Mobile Communications Best Practice Guidance

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) has identified cyber espionage activity by People's Republic of China (PRC) government-affiliated threat actors targeting commercial telecommunications infrastructure. This activity enabled the theft of customer call records and the compromise of private communications for a limited number of highly targeted individuals. While applicable to all audiences, this guidance specifically addresses "highly targeted" individuals who are in senior government or senior political positions and likely to possess information of interest to these threat actors. CISA is releasing this best practice guidance to promote protections for mobile communications from exploitation by PRC-affiliated and other malicious cyber threat actors.

Best Practices

CISA strongly urges highly targeted individuals to **immediately review and apply** the best practices below to protect mobile communications. Highly targeted individuals should assume that all communications between mobile devices—including government and personal devices—and internet services are at risk of interception or manipulation. While no single solution eliminates all risks, implementing these best practices significantly enhances protection of sensitive communications against government-affiliated and other malicious cyber actors. Organizations may already have these best practices in place, such as secure communication platforms[1] and multifactor authentication (MFA) policies. In cases where organizations do not, apply the following best practices to your mobile devices.

General Recommendations

Apply these best practices to your **devices** and **online accounts.**

1. **Use only end-to-end encrypted communications.**
   - ☐ Adopt a free messaging application for secure communications that guarantees end-to-end encryption, such as Signal or similar apps. CISA recommends an end-to-end encrypted messaging app that is compatible with both iPhone and Android operating systems, allowing for text message interoperability across platforms. Such apps may also offer clients for MacOS, Windows, and Linux, and sometimes the web. These apps typically support one-on-one text chats, group chats with up to 1,000 participants, and encrypted voice and video calls. Additionally, they may include features like disappearing messages and images, which can enhance privacy. When selecting an end-to-end

[1] Some examples include, but are not limited to, Microsoft Teams, Google Workspace, Slack, and WebEx.

encrypted messaging app, evaluate the extent to which the app and associated services collect and store metadata.

2. **Enable Fast Identity Online (FIDO) phishing-resistant authentication**. FIDO authentication uses the strongest form of MFA and is effective against MFA bypass techniques. Where feasible, hardware-based FIDO security keys, such as Yubico or Google Titan, are the most effective; however, FIDO passkeys are an acceptable alternative.
   - ☐ Take inventory of valuable accounts, including email and social media. Review any accounts where information leakage would benefit threat actors.
   - ☐ Enroll each account in FIDO-based authentication, especially Microsoft, Apple, and Google accounts. Once enrolled in FIDO-based authentication, disable other, less secure forms of MFA.
   - ☐ For Gmail users, enroll in Google's Advanced Protection (APP) program, as it strengthens your defenses against phishing and account hijacking.
3. **Migrate away from Short Message Service (SMS)-based MFA.** Do not use SMS as a second factor for authentication. SMS messages are not encrypted—a threat actor with access to a telecommunication provider's network who intercepts these messages can read them. SMS MFA is not phishing-resistant and is therefore not strong authentication for accounts of highly targeted individuals.
   Note: Some online services may default to SMS during account recovery flows; it may not be feasible for you to completely eliminate SMS messages from the service.
   - ☐ For less valuable accounts, use other forms of MFA such as authenticator codes. Set up these accounts with a free authenticator application for MFA, such as Google Authenticator, Microsoft Authenticator, or Authy.
     Note: While authenticator codes are better than SMS, they are still vulnerable to phishing. Only FIDO authentication is phishing-resistant.
   - ☐ Once enrolled, disable SMS for each account. Enrollment in authenticator-based MFA does not automatically unenroll the account's SMS. This can create a weak, exploitable fallback mechanism that can be exploited by threat actors.
4. **Use a password manager** to store all passwords. Some password managers, such as the Apple Passwords app, LastPass, 1Password, Google Password Manager, Dashlane, Keeper, and Proton Pass, automatically alert on weak, reused, or leaked passwords. Additionally, some of these password managers generate authenticator codes.
   - ☐ Protect the vault (primary) password with a strong passphrase (i.e., long, unique, and random).
   - ☐ Review existing passwords to ensure they are long, unique, and random. If they are not, change to passwords generated by the password manager. See CISA's Use Strong Passwords guidance for more information.
5. **Set a Telco PIN**. Most telecommunications providers offer the ability to set an additional PIN or passcode for your mobile phone account. This PIN is required for logging into your account or completing sensitive operations, such as porting your phone number—a critical step in countering subscriber identity module (SIM)-swapping techniques.
   - ☐ Add a PIN and MFA to your mobile carrier account to reduce the risk of SIM-swapping techniques. Then, use your password manager to change your mobile account password.

6. **Regularly update software.**
   - ☐ Regularly update operating systems and applications on mobile devices. Check weekly to ensure devices are up to date.
   - ☐ Enable auto-update on mobile devices to ensure timely patching of the operating system and applications.
7. **Opt for the latest hardware version from your cell phone manufacturer.** Newer hardware often incorporates critical security features that older hardware cannot support. Without the most recent version of the hardware, software updates alone will not provide the maximum available security benefits.
8. **Do not use a personal virtual private network (VPN).** Personal VPNs simply shift residual risks from your internet service provider (ISP) to the VPN provider, often increasing the attack surface. Many free and commercial VPN providers have questionable security and privacy policies. However, if your organization requires a VPN client to access its data, that is a different use case.

iPhone-Specific Recommendations

The below recommendations are specific to iPhone users to enhance protections of mobile communications.

1. **Enable** Lockdown Mode. Lockdown mode strictly limits certain apps, websites, and features, or makes some features unavailable, to reduce the attack surface that could potentially be exploited by threat actors.
2. **Disable the following setting** to ensure messages do not send as SMS if iMessage is unavailable. iMessage offers end-to-end encryption between Apple users.
   - ☐ Disable: Settings → Apps → Messages → "Send as Text Message"
3. **Protect your Domain Name System (DNS) queries.** Apple iCloud Private Relay provides enhanced privacy and security; as a partial free alternative, use encrypted DNS services for iOS from providers such as Cloudflare's 1.1.1.1 Resolver, Google's 8.8.8.8 Resolver, and Quad9's 9.9.9.9 Resolver. These services support encrypted DNS to prevent interception and manipulation by threat actors.
4. **Enroll in Apple iCloud Private Relay.** For additional protections, enroll in Apple iCloud Private Relay (see the iCloud User Guide for configuration instructions). Private Relay ensures iCloud devices use secure DNS, masks IP addresses, and splits traffic between servers controlled by Apple and a third party to reduce the chances that a single entity can link browser behavior to the user's identity.
   Note: These benefits are limited to the Safari browser.
5. **Review and restrict app permissions** through Settings → Privacy & Security. Review which apps access sensitive data, such as location, camera, and microphone. Revoke and avoid granting permissions that are unnecessary or excessive for functionality of the app.

Android-Specific Recommendations

The below recommendations are specific to Android users to enhance protections of mobile communications.

1. **Prioritize models from manufacturers with strong security track records and long-term security update commitments.** For example, review Android's Enterprise Recommended knowledge worker and dedicated devices to ensure models meet security and update standards. By combining up-to-date hardware with regular software updates, Android users can take full advantage of the platform's evolving security enhancements. Prioritize models that:
   - ☐ Support hardware-level security features—often referred to as secure enclave or hardware security module (HSM)—to enable secure storage of cryptographic keys.
   - ☐ Offer security updates at least monthly.
   - ☐ Commit to security updates for at least the next five years.
2. **Only use Rich Communication Services (RCS) if end-to-end encryption is enabled.** If all participants are using Google Messages, your conversation will use end-to-end encryption. Review Google's Turn on RCS chats in Google Messages and Use end-to-end encryption in Google Messages for additional guidance.
3. **Configure Android Private DNS** to use a trusted, high-privacy resolver, such as Cloudflare's 1.1.1.1 Resolver, Google's 8.8.8.8 Resolver, and Quad9's 9.9.9.9 Resolver.
4. **Confirm Always Use Secure Connections is enabled** in the Chrome browser on your Android device to enhance mobile browsing security. This feature should be turned on by default and ensures all website connections default to HTTPS whenever possible, protecting against threat actor interception and manipulation. See Google's Manage Chrome safety and security guidance.
5. **Confirm Enhanced Protection for Safe Browsing is enabled** in the Chrome browser on your Android device to provide an additional layer of protection against malicious websites, phishing attempts, and harmful downloads. The Safe Browsing feature should be turned on by default and alerts you if you attempt to navigate to potentially dangerous sites or download suspicious files. To enable and optimize this feature, see Google's Choose your Safe Browsing protection level in Chrome guidance.
6. **Confirm Google Play Protect** is enabled to detect and prevent malicious apps. Regularly review the app scans to identify potential threats. Exercise caution if using third-party app stores or "sideloading" apps from other sources.
7. **Review and restrict app permissions** through Settings → Apps → Permissions Manager. Revoke permissions that are unnecessary or excessive for the app's functionality. Unless absolutely required, avoid granting apps access to sensitive permissions such as location, camera, or microphone.

Incident Reporting Information

Cyber incidents can be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), emailing report@cisa.dhs.gov, or reporting online at CISA Services. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Disclaimer

CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.