citi Wealth

# Personal safety and security

## A comprehensive guide

# Contents

# Introduction

The importance of maintaining personal privacy and security has grown exponentially for wealthy individuals and their families in an era of accelerating technological change and continuously emerging and expanding threats. A robust security strategy and understanding of the evolving threat landscape is essential to proactively protect themselves, their families and their assets.

This white paper guides individuals, families and family offices in enhancing personal safety and security, including online safety, personal device safety and personal physical security. We also explore evolving threats and offer practical tips and strategies to mitigate risks, drawing on insights from recent industry research and best practices.

Effective risk mitigation involves understanding threats, implementing preventative measures, and building resilience to respond to inevitable incidents. For wealthy individuals, the efficacy of such mitigations depends on the resilience of an entire ecosystem, including themselves, their family members, their family office, and even personal and household staff.

Education, communication, and buy-in are critical for all stakeholders within this broader network to continuously and effectively mitigate security threats. Personal safety and security should be prioritized not only to safeguard physical well-being, but also because neglecting personal, online, or device security can lead to broader risks, including cyberattacks and fraud. Our goal is to empower all members of the family ecosystem with the knowledge and tools necessary to build resilience, maintain vigilance, and safely navigate an ever-evolving global physical and digital security environment.

# Comprehensive online safety

Personal and professional lives are digitally intertwined, and robust personal online safety is crucial for safeguarding individuals in the family ecosystem.

**General online hygiene best practices**
Individuals and families should adopt core practices to minimize their digital footprint and exposure.

- **Limit public sharing of personal details:** Avoid publicly sharing real-time locations, travel dates, home addresses, or identifying characteristics of your home on social media. Such information can be used to locate you.
- **Lock down social media privacy settings:** Review and tighten privacy controls on all social media platforms. Restrict profile visibility to trusted contacts only and manage your username and avatar carefully.
- **Minimize geotagging and be alert for hidden metadata:** Turn off automatic geotagging on your smartphone's camera and all social media applications to avoid unintentionally disclosing your location. Regularly check applications and social media posts for metadata that might betray locations and other personal details.
    - Be aware that some metadata, especially within pictures, might be hidden, but can still be accessed if images are downloaded. Check camera settings before taking pictures and scrub metadata before sharing images, videos or audio.
- **Be discreet about family member locations and activities:** Avoid sharing sensitive details like school names, sports teams or specific schedules of family members online. This information can be exploited by data brokers and threat actors.
- **Practice safe file sharing:** Use encrypted cloud services or secure file transfer tools for sensitive documents; never use public file-sharing links. Always verify if the recipient has received the file and can access contents. Consider services such as Microsoft OneDrive, Proton Drive or Dropbox.
- **Avoid phishing and malware scams:** Do not click on suspicious links or open attachments from unknown senders; keep anti-virus software up to date and purchase malware scanners for home network.
- **Educate and train family members and staff:** Ensure all family members, especially children, and staff are aware of online safety best practices, social media security, and how to identify and avoid scams. This includes awareness of scams that specifically target teenagers and young adults, such as sextortion and other blackmail schemes. Individual digital habits can create vulnerabilities for the entire family.

**Managing your digital footprint**
Data brokers are companies that collect and sell personal information compiled from thousands of public sources (social media, credit card data, web history, public records), making it easily searchable People-finder companies offer detailed background reports on individuals containing contact information, addresses, properties, and court and criminal records. Removing data from these sites helps to mitigate personal privacy and safety risks.

Key protective measures:

- Use subscription-based data deletion services.
- Engage services like DeleteMe or 360 Privacy to actively find and request the removal of your information from data broker and people finder sites on your behalf.
- Remember, these services may not remove all instances of your information.
- Include family members in this process as threat actors often leverage these connections.
- Removable information typically includes names, family details, occupation, addresses, social media presence, phone numbers, email addresses, marital status and property data.

Manually removing your information:

- Search data broker sites (e.g., Equifax, TransUnion, Experian, US Phone Book, White Pages, Veripages) for your information, verify it and follow the site's opt-out procedures.
- Be prepared to provide personal details for verification.

**Navigating social media safely**
Social media platforms are an undeniable part of daily life, demanding a deliberate and secure approach to protect privacy, security and reputational integrity.

- **Control visibility:** Control who can see posts and photos by setting posts to "friends only" and regularly checking that unknown or unwanted parties do not have access.
- **Limit connections:** Restrict who can contact you on social media.
- **Delete unused accounts:** Remove accounts that are no longer in use.
- **Understand privacy policies:** Review platform policies to identify whether information is shared with third parties. Be aware that "friends only" posts can still inadvertently be public. See **Figure 1** for definitions of common privacy terms.
- **Regular review:** Periodically check security and privacy settings as platforms change options.
- **Be mindful of posted information:** Avoid sharing sensitive personal details like addresses or daily routines.
- **Education and communication are key:** Educate family members and staff on social media security. Maintain awareness of individual and family member accounts to prevent vulnerabilities.

FIGURE 1. COMMON PRIVACY TERMS

| Privacy term | What it means | Safety implications |
|---|---|---|
| **Data collection** | Platforms gather personal details (profile information, posts, browsing history, device and often location data) | More data collected results in higher risk of tracking, profiling or leaks. Users should limit optional information shared (e.g., birthdays, contacts, precise location). |
| **Cross-platform data sharing** | Data is shared across apps owned by the same company (e.g., Meta, Google) or with business partners | An action in one application can have impact on profiles across several connected apps. It is important to review linked accounts and adjust ad settings. |
| **Advertiser access** | Collected data is sold/shared with advertisers to target ads | Creates digital profiles that may feel invasive. Users should manage ad preferences and limit tracking permissions. |
| **User data control** | Ability to download/export your data and delete your account/history | Offers some transparency but deletion is not always complete as logs or backups may persist. Always assume some residual data remains in the application. |
| **Personalized ad targeting** | Ads are tailored using browsing habits, interests, location, or even career information | Improves the relevance of ads but increases surveillance risk. It is safer to turn off location-based ads regularly. |
| **Ephemeral content & retention** | Some posts auto-delete (e.g., Snapchat Snaps) but metadata is often retained | Provides a false sense of privacy, as even if a post "disappears," companies may keep records. Screenshots can also bypass deletion. |
| **Federated / decentralized privacy** | Privacy rules depend on the server or community, not one company | Gives users more control but rules vary widely. Users should check their server's specific retention/sharing policies. |
| **Law enforcement / third-party requests** | Data can be shared with authorities or partners if legally required | Any data may be accessible, including private messages. |

**Geolocation and social media exposure**
Fitness platforms like Strava and MapMyRun and other location-sharing applications often collect and share geolocation data which can be leveraged by threat actors. Platforms and applications that enable pattern of life analysis, facility mapping, travel disclosures and other details can facilitate targeted robberies, harassment, protests, kidnappings and other threats. This seemingly innocent data can be aggregated to build comprehensive profiles of an individual's movements and habits.

Key protective measures:

- **Review application privacy settings:** Regularly audit and tighten privacy settings on all fitness, social media and location-sharing applications. Ensure location data is only shared with trusted contacts or disabled. Understand how each application collects and uses data.
- **Disable geotagging by default:** Turn off automatic geotagging on your smartphone's camera and all social media applications. Manually remove location data from photos before sharing.
- **Practice data and information discretion:** Avoid publicly sharing real-time location data, detailed travel plans (past or future) or routines (e.g., daily runs, school drop-offs) publicly on social media or applications.
- **Educate family members:** Ensure all family members, especially children and young adults, understand location data risks and application settings. Foster open communication about digital practices and privacy awareness within the family to protect overall safety.

**Recognizing and avoiding social engineering**
Social engineering is a manipulative tactic used by threat actors to deceive victims into granting access to computer systems or divulging personal or financial information.

Key protective measures:

- **Identify common indicators:** Look for suspicious sender addresses, unexpected attachments, generic greetings and signatures, misspellings, inconsistent formatting, spoofed hyperlinks, and poor grammar.
- **Be suspicious:** Be wary of unsolicited calls, visits or emails requesting internal information.
- **Verify authority:** Do not provide personal or organization details unless certain of the requestor's authority and legitimate need.
- **Check website security:** Always verify website security before submitting sensitive information online. Make sure the URL begins with "https://" and check the padlock or tune icon in the address bar to verify that the connection is encrypted. Additionally, inspect the icon to verify that the SSL/TLS certificate is valid, not expired, and issued to the correct organization.
- **Avoid suspicious attachments:** Never open email attachments from unverified sources.

**Identifying and preventing executive impersonations**
Executive impersonations involve threat actors creating fake social media or email accounts that appear to belong to an executive. These impersonations require minimal personal information (often just a name and public photo) but can lead to reputational damage, financial loss, misleading clients or the public, and incurring legal and regulatory consequences.

Key protective measures:

- **Monitor social media:** Routinely monitor platforms for imposter accounts targeting family members and family office personnel.
- **Verify authenticity:** Executives should consider maintaining a verified public LinkedIn profile with their work email address to help discern impostor accounts.
- **Add disclaimers:** Include a disclaimer on public LinkedIn profile stating, "I do not make contact through any other social media accounts; if you are contacted by me on another platform, the contact is fraudulent."
- **Adjust privacy settings:** Limit publicly available information by adjusting privacy settings on all social media profiles.

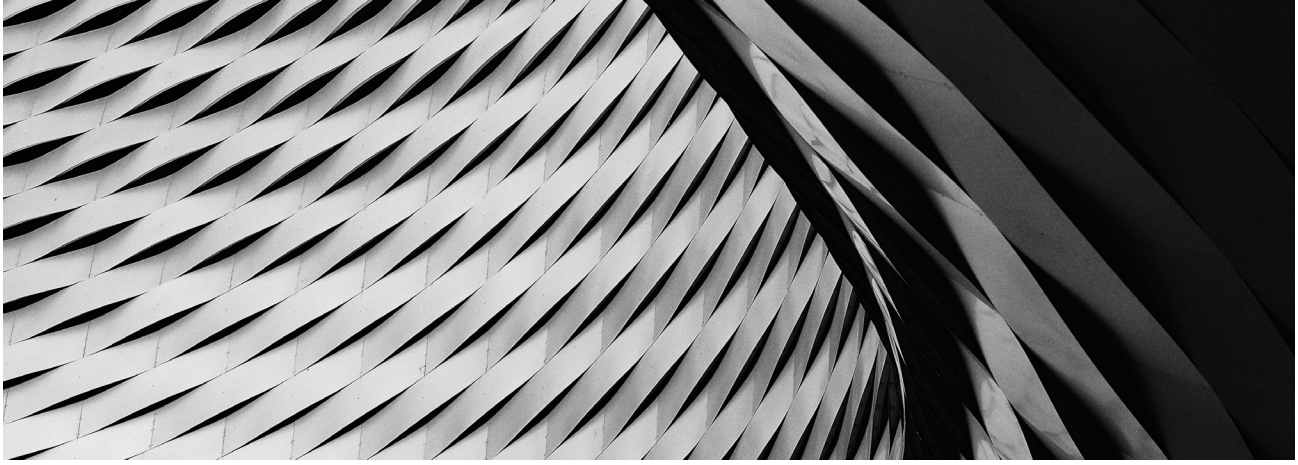
**Understanding and avoiding QR code scams**
Scammers exploit QR codes by placing fraudulent codes in public places including restaurants, transportation hubs and parking meters or by sending them via mail or email, often spoofing legitimate organizations. Scanning these fake codes can compromise personal data or install malware.

To avoid QR scams:

- **Preview URLs:** Always preview the URL before scanning a QR code; a preview link should appear on your device, allowing you to inspect the destination link for legitimacy. To verify whether a URL is legitimate, ensure the URL begins with "https://" and look carefully for misspellings, extra words, special characters, or slight variations that could indicate a fake or malicious site.
- **Check for tampering:** Physically inspect public QR codes for signs of alteration or overlaying stickers.
- **Verify sender:** If a QR code is unsolicited via text or email, confirm its legitimacy directly with the sender and check for spoofing.
- **Avoid unknown QR codes when possible:** It is generally safer to refrain from scanning unknown QR codes; instead, manually visit the intended website.

If you fall victim to a QR code scam:

- **Change passwords:** Immediately change passwords if login information was entered on a fraudulent site after scanning a QR code.
- **Contact financial institutions:** Inform financial institutions if financial details were compromised.
- **Report the scam:** Report suspected QR code scams to the Federal Trade Commission via its official website.



# Securing personal devices and accounts

Personal devices and online accounts are prime targets for cyber threats and implementing security measures is crucial for all family members.

**Robust account authentication**
Strong authentication is the cornerstone of account security for personal and professional accounts.

Implement strong passwords and passphrases:

- **Password managers:** Use a password manager to generate and securely store unique, randomly generated passwords for each account.
- **Strong passwords:** All passwords should be at least 12 characters, incorporating numbers, symbols and mixed-case letters.
- **Change defaults:** Immediately change default passwords on new devices and services.
- **Avoid personal information:** Do not use passwords based on personal information, family names, or frequently used words.
- **Longest possible:** Use the longest password or passphrase permissible by each system.
- **Passphrases:** Consider using passphrases (e.g., "h0ney-Br1cks-bored-conci5e") with mixed case letters, numbers and symbols for enhanced strength.
- **Unique passwords:** Ensure every account has a unique, complex password to prevent cascading compromises. Password managers can audit for repeated and compromised passwords.

Leverage multi-factor authentication (MFA):

- **Enable MFA everywhere:** Enable MFA on all online accounts, including email, social media and financial platforms. MFA is a multi-step login process designed to enhance account security by requiring more than just a password. For instance, in addition to a password, users might need to provide a code received via email or text, approve a push notification from a mobile app, enter a code from an authenticator app, answer a security question, or use a fingerprint scan. This secondary layer of authentication significantly helps to prevent unauthorized access, even if a system password has been compromised.
- **Prioritize phishing-resistant MFA**
  - **Hardware MFA:** Use physical security keys utilizing FIDO standards for the strongest protection, especially for critical accounts.[1]
  - **App-based MFA:** Use authenticator apps (e.g., Google Authenticator, Okta Verify, Microsoft Authenticator) for time-based one-time passkeys.
  - **Avoid SMS/voice MFA:** Use SMS or voice MFA only if absolutely necessary, as these methods are more vulnerable to interception.
- **Passkeys:** Adopt passkeys where supported, as they offer faster, easier and more secure sign-ins that are highly resistant to phishing by using public key cryptography.

[1] The FIDO Certified Showcase highlights FIDO Alliance members and their FIDO Certified solutions

- **Consistency is key:** Consistent adherence to strong authentication practices across all accounts is a fundamental cybersecurity best practice.

**Device and system security**
Keeping devices and their software updated and secure is fundamental.

Maintain system and software updates:

- **Enable automatic updates:** Ensure automatic updates are enabled for all operating systems (on phones, tablets and computers), applications and internet browsers to receive the latest security patches and features.
- **Replace end-of-life devices:** Prioritize replacing devices that have reached end-of-life and no longer receive manufacturer updates to avoid critical, unpatched vulnerabilities.
- **Regular restarts:** Turn your phone off and on at least once a week to reduce the risk of unauthorized access, data leaks and hacking attempts. Restarting your phone can effectively disrupt and eliminate certain types of malware, particularly those residing in temporary memory, thereby mitigating further harm and preventing continued data leakage.

Implement data protection and privacy:

- **Regular data backups:** Create regular backups of all essential data from devices. Store backups separately from the source systems, ideally in a secure cloud environment or offsite. Visit Apple Support and Microsoft Support for guidance on iCloud and OneDrive cloud backup services.
- **Encrypt devices:** Encrypt all devices (laptops, smartphones) and sensitive data stored on them. Visit Apple Support and Microsoft Support for guidance on device encryption.
- **Review mobile application permissions:** Regularly review and adjust privacy settings and permissions. Grant access judiciously, as many applications request unnecessary access (location, camera, microphone, texts, contacts). Revoke unneeded permissions.

Utilize advanced protection programs:

- **Google's advanced protection program:** Designed for high-visibility users with sensitive information, this program requires a passkey or security key for login, preventing unauthorized access even if the username and password are known. It also limits access to Google applications and verified third-party applications, blocks harmful downloads, and only permits application downloads from verified stores.[2]
- **Apple's advanced data protection:** This optional setting provides end-to-end encryption for most iCloud data (including Notes, Photos and iCloud Backup). This ensures that even Apple cannot access this data, enhancing security even during cloud breaches.[3]

**Browser best practices**
Web browsers are a primary interface for online activity; secure browsing is essential.

Stay updated:

- **Keep browsers updated:** Regularly update browser software and review its security settings.
- **Disable pop-ups:** Disable pop-ups to prevent malicious software execution.

Enhance privacy and security settings:

- **Private browsing:** Utilize your browser's private-browsing or do not track features to prevent information from being saved to your device.
- **Privacy-focused search engines:** For enhanced privacy, consider using a search engine like DuckDuckGo or Brave Search, which does not track your searches or collect personal data.
- **Limit browser extensions:** Install browser add-ons, plug-ins, toolbars and extensions sparingly, especially those from unreputable sources as they can pose privacy and data security risks.
- **Reject third-party cookies:** Reject third-party tracking cookies when possible to mitigate security and privacy concerns and limit online activity tracking.
- **Always use secure protocols:** Ensure websites use "https" (indicated by a padlock icon in the URL bar) for encrypted communication.

[2] https://landing.google.com/advancedprotection
[3] https://support.apple.com/en-us/108756

**Defending against spyware**
Spyware is a type of malware that, once installed, collects sensitive personal data, logs keystrokes, and captures login credentials. It commonly spreads through malicious links from phishing campaigns, click bait ads or fraudulent QR codes.

Signs of a spyware infection:

- Your device runs significantly slower than usual.
- You experience unexpected system crashes.
- Frequent pop-up warnings or error messages appear.
- Your device inadvertently warns of low hard drive space.
- Your internet browser's homepage has changed, or new, unadded toolbars or plugins appear.
- Unfamiliar program icons appear on your device.

Protecting from spyware:

- **Avoid suspicious communications:** Do not open unsolicited email attachments or click suspicious links in text messages.
- **Use reputable antivirus software:** Install and regularly update reputable antivirus and anti-spyware software with real-time protection.
- **Install applications from trusted sources only:** Download and install applications from only official application stores or directly from trusted device manufacturers.
- **Employ pop-up blockers:** Use a pop-up blocker in your web browser and avoid clicking on any suspicious pop-up advertisements.
- **Keep systems updated:** Regularly update your computer and mobile operating systems and all software, as this is a core cybersecurity best practice against malware and spyware threats.
- **Regular restarts:** Turn your phone off and on at least once a week to reduce the risk of unauthorized access, data leaks and hacking attempts.

**Wi-Fi and network best practices**
Your home network is a key defense layer; configure it securely. Use caution on all outside networks.

Public Wi-Fi best practices:

- **Avoid unsecured public Wi-Fi:** Use public Wi-Fi with extreme caution. Connecting to websites that do not use "https" is especially risky on public networks. Connecting to secured public networks is always preferable.
- **Use a virtual private network (VPN):** When using any public Wi-Fi, use a trusted VPN service to encrypt all network traffic.

Router best practices:

- **Change default password:** Immediately change your Wi-Fi router's default password as these are widely known and create vulnerabilities.
- **Update firmware:** Regularly update your router's firmware to apply critical security patches.
- **Use strong encryption:** Ensure your Wi-Fi network and any guest networks use WPA2 or WPA3 encryption.
- Disable unnecessary features: Disable guest networks and port forwarding if not specifically required.

Network segmentation and monitoring:

- **Dedicated Internet of Things (IoT) network:** Connect all smart home and other IoT devices to a dedicated, separate network to isolate them from primary devices with sensitive data.
- **New device alerts:** Enable router or network management alerts for new device connections to your network.
- **Access controls:** Implement strong network segmentation and access controls to safeguard sensitive data and operations.

# Prioritizing physical safety

Physical security remains critical for overall safety, especially for high-profile individuals and their family members. Digital and physical security are often linked, necessitating attention to physical risks to digital infrastructure, including access. For traditional physical security and personal safety, situational awareness is key, particularly in unfamiliar places. Travel for wealthy individuals, whether for business or leisure, carries unique security concerns due to increased visibility and potential for targeting.

**Personal movement and situational awareness**
Maintaining situational awareness when moving can significantly reduce risks.

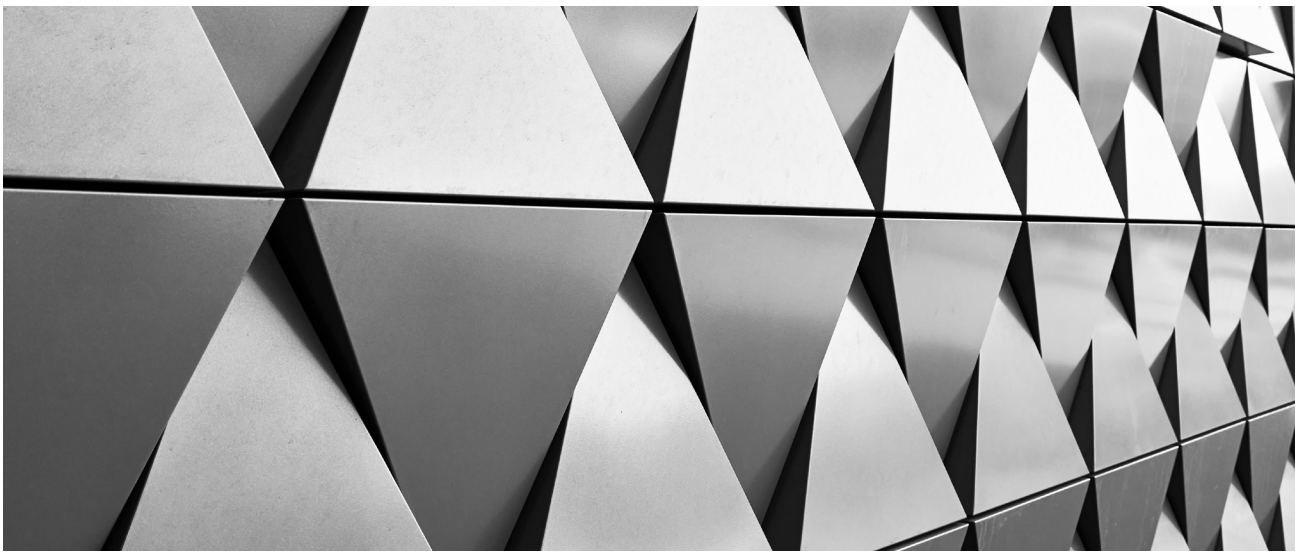
- **Choose populated routes:** Opt for well-populated, well-lit streets; walk in groups in desolate areas.
- **Avoid isolation:** Avoid deserted blocks; head towards public spaces or open stores.
- **Ensure safe entry:** If driven home, have the driver wait until you are safely inside.
- **Respond to threats:** If bothered while walking, reverse direction. If still followed, seek safety and yell for help if possible.
- **Vary routines:** Avoid predictable routines and routes to deter potential targeted attacks.
- **Maintain a low profile:** When traveling, avoid overt displays of wealth (e.g., expensive jewelry, luxury vehicles). Opt for understated attire and transportation. Only use trusted vendors for travel and clear details with security staff.
- **Be mindful of social media exposure:** Limit or avoid real-time posting of activities and locations. Threat actors use social media to identify and monitor targets.

**Managing crowds and public gatherings**
Public events and large gatherings can pose risks if not approached cautiously.

- **Avoid volatile situations:** Steer clear of protests or demonstrations that may turn violent.
- **Be alert to abandoned items:** Move away from abandoned items (e.g., bags) and alert authorities immediately.
- **Observe behavior:** Be aware of others' behaviors. If these behaviors could provoke violence, move away.
- **Assess carry-ons:** Note items people are carrying that could be dangerous or instigate violence.
- **Pre-event security assessments:** For high-profile family members, consider professional security assessments of public event venues.
- **Emergency exits:** Identify emergency exits and rally points upon arrival at any venue.

**Travel security for wealthy individuals and families**
Travel, particularly international travel, introduces unique risks that require specific planning and precautions.

- **Pre-travel briefings:** Conduct thorough briefings for family members and accompanying staff, covering local risks, cultural sensitivities and emergency protocols.
- **Threat assessments:** Engage security professionals for country-specific threat assessments evaluating crime rates, political instability and health risks.
- **Secure transportation:** Arrange secure, pre-vetted transportation, including armored vehicles if necessary, and professional, security-trained drivers.
- **Vetted accommodation:** Use only vetted hotels, residences or private accommodations with robust security features. Conduct physical security sweeps for private residences.
- **Local support networks:** Establish contact with local security liaisons, consulates or trusted fixers who can provide assistance in an emergency.
- **Digital security while traveling:** Assume all public Wi-Fi is insecure. Use a VPN at all times. Be cautious with personal devices and avoid accessing sensitive information on public computers.
- **Kidnap and ransom planning:** For extreme risk environments, consider specialized kidnap and ransom insurance and professional training for family members.
- **Emergency contact plan:** Ensure all family members and staff have an accessible emergency contact plan with international communication capabilities.



# Emerging threats

The modern threat landscape continues to evolve, as threat actors take advantage of new technologies and trends to carry out physical threats, kidnapping, fraud, extortion and sophisticated cyberattacks.

**Cryptocurrency-related threats**
Recent reports highlight a significant increase in threats targeting cryptocurrency executives and individuals holding significant cryptocurrency assets. These heightened risks include targeted cyber intrusions, physical extortion, violent robberies and insider compromise. The decentralized and often pseudonymous nature of cryptocurrency transactions can make it difficult to trace related crimes, making these individuals particularly vulnerable.

Key protective measures:

- **Enable strong authentication:** Vigilant account management is especially critical when dealing with cryptocurrency assets. Always enable multi-factor authentication (MFA) on all cryptocurrency exchanges and wallet services. Prioritize app-based authenticators over SMS.
- **Exchange security:** Only rely on trustworthy exchanges with robust controls and partner with trusted security vendors to ensure added protection.
- **Avoid publicizing holdings:** Avoid disclosing the extent of your cryptocurrency wealth or transactions publicly, especially on social media. Avoid discussing in public or with individuals who do not have a need to know.
- **Be skeptical of offers:** Be wary of unsolicited investment opportunities involving cryptocurrencies. Verify all offers independently through trusted sources before committing any funds.
- **Physical security in the cryptocurrency ecosystem:** When dealing with large sums or high-value assets, ensure your personal physical safety is prioritized and consider professional security advice, especially when traveling or attending cryptocurrency-related events. Threat actors may also physically target infrastructure and technology related to cryptocurrency holdings such as wallets, servers, and even hand-written. keys. Be wary of sharing information online or in person about infrastructure specifics.

**Generative AI deepfakes**
The advent of generative AI has introduced a new threat: deepfakes. Threat actors can now use sophisticated deepfakes to target staff and family members to gain access to data or sensitive information. This includes the creation of synthetic video calls or voice clones for kidnapping threats, offering false proof of life, making them increasingly difficult to detect. These AI-driven threats increase the risks of reputational damage, financial fraud and industrial espionage through the manipulation of existing images, video or audio.

Key protective measures:

- **Verify unexpected requests:** If you receive an unusual or urgent request (especially for money or sensitive information) from someone you know, particularly via voice or video call, use a pre-arranged out-of-band verification method. This could be a pre-determined code word, a call to a known and verified number, or an in-person meeting.
- **Limit public digital footprint:** Minimize the number of high-quality images, video and audio recordings of yourself and family members available on public platforms outside of official business. Regularly audit your social media and that of your family members for risk exposure.
- **Educate on deepfake indicators:** Learn to recognize common signs of deepfakes, such as unnatural movements, inconsistent lighting, distorted audio or strange blinking patterns.
- **Establish a family code word:** Create a unique, private family code word that can be used during unexpected or suspicious communications to quickly verify the identity of a family member. This word should be known only to immediate family.

**Third-party fraud and data risks**
Third-party vendors and staff, such as accountants, law firms, travel agents, and even personal staff (nannies, pilots, chefs, etc.) often have less robust physical security and cybersecurity controls. However, they frequently handle or access sensitive data such as travel itineraries, personal identifiers, financial information and business agreements. This sensitive data can be combined to map household routines, upcoming travel, and identify security gaps, thereby facilitating physical threats such as kidnapping, burglary or stalking. This extends to vulnerabilities in service providers like property managers, private jet operators, and even security firms themselves.

Key protective measures:

- **Practice thorough due diligence:** Conduct rigorous due diligence on all third-party vendors, service providers, and personal staff with access to sensitive information. This includes assessing data protection policies, incident response capabilities, and conducting background checks for staff.
- **Secure contracts:** Ensure all third parties and personal staff contracts include strong data protection clauses, clear incident reporting requirements, audit rights, and data retention and destruction policies.
- **Limit data sharing:** Minimize application privileges and only share essential data with third parties. Avoid oversharing personal details.
- **Monitor access:** Regularly monitor and audit third-party access to your data and systems.
- **Secure communication channels:** Use encrypted and secure communication channels (e.g., secure portals or encrypted email) when exchanging sensitive information with third parties.

# Conclusion

In an increasingly complex and digitally interconnected world, safeguarding the security and privacy of wealthy individuals and their families requires a proactive, multi-faceted approach. By implementing the best practices and strategies outlined in this paper, from enhancing online and device security to prioritizing physical safety, families can significantly reduce vulnerabilities and protect against potential threats. Technology should enhance, not diminish, the family personal privacy and security by maximizing the benefits while minimizing risks. Ongoing vigilance and continuously adapting security protocols are essential; security for wealthy individuals is only as robust as the entire family ecosystem. Clear communication, consistent education, and buy-in from all stakeholders are key. By implementing these strategic adjustments and maintaining awareness, families can protect their privacy and security within an interconnected and ever-evolving global threat environment.

# About Citi Security and Investigative Services

Citi Security and Investigative Services (CSIS) is a full-service security and investigative team that is responsible for the safety and security of the assets, integrity and reputation of Citi. We accomplish this by offering in-house professional security services, independent investigations and crisis management to clients across Citi's businesses and regions, partnering with other Citi business groups, law enforcement agencies, governments and industry counterparts to maintain a secure environment for Citi’s operations and to safeguard the interests of its clients and stakeholders.

**Important information**

**For European resident clients this communication is considered marketing material.**

Citi Private Bank, Citi Global Wealth at Work, and Citi Personal Wealth Management are businesses of Citigroup Inc. ("Citigroup"), which provide clients access to a broad array of products and services available through bank and non-bank affiliates of Citigroup. Not all products and services are provided by all affiliates or are available at all locations. In the U.S., investment products and services are provided by Citigroup Global Markets Inc. ("CGMI"), member FINRA and SIPC, Citi Private Alternatives, LLC ("CPA"), member FINRA and SIPC. CPA acts as distributor of certain alternative investment products to certain eligible clients' segments. CGMI accounts are carried by Pershing LLC, member FINRA, NYSE, SIPC. Investment management services (including portfolio management) are available through CGMI, Citibank, N.A. and other affiliated advisory businesses. Insurance is offered through Citigroup Life Agency LLC ("CLA"). In California, CLA does business as Citigroup Life Insurance Agency, LLC (license number 0G56746). CGMI, CPA, CLA and Citibank, N.A. are affiliated companies under the common control of Citigroup.

Outside the U.S., investment products and services are provided by other Citigroup affiliates. Investment Management services (including portfolio management) are available through CGMI, Citibank, N.A. and other affiliated advisory businesses. These Citigroup affiliates, will be compensated for the respective investment management, advisory, administrative, distribution and placement services they may provide.

In Canada, Citi Private Bank is a division of Citibank Canada, a Schedule II Canadian chartered bank. References herein to Citi Private Bank and its activities in Canada relate solely to Citibank Canada and do not refer to any affiliates or subsidiaries of Citibank Canada operating in Canada. Certain investment products are made available through Citibank Canada Investment Funds Limited ("CCIFL"), a wholly owned subsidiary of Citibank Canada. Investment Products are subject to investment risk, including possible loss of principal amount invested. Investment Products are not insured by the CDIC, FDIC or depository insurance regime of any jurisdiction and are not guaranteed by Citigroup or any affiliate thereof.

CCIFL is not currently a member, and does not intend to become a member of the Canadian Investment Regulatory Organization ("CIRO"); consequently, clients of CCIFL will not have available to them investor protection benefits that would otherwise derive from membership of CCIFL in the CIRO, including coverage under any investor protection plan for clients of members of the CIRO.

In the United Kingdom, Citibank N.A., London Branch (registered branch number BR001018), Citigroup Centre, Canada Square, Canary Wharf, London, E14 5LB, is authorized and regulated by the Office of the Comptroller of the Currency (USA) and authorized by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request. The contact number for Citibank N.A., London Branch is +44 (0)20 7508 8000.

Citibank Europe plc, UK Branch is registered as a branch in the register of companies for England and Wales with registered branch number BR017844. Its registered address is Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB. VAT No.: GB 429 6256 29. Citibank Europe plc is registered in Ireland with number 132781, with its registered office at 1 North Wall Quay, Dublin 1. Citibank Europe plc is regulated by the Central Bank of Ireland. Ultimately owned by Citigroup Inc., New York, USA.

Citibank Europe plc, Luxembourg Branch, registered with the Luxembourg Trade and Companies Register under number B 200204, is a branch of Citibank Europe plc. It is subject to the joint supervision of the European Central bank and the Central Bank of Ireland. It is furthermore subject to limited regulation by the Commission de Surveillance du Secteur Financier (the CSSF) in its role as host Member State authority and registered with the CSSF under number B00000395. Its business office is at 31, Z.A. Bourmicht, 8070 Bertrange, Grand Duchy of Luxembourg. Citibank Europe plc is registered in Ireland with company registration number 132781. It is regulated by the Central Bank of Ireland under the reference number C26553 and supervised by the European Central Bank. Its registered office is at 1 North Wall Quay, Dublin 1, Ireland.

This document is communicated by Citibank (Switzerland) AG, which has its registered address at Hardstrasse 201, 8005 Zurich, Citibank N.A., Zurich Branch, which has its registered address at Hardstrasse 201, 8005 Zurich, or Citibank N.A., Geneva Branch, which has its registered address at 2, Quai de la Poste, 1204 Geneva. Citibank (Switzerland) AG and Citibank, N.A., Zurich and Geneva Branches are authorised and supervised by the Swiss Financial Supervisory Authority (FINMA).

In Jersey, this document is communicated by Citibank N.A., Jersey Branch which has its registered address at PO Box 104, 38 Esplanade, St Helier, Jersey JE4 8QB. Citibank N.A., Jersey Branch is regulated by the Jersey Financial Services Commission. Citibank N.A. Jersey Branch is a participant in the Jersey Bank Depositors Compensation Scheme. The Scheme offers protection for eligible deposits of up to £50,000. The maximum total amount of compensation is capped at £100,000,000 in any 5 year period. Full details of the Scheme and banking groups covered are available on the States of Jersey website www.gov.je/dcs, or on request.

**Hong Kong / Singapore: Citibank, N.A., Hong Kong / Singapore organized under the laws of U.S.A. with limited liability.** This communication is distributed in Hong Kong by Citi Private Bank operating through Citibank N.A., Hong Kong Branch, which is registered in Hong Kong with the Securities and Futures Commission for Type 1 (dealing in securities), Type 4 (advising on securities), Type 6 (advising on corporate finance)

and Type 9 (asset management) regulated activities with CE No: (AAP937) and is distributed in Singapore by Citi Private Bank operating through Citibank, N.A., Singapore Branch which is regulated by the Monetary Authority of Singapore. Any questions in connection with the contents in this communication should be directed to registered or licensed representatives of the relevant aforementioned entity. The contents of this communication have not been reviewed by any regulatory authority in Hong Kong or any regulatory authority in Singapore. Investors should exercise caution in relying on this material. This communication contains confidential and proprietary information. It is strictly intended for and may only be distributed to (i) an investor who qualifies as an "accredited investor" in Singapore (as defined under the Securities and Futures Act 2001 of Singapore if the investor is in Singapore or (ii) an investor who qualifies as a "professional investor" in Hong Kong (as defined under the Hong Kong Securities and Futures Ordinance and its subsidiary legislation) if the investor is in Hong Kong.

For regulated asset management services, any mandate will be entered into only with Citibank, N.A., Hong Kong Branch and/or Citibank, N.A. Singapore Branch, as applicable. Citibank, N.A., Hong Kong Branch or Citibank, N.A. Singapore Branch may sub-delegate all or part of its mandate to another Citigroup affiliate or other branch of Citibank, N.A. Any references to named portfolio managers are for your information only, and this communication shall not be construed to be an offer to enter into any portfolio management mandate with any other Citigroup affiliate or other branch of Citibank, N.A. and, at no time will any other Citigroup affiliate or other branch of Citibank, N.A. or any other Citigroup affiliate enter into a mandate relating to the above portfolio with you. To the extent this communication is provided to clients who are booked and/or managed in Hong Kong: No other statement(s) in this communication shall operate to remove, exclude or restrict any of your rights or obligations of Citibank under applicable laws and regulations. Citibank, N.A., Hong Kong Branch does not intend to rely on any provisions herein which are inconsistent with its obligations under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, or which misdescribes the actual services to be provided to you.

Citibank, N.A. is incorporated in the United States of America and its principal regulators are the US Office of the Comptroller of Currency and Federal Reserve under US laws, which differ from Australian laws. Citibank, N.A. does not hold an Australian Financial Services Licence under the Corporations Act 2001 as it enjoys the benefit of an exemption under ASIC Class Order CO 03/1101 (remade as ASIC Corporations (Repeal and Transitional) Instrument 2016/396 and extended by ASIC Corporations (Amendment) Instrument 2024/497).

**Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside Citi. Any statement in this Communication regarding tax matters is not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.**

**Neither Citi nor any of its affiliates can accept responsibility for the tax treatment of any investment product, whether or not the investment is purchased by a trust or company administered by an affiliate of Citi. Citi assumes that, before making any commitment to invest, the investor and (where applicable, its beneficial owners) have taken whatever tax, legal or other advice the investor/beneficial owners consider necessary and have arranged to account for any tax lawfully due on the income or gains arising from any investment product provided by Citi.**


citi
Wealth