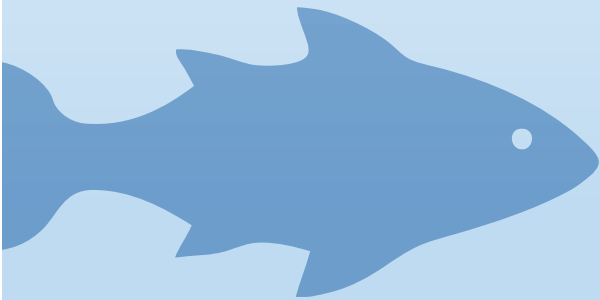




Cybersecurity Awareness and **Fraud** **Prevention**



JPMORGAN CHASE & Co.

*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

Cybersecurity Awareness and Fraud Prevention

TABLE OF CONTENTS

• Cybersecurity Awareness Program Overview “Protect the Client”	3
• Protect yourself and your personal information	5
Lists top tips and cyber safeguards that can be put in place, as well as features to look for when choosing services, software and equipment.	
• Passwords and password managers	7
• Recognizing email threats and social engineering	9
Highlights the potential consequences of the top email threats and social engineering techniques, as well as how to protect yourself and your business.	
• Securing your email accounts	11
Provides email security best practices, including account security features and what to do if you believe your account has been compromised for Gmail, Yahoo, Hotmail/Outlook and AOL accounts.	
– Gmail account	13
– Yahoo account	15
– Hotmail/Outlook account	17
– AOL account	19
– iCloud Mail account	21
• Securing your mobile devices	23
Offers advice on how to secure Apple, Android and other popular mobile devices.	
– iPhone and iPad	25
– iPhone X	27
– Samsung Galaxy S9	29
– Android Google Pixel and Pixel XL	31
• Securing your social media accounts	33
Provides social media safety guidelines and steps to keep information more secure on popular platforms including Facebook, LinkedIn, Twitter, Snapchat and Instagram.	
• Safeguards for travel protection	41
Includes suggestions for protecting your devices and personal information while traveling.	
– Protect yourself while traveling	43
• Tips on fraud prevention	47
Includes best practices for recognizing and preventing against fraud in email, credit, and payments.	
– Securing your credit	49
– Keep yourself safe from fraud	51
– Fraud scheme: Invoice fraud	53
• How J.P. Morgan helps protect you	55
At J.P. Morgan, protecting your information and assets is our top priority.	
– Corporate IT Risk and Security Management Program	57

*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

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.



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.

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

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

	FEATURES TO LOOK FOR	
Email providers <p>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.</p>	AUTHENTICATION <p>Provides secure authentication to help prevent spam and spoofing.</p>	SPAM FILTERING <p>Providers should filter spam messages from your inbox.</p>
	VIRUS SCANNING <p>Email is scanned for malicious content by the provider.</p>	PHISHING PROTECTION <p>Identifies potential phishing emails.</p>
	Look for a provider that offers multi-factor authentication and an intuitive interface.	
Password managers <p>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.</p> <p>Password management tools help users store and organize passwords, and can even provide additional features, such as form filling and password generation.</p>	SYNCHRONIZATION <p>A password manager should allow secure access from anywhere and synchronize across devices.</p>	ENCRYPTION <p>Passwords should be stored with at least 256-bit AES encryption.</p>
	PASSWORD GENERATOR <p>Can automatically generate strong, complex passwords.</p>	MULTI-FACTOR AUTHENTICATION <p>Offers multi-factor authentication.</p>
	Look for a password management tool that supports the types of browsers, operating systems and mobile devices you use.	
Virus and malware protection <p>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.</p> <p>Running real-time anti-virus products and keeping them up-to-date is an essential step to reduce risks from malware.</p>	DETECTION <p>Should detect existing and new variations of malicious software.</p>	PERFORMANCE <p>Does not slow down your system.</p>
	CLEANING <p>Effectively quarantines or removes malicious software from an infected device.</p>	PARENTAL CONTROLS <p>Optional feature to help limit content when devices are being used by children.</p>
	PROTECTION <p>Helps maintain a healthy system by proactively preventing malicious infection.</p>	BACK-UPS <p>Optional back-up protection in case of system failure.</p>
	Consider the number of devices that each vendor will allow the software to be installed on per license subscription purchase.	
Wireless routers <p>A wireless router allows you to connect devices to the internet and communicate with other devices on your network.</p> <p>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.</p>	AUTO-UPDATE <p>Choose a router that automatically updates its software, also known as firmware.</p>	GUEST NETWORK <p>Allows for a separate and secure network and credentials for guests and children.</p>
	FIREWALL <p>Secures your network from intruders.</p>	
	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.	

Passwords and password managers

We use passwords for nearly everything we do on the internet, from shopping, making dinner reservations, streaming media, and banking, to name a few. Passwords are how you prove your identity to a site you are logging into. Simple passwords may seem convenient, but they also make it easy for hackers to steal confidential information. Today’s hackers have automated tools designed to scan target databases for words, names and linguistic patterns, working to crack your password.

If your password is “123456,” your pet’s name or looks like one of the bad passwords on the right, you may as well not even have a password. Hackers are able to crack passwords like these in under a minute.

Top bad passwords: ¹		
123456	qwerty	football
password	princess	iloveyou

Taking some simple steps will go a long way to keeping your private information more secure.

1. The longer and more complex the password, the better. Create passwords with at least 10-15 characters. Try something more complex: use a book, song title, or a line from a poem as a password—something unique to you:
2BorNot2B_ThatIsThe?
DONTstop.B3li3v1n

2. Do not use the same password for multiple accounts

3. Include upper- and lower-case letters, numbers and special characters, such as “ ! & \$ * # “

4. Doubling basic passwords and adding special characters can increase length and strength, as can adding a prefix or suffix

Using a password manager

If you have a lot of passwords to manage, consider using a reputable password manager with state-of-the-art encryption to help you better manage them and stay secure.

A **password manager** is a software application used to store and manage the passwords for your various online accounts. Password managers store the passwords in an encrypted format and provide secure access to all the password information with the help of one master password. Password Managers can also suggest better and secure passwords and autofill this information when you return to a site.

What are the benefits and is it safe?

One single password

You only ever need to remember the master password to the manager. The manager will take care of everything else. You can use these on smart phones via an app, or on a laptop, or tablet.

Secure password suggestions

A built-in password generator will suggest secure and unique passwords whenever you create or update an account. You can also elect to have the password manager change passwords regularly on sites, such as daily, weekly, etc.

Auto-entry

Once you enter the login credentials for a site, the password manager will autofill this information whenever you return to the site. You will not need to memorize numerous passwords anymore, just the main password for the password manager.

¹ “Worst passwords of 2018,” *Splashdata*, December 2018.

Password manager benefits (continued)

Password syncing

Login data syncs in the cloud, so your passwords are available on all of your devices, and even across users. If you and your spouse share an online shopping account, or movie streaming service—the password to this will sync across both users devices.

Digital vault

For information or codes you do not want to forget, many password managers offer a digital vault, in which you enter information such as a passport number, the entry code to a vacation home, answers to security questions, or wi-fi passwords.

Digital legacy

Several password managers offer the ability to designate an emergency contact who can receive access to your online accounts if you die or are incapacitated. Your digital legacy contact can help manage or shutdown your email, social media, online banking and other online accounts, as needed.

Is it safe?

Your data is safe, since your passwords are buried under several layers of encryption. Most services do not track your master password so it is critical that you remember it.

How do I select the right password manager?

There are many password managers available from which to choose. You should research a few to find the right mix of features, services and convenience that will work best for you and your family, or for your business. Perhaps trial one or two before making your decision.

In addition to state of the art encryption, a good password manager should have these key features:

- secure sharing across users, such as other family members or colleagues
- digital legacy contact
- digital vault
- two-factor authentication

A few reputable services such as LastPass, DashLane, Keeper, and 1Password consistently rank highly year after year with independent reviews. You can easily compare services with a quick online search.

How do password managers work?

1. Download and install the password manager software of your choice.
2. Create a master password to access and edit your password list. This is the only password you will need to remember.
3. Manage your passwords: Start adding sites and password information to your password manager list.
4. Log into a site: When you login to a website or app you've registered with the password manager, you will be prompted to autofill the information from your password manager to log you in.

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.

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

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.

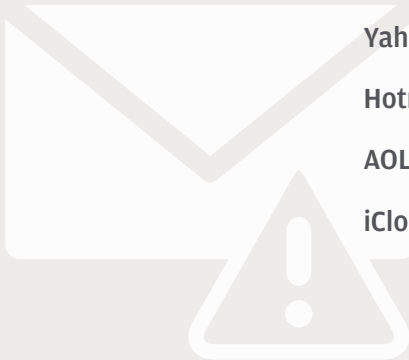
Email security best practices

- 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 contain 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

Gmail account	13
Yahoo account	15
Hotmail/Outlook account	17
AOL account	19
iCloud Mail account	21



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

SECURING YOUR 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)

- 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

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

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.

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**

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.

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**

SECURING YOUR iCloud MAIL ACCOUNT

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

Account security features**Strengthen your password**

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


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


Enable 2-step verification

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

Tools to identify if your account has been compromised**Check email forwarding and filter settings**

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

- Navigate to **icloud.com/mail** > In the bottom left, select Settings  > **Rules...**
 - 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 "Move to Trash" filter)

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

Enable recovery contact information


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

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

Filter suspicious emails

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

Report spam:

- Select the message you'd like to report > Select the Flag  > Select **Move to Junk**

- Navigate to **icloud.com/mail** > In the bottom left, select Settings  > **Preferences...** > **General**

– Ensure messages aren't being forwarded to an unknown account and are not being deleted after forwarding

Account recovery

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

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

Closing your account

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

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

Securing your mobile devices

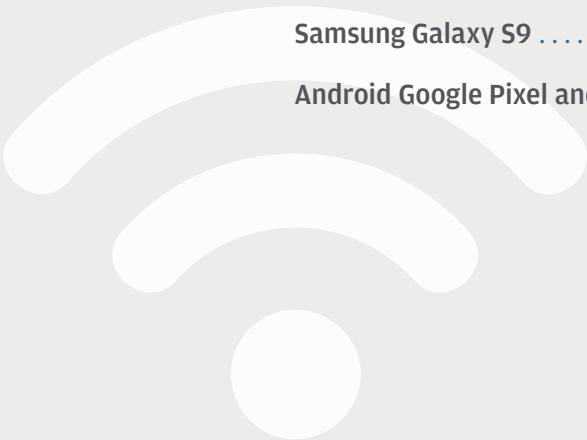
Your mobile device, which has made life so much more convenient, can track who you are, where you have been, and information about your friends, family and contacts. This can make you and your device a prime target for hackers. Here are some easy steps to keep your information more secure.

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

Mobile device safety guidelines

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

iPhone and iPad	25
iPhone X	27
Samsung Galaxy S9	29
Android Google Pixel and Pixel XL	31



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

SECURING YOUR IPHONE AND IPAD

Operating System: iOS 12

Limit your potential exposure**1. Lock your device**

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

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

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

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

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

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

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

Disable wireless technologies when not in use:

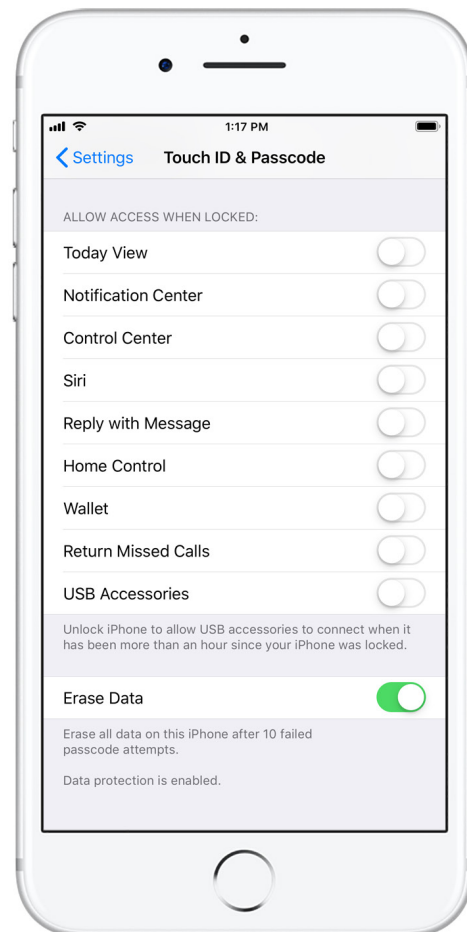
- Wi-Fi and Bluetooth:
Settings > Switch OFF: Wi-Fi and Bluetooth
- AirDrop:
Settings > General > AirDrop > Suggestion: Switch to “Receiving Off” or “Contacts Only”

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

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

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

Note: Regularly back up your device to iCloud or your computer, via USB with iTunes, to ensure you can reinstall your data, apps and settings upon recovery.



4. Disable tracking of your device

By default, iOS tracks your device's most frequently visited locations. Disabling this feature ensures that information could never end up in the wrong hands:

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

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

5. Limit data and location tracking

Application tracking

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

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

Advertising

Limit advertisers from building a personal profile about you:

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

Browser controls

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

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

6. Find your device if it's misplaced, lost or stolen

Locate and maintain control of your iPhone or iPad, even if it's not in your possession, by:

- Changing your passcode
- Preventing it from being reactivated with another phone number
- Erasing all of your data

- Navigate to **Settings > 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**

SECURING YOUR IPHONE X

Operating System: iOS 12

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**

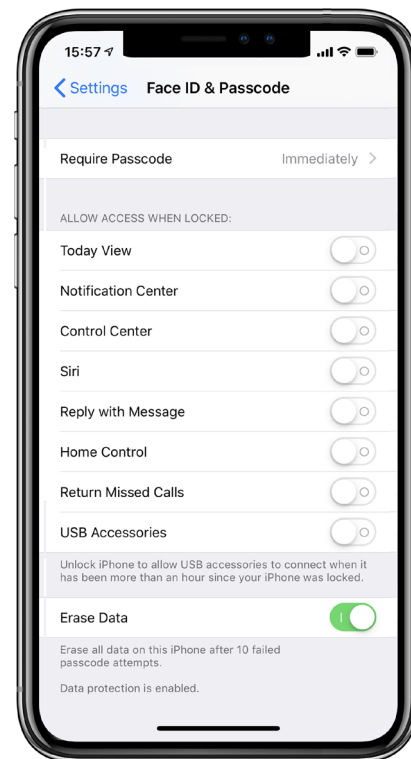
Note: Wallet will still be accessible via “Control Center” and the “Wallet” Home Screen icon.

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.



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**

SECURING YOUR SAMSUNG GALAXY S9

Operating System: Android 8 Oreo

Limit your potential exposure**1. Lock your device**

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

- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Screen lock type** > Enter password (if prompted) > **Pin** > Enter a 6-digit passcode and confirm

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

- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Secure lock settings** > **Lock automatically** > **Immediately** > Switch ON: **Lock instantly with power key, Auto factory reset** and **Lock network and security**

Additionally, use Fingerprint Scanner if you prefer to unlock your Galaxy with your fingerprint:

- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Screen lock type** > Switch ON: **Fingerprints** > Follow activation steps

2. Limit information appearing on your lock screen

Android allows you to select the type of notification displayed on your locked Android device. "Hide content" will limit the information about the sender and message contents:

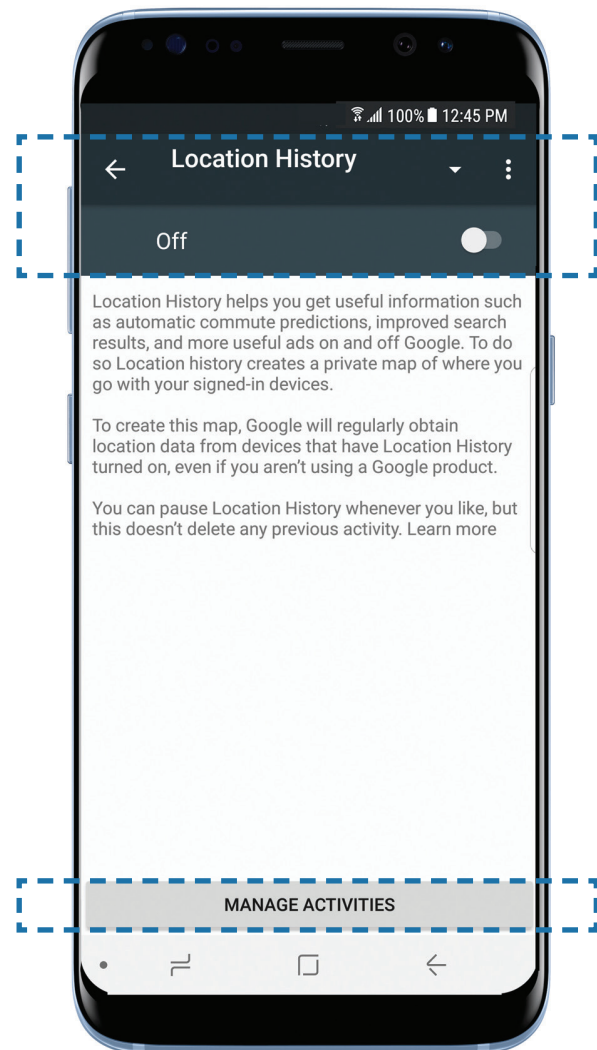
- Navigate to **Settings** ⚙️ > **Lock screen and security** > **Notifications** > Switch ON: **Hide Content**

3. Disable tracking of your device

By default, Android tracks where you have taken your device. Disabling this feature will help protect you.

Disable Google Location History:

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



4. Limit data tracking on your device

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

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

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

Android Device Manager allows you to locate the physical location of your device and also:

- Lock and reset device password
- Make device ring
- Remotely erase all data on your device
- Navigate to **Settings ⚙ > Google > Security > Find My Device** > Switch ON: **Find My Device**

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

6. Password protect app purchases

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

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

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

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

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

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

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

SECURING YOUR ANDROID GOOGLE PIXEL AND PIXEL XL

Operating System: Android 9 Pie

Limit your potential exposure**1. Lock your device**

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

- Navigate to **Settings** ⚙️ > **Security & location** > **Screen lock** > Enter passcode (if prompted) > **PIN** > Enter a 6-digit passcode and confirm

Additionally, use Pixel Imprint if you prefer to unlock your Pixel with your fingerprint:

- Navigate to **Settings** ⚙️ > **Security & location** > **Pixel Imprint** > Follow activation steps

2. Limit information appearing on your lock screen

Android allows you to select the type of notification displayed on your locked Android device.

“Hide sensitive notification content” will limit the information about the sender and message contents:

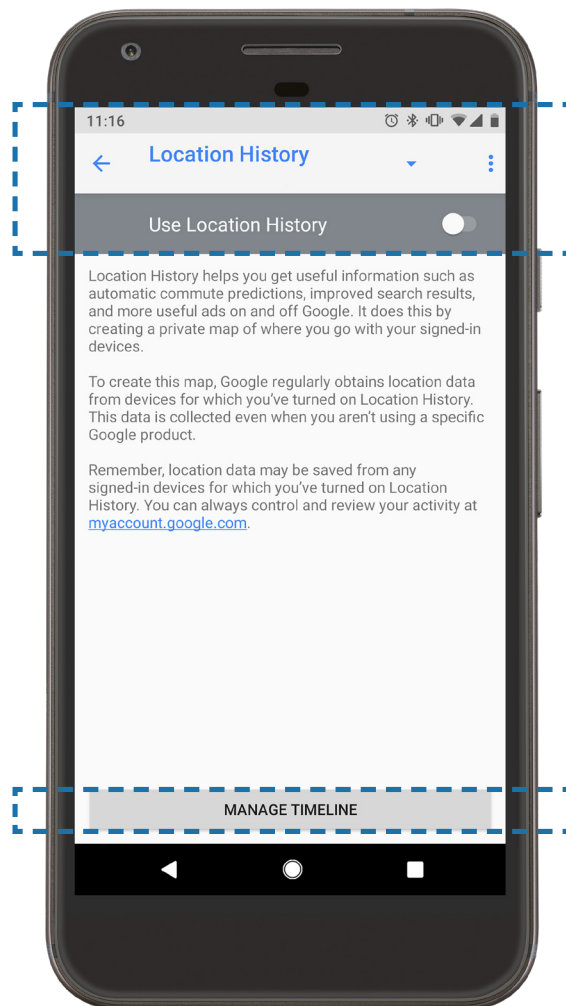
- Navigate to **Settings** ⚙️ > **Apps & notifications** > **Notifications** > **On lock screen** > **Hide sensitive content**

3. Disable tracking of your device

By default, Android tracks where you have taken your device. Disabling this feature will help protect you.

Disable Google Location History:

- Navigate to **Settings** ⚙️ > **Security & location** > **Location** > **Advanced** > **Google Location History** > **Switch OFF: Use Location History** > then select **Manage Timeline** > **Menu** ⋮ > **Settings** > **Delete all Location History**



4. Limit data tracking on your device

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

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

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

Find My Device allows you to locate the physical location of your device and also:

- Lock and reset device password
- Make device ring
- Remotely erase all data on your device
- Navigate to **Settings** ⚙ > **Google** > **Security** > **Find My Device** > Switch ON: **Find My Device**

Find My Device can be accessed via a web browser at:

<https://www.android.com/find>

6. Password protect app purchases

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

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

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

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

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

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

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

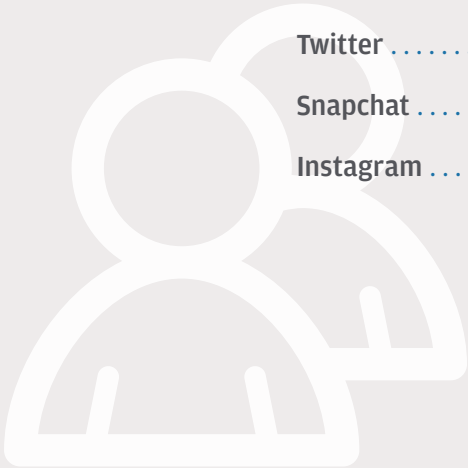
Securing your social media accounts

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

Social media safety guidelines

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

Facebook	35
LinkedIn	37
Twitter	38
Snapchat	39
Instagram	40



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

SECURING YOUR FACEBOOK ACCOUNT**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

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

1. Privacy (continued)

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

- **iOS and Android:** Navigate to **Menu ≡ > Settings & Privacy > 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

SECURING YOUR LINKEDIN ACCOUNT**1. Privacy**


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

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

SECURING YOUR TWITTER ACCOUNT**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

SECURING YOUR SNAPCHAT ACCOUNT**1. Privacy**

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



- **iOS and Android:** Navigate to the **Picture dropdown**  > **Settings**  > **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






SECURING YOUR INSTAGRAM ACCOUNT**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

Safeguards for **travel protection**

Protect yourself while traveling 43



*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.

Protect yourself while traveling

Whether traveling for business or pleasure, cyber threats are pervasive and exist beyond country borders. Your devices, which have made life so much more convenient, can be prime targets for hackers anywhere and anytime. They can contain or provide easy access to sensitive, confidential or financial information, so it is important to take precautions before, during and after your trip to ensure your data remains secure.

GENERAL TRAVEL GUIDELINES

When planning a trip, prepare well in advance

What do locations like New York's Times Square, Paris's Cathédrale Notre-Dame and Bangkok's Grand Palace have in common? They're extremely popular with travelers—and with cybercriminals who target them through unsecured Wi-Fi networks and other means. Before you go, ensure your devices' operating systems and anti-virus software are up-to-date. Password protect and encrypt all your devices, and back up your data prior to leaving so you have a recent copy. While traveling, avoid accessing your financial accounts from public computers and hotel, airport and other public Wi-Fi locations.

Learn about your destination's cybersecurity

Traveling to some countries may pose a higher risk due to known cybercriminal activity or potential state-sponsored surveillance. Before any travels, please check for guidance from your government authorities and law enforcement for recommended country-specific precautions.

Take only what you need

Consider leaving your devices at home when traveling to countries that may pose a higher risk to your information. Alternatively, consider taking a "loaner" phone, and have your phone calls and emails forwarded to them. If your loaner device is compromised, your exposure is limited to the data on that device rather than all the sensitive data on your primary device.

Think twice before booking travel plans through an unfamiliar site

Each year, travelers lose an extraordinary amount of money to phony bookings and travel-related scams. Because new domains are inexpensive and easy to procure, there is little stopping criminals from continuing to create fake sites that offer too-good-to-be-true deals. Use trusted travel and vacation-home rental services, and only message and send funds through the site's payment and messaging tools.

Keep your plans private

Do not post your intended travel plans, itinerary or location updates on social media prior to or during your trip. While you may enjoy sharing on social media, criminals can use your posts to determine when you are out of town and likely out of your routine, and not as attentive to your online safety.

Traveling to remote areas

In case your mobile device or GPS is not available, consider keeping hard copies of vital documents and maps on hand.

Prior to your trip

Inform yourself not just about visa, travel and physical safety considerations, but also the cyber safety precautions you should take prior to the trip, including the transit hubs and locations you will pass through before reaching your final destination.

Secure your devices

- **Upgrade to the latest operating system** release on your computer and mobile devices
- **Install reputable anti-virus and ad-blocking software**, and ensure they auto-update so that you are using the latest version
 - Strongly consider installing a mobile security application like *Lookout Security* tools, which can help monitor your devices for potentially malicious activity, even during your trip
- **Install a reputable Virtual Private Network (VPN) app** on your personal devices, so that you can use it throughout your travels and have it in place before it is needed

Note: Certain countries do not have outright bans on VPNs, but may have Internet censorship laws that can make it risky to use such a service. Research before you go.
- **Back up your computer and mobile devices** – including your phone – to a secure external hard drive or to an encrypted cloud storage service
- **Password protect all devices**, including laptops, phones and tablets
 - Consider encrypting devices and files using built-in or trusted third-party encryption tools
- **Consider disabling backups before entering any country that may pose a risk to device security.** With backups disabled, no personal data on your device will be backed up until it is turned back on (including pictures, videos, messages and notes)
 - To turn off iCloud (Apple devices): Tap **Settings** > **[Your name]** > **Sign out** (at bottom of page)
 - To turn off Google Drive backup (Android devices): Tap **Settings** > **System** > **Backup** > Turn off **Backup to Google Drive**

Pack copies of all important documents, such as passports, identification and health insurance cards, and avoid carrying the originals if possible

Consider purchasing radio-frequency identification (RFID) protective gear (e.g., wallets and document sleeves) to protect credit cards, passports and other sensitive documents from RFID skimming; wrapping items in aluminum foil or placing them in metal tins might afford some protection

Record contact information for key contacts, such as your financial institution, local embassy in each country you are visiting, law enforcement, etc., separately from your devices

Inform your financial institutions if you are traveling out of the country. This will ensure that your credit card transactions are not declined and your institution can monitor for suspicious activity

During your trip

Dangers are present, even if you may not see them. Be aware of your surroundings, as well as how and when you connect to the internet.

- **Use your mobile phone carrier's network** whenever possible; avoid using public Wi-Fi at hotels, airports, cafes and planes, as they are more likely to be compromised or spoofed. Do not assume a public network is legitimate or secure
- **Use a Virtual Private Network (VPN)** on your device to help communicate and browse securely if you are using public or hotel, airport, or other Wi-Fi
 - *The following countries have either blocked or passed laws prohibiting the use of VPNs: Belarus, China, Iran, Iraq, Oman, Russia, Turkey, Uganda, United Arab Emirates, Venezuela¹*
- **Make sure your devices do not auto connect to Wifi, Bluetooth and other technologies.** Disable Wi-Fi, Bluetooth, AirDrop and other wireless technologies when not in use
- **Power off all devices when not in use** or when being handled by others (e.g., at customs) to help prevent unobtrusive access to the data on your devices
- **Limit the use of third-party applications** during your travels, especially if you are not sure how your information is stored, or how it might be accessed or shared
- **When renting a car, use a personal device for navigation instead of an in-car system.** If using the car's system is not avoidable, delete your entries before returning the car, as data about your destinations could potentially be stored and accessed in the future
- **Avoid plugging USB devices into anything but your own equipment,** including charger devices via USB plugs in hotels and public spaces. USB docking stations could be used to load malware onto your devices
- **Beware of people "shoulder surfing."** It can be very easy for others to see or record information you are viewing, typing into your device or saying to someone else, including passwords and account information

IF YOUR DEVICE IS LOST OR STOLEN

To protect your information in the event your device is lost or stolen:

- Take necessary precautions to keep information more secure by adjusting security settings on all devices
- Consider enabling a mobile security application, such as *Lookout*
- Change your account passwords (e.g., email, social media)
- Report lost or stolen devices as soon as possible to all necessary financial, law enforcement and government institutions

After your trip

If you believe your device has been compromised or if it is acting suspiciously, immediately reset laptops and mobile devices to their factory settings, which will erase all data. If you have made the device backups prior to your trip, you can restore the data.

¹ Proton VPN, October 2018. <https://protonvpn.com/blog/are-vpns-illegal>

*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.

Tips for fraud prevention

Securing your credit 49

Keep yourself safe from fraud 51

Fraud scheme: Invoice fraud 53



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

Securing your 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
800.349.9960
www.freeze.equifax.com

Experian
888.397.3742
www.experian.com/freeze

TransUnion
888.909.8872
www.transunion.com/freeze

Place a fraud alert

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

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

Three types of fraud alerts are available:

- **Initial Fraud Alert:** Principally designed for, but not reserved to, individuals who feel their identity has been compromised. Initial Fraud Alerts last one year from the date issued, are free of charge and can be continuously renewed
- **Extended Fraud Alert:** Reserved exclusively for victims of identity theft and designed to protect your credit for seven years
- **Active Duty Military Alert:** Reserved for military personnel who want to protect their credit during deployment. Alerts last for one year and can be renewed

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

Equifax
888.766.0008
www.equifax.com/CreditReportAssistance

Experian
888.397.3742
www.experian.com/fraudalert

TransUnion
800.680.7289
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
www.equifax.com/personal/credit-report-services

Experian
www.experian.com/fraud/center.html

TransUnion
www.transunion.com/freeze

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	<p>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.</p> <p>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.</p>	<p>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.</p>
Social Engineering	<p>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</p>	<p>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.</p>
Wire and ACH Fraud	<p>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.</p>	<p>ACH fraud occurs when an account is accessed for unauthorized ACH payments (debits).</p>
Online Banking Fraud	<p>Online banking fraud occurs when malicious software, also known as malware, is installed on your computer. Through viruses, keystroke loggers, ransomware or</p>	<p>other types of malware, fraudsters gather confidential account credentials and financial information.</p>
Remote Access	<p>Fraudsters can gain remote access to your computer through malware or phishing attempts claiming to be reputable virus protection providers. With this access,</p>	<p>fraudsters can take over your computer and complete transactions without your knowledge.</p>

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!

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, @deancoLLC.com can appear similar to a known vendor @cleancoLLC.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.

How J.P. Morgan **helps protect you**

Corporate IT Risk and Security
Management Program 57



*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.

May 2019

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. CTC is a global team responsible for the intelligence-driven delivery and operations of Cybersecurity and Technology Controls that enable us to manage within the risk profile and to help our employees, developers and customers to do the right thing.

How We are Governed

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

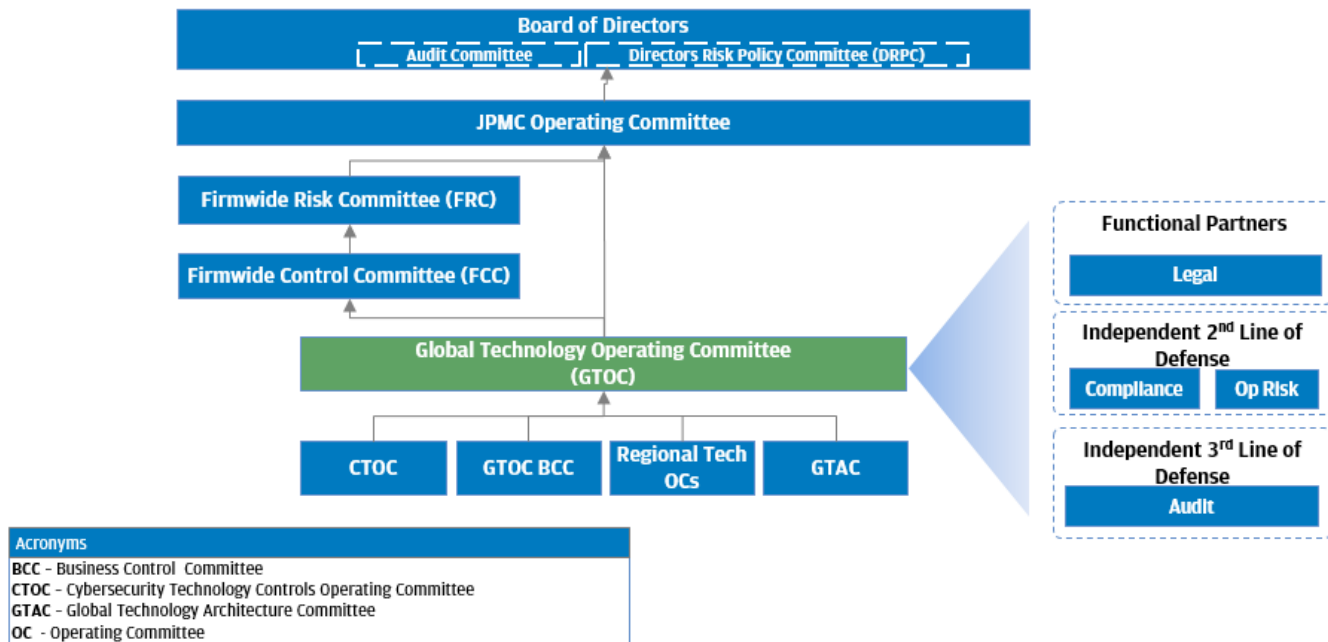
The technology governance structure is designed to identify, escalate, and mitigate information security risks. This structure uses key governance forums to disseminate information and monitor technology efforts.

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.

JPMC’s Information Security Program is overseen by the Firm’s Board of Directors as illustrated below:



How the Program is Implemented

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

1. Governance and Controls

With the accelerating change in technology and an increasingly sophisticated cyber threat landscape, it is critical that the Firm continues to effectively govern existing and emerging risks in a systematic manner consistent with the risk appetite and tolerance of the Firm’s senior management. Governance and Controls provides the framework and capabilities to achieve that objective. The framework covers the domains of Govern, Identify, Control, Assess and Measure, and Treat which are further detailed below:

- Govern – Ensure proper oversight of our technology risk through a clear risk management strategy which supports the Firm’s risk appetite, robust governance and reporting processes, and effective regulatory, audit and client engagement processes
- Identify – Define and execute the comprehensive processes for identifying risks
- Control – Protect the Firm by establishing appropriate policies, standards and control procedures
- Assess and Measure – Measure compliance to our control requirements by establishing assessment and continuous monitoring capabilities
- Treat – Manage control performance and risk exposure through prioritized remediation

2. Cyber Defense and Fraud

The Cyber Defense and Fraud (CD&F) function build, enhances, and sustains strategic cybersecurity controls to detect and defend the bank against Cyber Attack. The suite of CD&F capabilities includes Network, Endpoint and Email Security, Security Event and Incident Management, Data Loss Prevention, Digital Forensics, Fraud and Threat Intelligence, Vulnerability Management, Operational Assessments, and Connectivity Assurance.

3. 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. Control procedures include dual approvals for privileged access and separation of approval and fulfilment for the same access request.

4. Data Management, Protection and Privacy

JPMC recognizes data as foundational to all aspects of daily operations, and as a key enabler to our ability to serve clients, manage risk, ensure regulatory compliance, and make informed strategic decisions. CTC is accountable for designing and governing controls to ensure confidentiality, integrity, and availability of data throughout its lifecycle from collection to disposal to enable all aspects of existing businesses and to reveal new opportunities.

5. Technology Resiliency

The Technology 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.

6. Software and Platform Enablement

The Software and Platform Enablement function simplifies software and platform security to enable software engineers and operations teams to develop, implement and run secure applications that deliver exceptional client and employee experiences.

The Software Enablement team is focused on enabling our people, optimize our processes and protect our technology through the strategic drivers of using threat intelligence, business context, data driven insights and the right tools and integration to unlock business value. Our aim is to automate where possible, increase development speed, increase security and reduce risk across the lifecycle and to the firm. Capabilities include secure application design and build, test and deploy, enterprise services, application security assessments and operations, and mobile security.

7. Security, Investigation and Crisis Management

Global Security and Investigations (GS&I) organization is responsible for the security for the Firm. The Physical Security, Business Resiliency, Global Investigations, Global Workforce Screening and Crisis Management programs, managed by the GS&I, are designed to collectively protect employees, clients and our assets from external and internal threats.

As part of that protection, GS&I coordinates firmwide responses to global and regional crises plus controls physical access and conducts surveillance monitoring at JPMC locations including computer facilities that contain critical systems and confidential information. GS&I also screens employees and potential news hires. Screening activities include fingerprinting and background checks on all U.S.-based employees as well as those who are responsible for, or have access to, JPMC customer information, premises or systems. GS&I Investigators examine internal and external fraud incidents including employee wrongdoing, to identify not only root causes and impact but also corresponding remediation solutions.

8. Global Privacy Incident Management

The Global Privacy Office (GPO) 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 Team Managers (IRTMs), and the support functions surrounding the minimum requirements that must be addressed in privacy incident response procedures.

Core responsibilities of the GPO include:

- Maintaining the Privacy Incident Program including the Policy, Privacy Incident Standards and global guidance materials;
- Developing and disseminating reporting on firmwide potential incidents and breaches, including privacy breach and incident metrics for the annual Gramm-Leach-Bliley Act (GLBA) board report;

- Providing firmwide guidance, training and reporting criteria for Incident Response Teams to include in procedures

9. 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.

10. Global Information Management (GIM) – Records Management

GIM supports the Firm's record retention program by working with internal and external counsel to maintain the record retention schedules according to the laws, regulations and standards in the countries in which the Firm conducts business.

GIM guides and educates staff on record management compliance issues through awareness programs, procedures, internal training and serves as a contact point for record retention, record disposition and questions from staff members.

In partnership with Legal, GIM maintains the Firmwide Records Management Policy, which establishes the principles for the Firm's record retention program. GIM also maintains firmwide procedures for records disposition and records management. These documents guide staff on the appropriate implementation of related laws, regulations and standards.

11. Training and Awareness

Information Security Training and Awareness is supported by the Cybersecurity and Technology Controls organization to ensure ongoing communication with regional and business representatives.

- The Security Education and Awareness program offers live, virtual and computer-based training to all IT risk and controls practitioners across the Firm.
- Our Global Privacy Program requires all employees to take annual awareness training on data privacy. The training includes information about confidentiality and security, as well as responding to the unauthorized access to, or use of information.
- Cybersecurity training is mandatory for all employees globally. The training is based on the Firm's cybersecurity policies and standards, and it is supplemented by a firmwide cyber awareness program and testing initiatives, to include quarterly, firmwide phishing tests.

- Employees who do not pass phishing tests are notified immediately with a policy reminder and available resources to improve their ability to recognize social engineering. Repeat offenders are assigned additional training with escalation paths through the employee compliance.

Information Security is a Shared Responsibility

At JPMorgan Chase, we take seriously our role in protection of our customers' data and implement the aforementioned capabilities, processes, controls and technology solutions to safeguard it. 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.



Jason Witty

Managing Director

Chief Information Security Officer

Head of Cybersecurity and Technology Controls

*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 LastPass, DashLane, 1Password, Alphabet, Yahoo, Microsoft, AOL, Apple, Lookout, Samsung Electronics, Facebook, LinkedIn, Twitter, Snap Inc, 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.