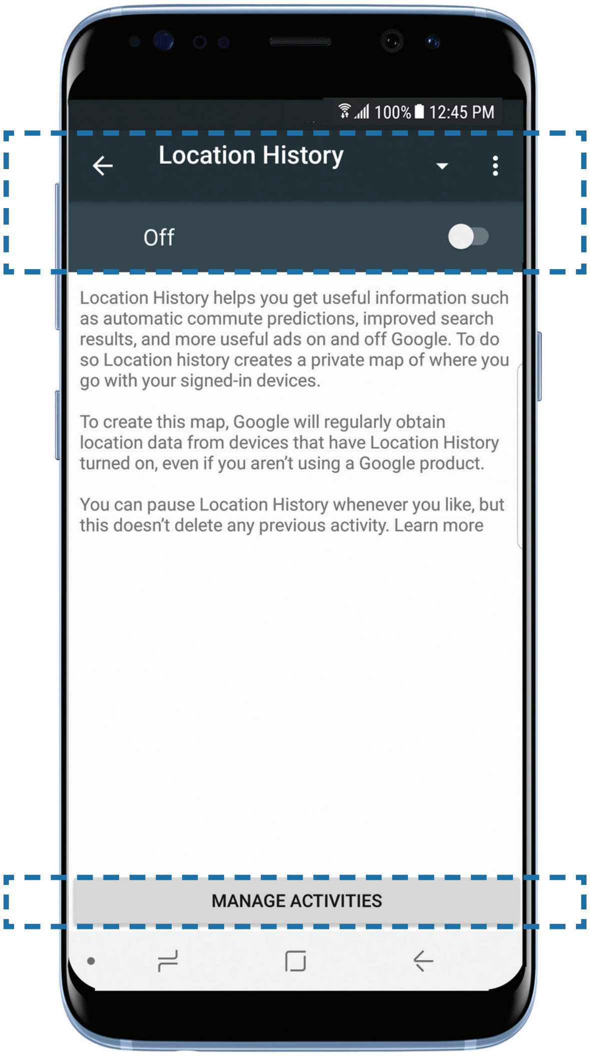
- Navigate to **Settings** ⚙ > **Lock screen and security** > **Notifications** > Switch ON: **Hide Content**

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**



Location History helps you get useful information such as automatic commute predictions, improved search results, and more useful ads on and off Google. To do so Location history creates a private map of where you go with your signed-in devices.

To create this map, Google will regularly obtain location data from devices that have Location History turned on, even if you aren't using a Google product.

You can pause Location History whenever you like, but this doesn't delete any previous activity. Learn more

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.

*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.

JPMorgan Chase & Co.

CYBER SAFETY

Securing your Android Google Pixel and Pixel XL*

Operating System: Android 9 Pie

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 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:

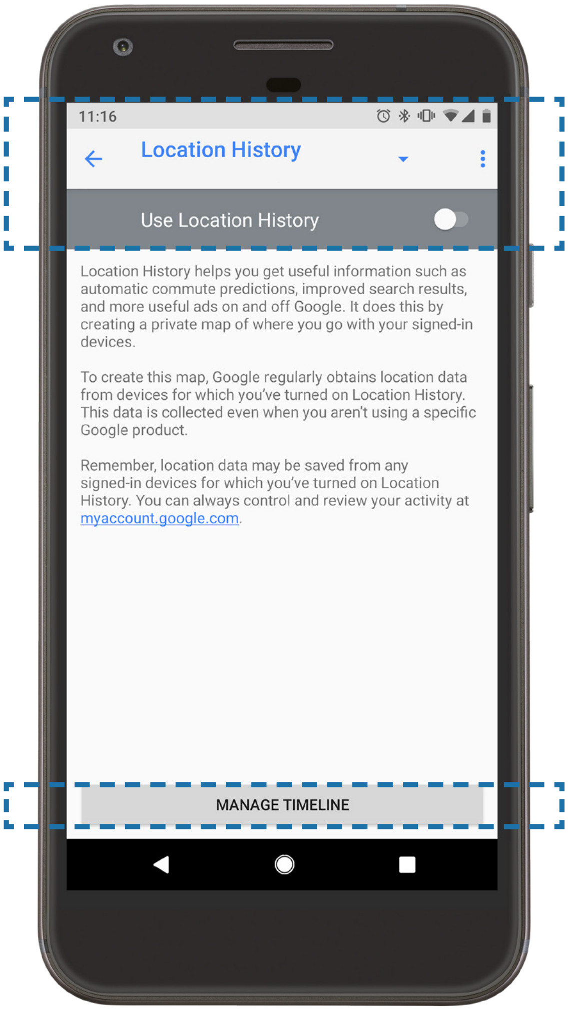
- Navigate to **Settings** ⚙ > **Apps & notifications** > **Notifications** > **On lock screen** > **Hide sensitive content**

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**



11:16

Location History

Use Location History

Location History helps you get useful information such as automatic commute predictions, improved search results, and more useful ads on and off Google. It does this by creating a private map of where you go with your signed-in devices.

To create this map, Google regularly obtains location data from devices for which you’ve turned on Location History. This data is collected even when you aren’t using a specific Google product.

Remember, location data may be saved from any signed-in devices for which you’ve turned on Location History. You can always control and review your activity at myaccount.google.com.

MANAGE TIMELINE

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.

*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 Alphabet, 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 device 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

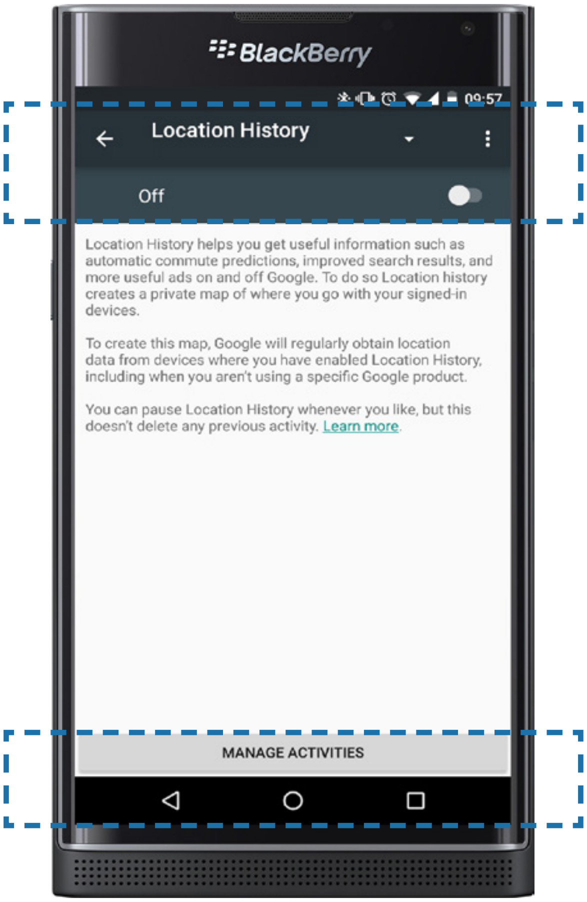
By default, Android tracks where you have taken your device. Disabling this feature will help protect you. Disable Google Location History:

- 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**



Location History helps you get useful information such as automatic commute predictions, improved search results, and more useful ads on and off Google. To do so Location history creates a private map of where you go with your signed-in devices.

To create this map, Google will regularly obtain location data from devices where you have enabled Location History, including when you aren't using a specific Google product.

You can pause Location History whenever you like, but this doesn't delete any previous activity. Learn more.

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 and payments** 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** > **Services** > **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** ≡ > **Settings** ⚙ > **Require authentication for purchases** > **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** ⚙ > **Device** > **Apps** > 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.

*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

Recognizing email threats and social engineering*

Hackers take advantage of our trust and natural willingness to be helpful by employing social engineering techniques to break our usual cybersecurity practices. Cybercriminals can trick you into performing actions or divulging confidential information via email, phone calls, social media and other interactions, which could lead to a compromise of your data or assets.

EMAIL THREATS

Email phishing

Cybercriminals attempt to trick individuals into replying to or clicking a link in an email that may appear to be legitimate. **Phishing** emails can contain malicious software (malware) or attempts to convince the recipient to divulge sensitive information such as confidential data or account credentials. **Spear phishing**, a more targeted form of phishing, can use information collected online or via social media to make the email, and request within it, appear more credible.

Email spoofing

Fraudsters mimic or **spoof** an email to convince targets that the email they are receiving is from a known and trusted source. This can be done by modifying the header in a malicious email to pose as a trusted sender – for example, **@deancoLLC.com** can appear similar to a known vendor **@cleancoLLC.com**. Similarly, a fraudster can copy a logo from a known company to trick their target into thinking it's a credible email.

Email account compromise

Cybercriminals use a victim's legitimate username and password to gain access to his account to send, receive and view their target's email. Through an **email account compromise**, they are looking to capture information such as details on upcoming financial transactions or to manipulate a wire transfer into their account.

CASE STUDIES/CONSEQUENCES

1. **Malware installed via phishing:**
   A CEO at a family office received a seemingly innocuous email notifying him that the family was to be profiled in a well-known business publication, and to expect a second email with a draft of the article featuring them. The second email contained an attachment appearing to be the draft article, which infected the firm's computer systems with a virus when opened. The fraudsters targeted the CEO to gain key information about the family office and its transactions.

2. **Information and credentials stolen via spoofing:**
   Cybercriminals registered domain names that closely resembled a company's legitimate domain name, with the difference being a single altered letter or character. They sent a spoofed email to employees at the company, targeting individuals responsible for making payments. The targets did not look closely at the sender's email address, and inadvertently sent out financial information and account credentials to the cybercriminals.

3. **Wire fraud via email account compromise:**
   An attorney emailed her client with payment instructions a few days before a real estate transaction was due to be completed. A hacker, who had already gained access to the law firm's email server, sent an email (which appeared to come from the attorney) to the client, changing the wire details hours before the payment was due. The client sent the updated wire instructions to the bank, who called back to confirm the transaction details. The client confirmed the fraudulent wire instructions without validating the change with the attorney via phone, and the money was wired to the hacker's account.

*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.

CYBER SAFETY Recognizing email threats and social engineering*

WHAT YOU CAN DO

Learning to protect yourself and your business from email phishing, spoofing and account compromise needs a multi-pronged approach that should address people, process and technology. Learn how to identify the warning signs of fraudulent emails, and educate and equip your employees with the tools and technology they need to stay ahead of fraudsters looking for information and access.

For individuals

1. Recognize phishing email warning signs, such as poor grammar and spelling, urgent language, hyperlinks or attachments, fake logos, a vague email address and no or vague contact information
2. Do not assume a request is genuine just because the requester knows information about you or your company
3. Confirm the identity of the requester via an alternate, verified method, and check the email address: scammers often use spoofed email addresses to send what seem to be legitimate requests
4. Be cautious of clicking on any links or attachments sent to you in emails
5. Limit the information you post on social media. Every account is a venue for a hacker to gain intelligence on you
6. Create strong and complex passwords, change them frequently and never share them
7. Update operating systems and anti-virus software on computers and mobile devices to the latest versions, as soon as they become available
8. Encrypt sensitive information such as account numbers, tax information or other personal information before emailing it

For businesses

1. Educate your employees about threats in the cybersecurity landscape and how they can mitigate risk. Consider conducting phishing tests of varying complexity as a practical way to measure the effectiveness of a cybersecurity education program
2. Implement a social media policy for employees to ensure critical information about staff with privileged responsibilities and their roles is not available to the public
3. Employ additional spam reduction solutions or filters, if needed, to help reduce the risk of malicious emails reaching employees' inboxes
4. Implement the email authentication protocols Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentications, Reporting and Conformance (DMARC) to greatly enhance the authenticity of the emails your organization sends and receives
5. Use a proxy internet filtering service to help block employees from visiting potentially malicious web pages and links found in spam email

*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.

JPMorgan Chase & Co.

CYBER SAFETY

Protect yourself from email threats*

Cybercriminals can trick you into performing actions or divulging confidential information via phone calls, email, social media and other interactions, which can lead to a compromise of data or assets.

EMAIL PHISHING

EMAIL SPOOFING

EMAIL ACCOUNT COMPROMISE

Protect yourself

1. **Recognize phishing email warning signs**, such as poor grammar and spelling, urgent language, hyperlinks or attachments, fake logos, a vague email address and no or vague contact information
2. **Do not assume a request is genuine** just because the requester knows information about you or your company
3. **Confirm the identity of the requester via an alternate, verified method**, and check the email address: scammers often use spoofed email addresses to send what seem to be legitimate requests
4. **Be cautious of clicking** on any links or attachments sent to you in emails
5. **Limit the information you post on social media**. Every account is a venue for a hacker to gain intelligence on you
6. **Create strong and complex passwords**, change them frequently and never share them
7. **Update operating systems and anti-virus software** on computers and mobile devices to the latest versions, as soon as they become available
8. **Encrypt sensitive information** such as account numbers, tax information or other personal information before emailing 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.

JPMorgan Chase & Co.

CYBER SAFETY

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

*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 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 Alphabet, Yahoo, Microsoft or AOL, or that such trademark owner has authorized JPMorgan Chase Bank, N.A., to promote its products or services. All trademarks are the property of their respective owners.

SECURING YOUR GMAIL 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 **myaccount.google.com** and log in > Select **Sign-in & security** > Select **Password** on the right > **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 **Sign-in & security** > In the "2-Step Verification" box on the right, select **Start setup** > 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 Sign-in & 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 **Personal info & Privacy** > Select **Change this setting** under Inactive Account Manager > 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 > In the Security Checkup section, select **Get Started** > 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 > In the Security 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
  - Check “Grant access to your account” section to ensure no unknown people have access to your account
  - Ensure all email addresses in the “Check mail from other accounts” section belong to you
- 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

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 **Delete your account or services** under Account preferences > Choose whether you would like to delete just a product (e.g. Gmail) or your Google Account and its data > Follow steps

- Select the **Forwarding and POP/IMAP** tab
  - Ensure messages aren’t being forwarded to an unknown account
  - Do not enable POP or IMAP access if it is not needed (e.g. Apple Mail uses IMAP)

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 **Sign-in & security** > Review **Recent security events** and **Recently used devices** in the Device activity & security events section 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

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 **Phone numbers** or **Email addresses** > **Add recovery phone number** or **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

Yahoo also has the ability to report an email sent from a hacked account, a phishing email or emails that were intended for someone else.

Report email sent from a hacked account:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Report a Hacked Account**

Report phishing scams:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Report a Phishing Scam**

Report emails intended for someone else:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Not My Mail**

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 **Settings** ⚙ > **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 **Terminating your Yahoo account** > Read the information under "Before continuing, please consider the following information" > Confirm your password > **Terminate this Account**

SECURING YOUR HOTMAIL/OUTLOOK 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** > **Change Password** > Enter your new complex password and confirm it > **Select Change Password**

Note: Hotmail and Outlook also provide you the ability to automatically be prompted to change your password every 72 days.

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 **Profile** > **View Account** > **Security** > **More Security Options** > **More Security Settings** > **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** > **Update your security 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** > **Options** > **Mail** > **Junk Mail** > **Filters and Reporting, Safe Mailing Lists, Safe Senders,** and **Blocked Senders**

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** > **Options** > **Accounts** > **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** ⚙ > **Options** > **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 **Options** in the upper-right corner > **Account Info** > **Account security** > **Change Password** > Enter your current password, then your new secure password and confirm > **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 **Options** in the upper-right corner > 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 **Create app passwords** > Choose an application from the drop-down menu > Enter device name > Open the app for which you created the password and enter the password into the "Password" field for this app

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 **Options** in the upper-right corner > **Account Info** > **Account 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 **Spam** button in the toolbar above your emails
- Forward suspicious emails to **aol_phish@abuse.aol.com**

AOL gives the option to block or allow emails from specific senders.

- Navigate to **Options** in the upper-right corner > **Mail Settings** > **Spam Settings** > **Sender Filter** > Enter or remove usernames or email addresses

Premium security features

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

- Navigate to **Options** > **Help** > **AOL Plans**

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 > **Filter Settings** > Ensure only filters you created are enabled

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.

Note: AOL automatically disables accounts that are inactive for 90 days.

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

Review recent activity

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

- Navigate to **Options** in the upper-right corner > **Account Info** > **Recent activity**

*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 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 Alphabet, Yahoo, Microsoft or AOL, or that such trademark owner has authorized JPMorgan Chase Bank, N.A., to promote its products or services. All trademarks are the property of their respective owners.

JPMorgan Chase & Co.

CYBER SAFETY

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 occuring. Facebook, LinkedIn, Twitter, Snapchat and Instagram provide specific instructions on how to do so

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

- **iOS and Android:** Navigate to **Menu ≡** > **Settings & Privacy** > **Account Settings** > **Privacy** > **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
  - Posts
  - Profile
  - Apps and Websites
    Suggestion: Avoid choosing Public 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** > **Account Settings** > **Privacy** > Modify each section to your level of risk comfort
- **Desktop:** Navigate to the **Menu ▼** > **Settings** > **Privacy** > Modify each section to your level of risk comfort

Sections to modify via mobile and desktop access:

- Who can see your future posts?
  Suggestion: Friends
- Who can send you friend requests?
  Suggestion: Friends of friends
- 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

*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.

Facebook (continued)

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** > **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 **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** > **Account Settings** > **Apps** > 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

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** > **Account Settings** > **General** > **Manage Account** > **Legacy Contact** > Set up trusted contact and preferences
- **Desktop:** Navigate to the **Menu ▼** > **Settings** > **General** > **Edit** next to Manage Account > 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** > **Account 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** > **Account 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** > **Account 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

*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.

- **iOS and Android:** Navigate to **Me** > **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

Control 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** > **Settings** ⚙ > **Communications** > Modify each setting based on your level of risk comfort
- **Desktop:** Navigate to **Me** > **Settings & Privacy** > **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 and partners
Suggestion: Introductions only

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

- **iOS and Android:** Navigate to **Me** > **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** > **Settings** ⚙ > **Change password** > Enter your current password, then your new secure password and confirm > **Save**
- **Desktop:** Navigate to **Me** > **Settings & Privacy** > **Account** > **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** > **Settings** ⚙ > **Privacy** > Switch ON: **Two-step verification** > Follow activation steps
- **Desktop:** Navigate to **Me** > **Settings & Privacy** > **Account** > **Security** > **Turn on** Two-step verification > 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.

- **iOS:** Navigate to **Me** 👤 > **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** > 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 **Me** 👤 > **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 **Me** 👤 > **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

*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.

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 **Picture dropdown** 👻 **> Settings** ⚙ > **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

  – My Location
  Suggestion: 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** ⚙ > **Login Verification** > **Continue** > **SMS** > 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.

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 ON: **Private Account**
- **Android:** Navigate to **Your profile** 👤 > **Options** ⋮ > 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:** 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 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 ON: **Require Security Code** > Follow activation steps
- **Android:** Navigate to **Your profile** 👤 > **Options** ⋮ > **Two-Factor Authentication** > Switch ON: **Require Security Code** > 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

*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, Twitter Inc. or Snap Inc., or that such trademark owners have authorized JPMorgan Chase Bank, N.A. to promote their products or services.