Security Guidance

Current as of *Oct 13, 2022*

As users of Community Tech Alliance's (CTA) offering, we require that you read and complete the security guidance below. Prioritize devices that you will actively use CTA's offering on, as well as devices and accounts that you use day-to-day. If you have any questions, please feel free to contact security@cta-tech.app. Our most up-to-date security measures are listed at communitytechalliance.org/security.

★ CTA staff will only email you from a **cta-tech.app** or **techallies.org** email address. All email is authenticated. You may also receive automated emails from google-noreply@google.com. These are valid emails generated by Google Workspace and Google Cloud Platform.

★ CTA will **never ask you for your password or other credentials,** and **you should never supply them.** We may, at your request, trigger a password reset for your CTA-provided Google account.

★CTA will **never ask you for credentials to any third-party applications via email or Slack.** If we require credentials or access to third-party tools or applications, we will request that you input credentials into our shared 1Password vault or provide access to a Google account, such as a service account.

★Service Accounts look like *service-account@project-id.iam.gserviceaccount.com*. **You must never grant access to any accounts (CTA or other vendor accounts) to service accounts you do not recognize. Always ask if you aren't sure.**

Contents

✔️ Secure These Accounts

📄 Additional Information

🖥️ Securing Your Devices

Adversaries frequently take advantage of personal and work devices and the applications on them, especially those that are not updated regularly. Always apply software updates as soon as they are made available.

Guidance	Personal	Work
Ensure your mobile device and computers are running the most up-to-date operating systems available	☐	☐
On your CTA (and personal and work accounts, if applicable), enable Google's Advanced Protection Program.	☐	☐
On your personal and work accounts, complete the Gmail Security Checkup.	☐	☐
At a minimum, enable local disk encryption (macOS and Windows) on the device on which you are using your CTA account.	☐	☐

🔑 Use a device that is secure by design

An essential technique to reducing the risk of a breach is to reduce your attack surface. To that end, consider using a Chromebook or an iPad for personal use. Both devices offer several key security features and dramatically limit our adversaries' options for running malware.

🔐 Managing Secrets and Credentials

CTA will provide you with a secure 1Password vault in order to store shared credentials. We recommend that you use a credential/password manager for your non-CTA credentials as well.

Guidance	Personal	Work
Set up a password manager to generate, store, and auto-fill all of your passwords. We recommend 1Password and Dashlane for paid options, and Google's Chrome password manager as a free option.	☐	☐
Create a 'master password' for your password manager that is longer than 16 characters, unique, and memorable. ★ Create a strong master password by using a passphrase. Sample strong passphrase: *worshiper favoring visa nest!*	☐	☐
Use your password manager's two-factor code generator for accounts that do not allow FIDO/hardware two-factor authentication keys. 1Password offers two-factor code generation.	☐	☐
At a minimum, enable local disk encryption (macOS and Windows) on the device on which you are using your CTA account.	☐	☐

★If someone obtains or guesses your master password, they may be able to decrypt all your passwords. Your master password must be long, random, and unique, but also memorable. **This is something you will type every day.**

★If your organization's IT or tech team has questions about the security recommendations above, please reach out to security@cta-tech.app.

🛡️ Two-Factor/Multi-Factor Authentication

1. Enable two-factor authentication (2FA) on all sites. Select the strongest form of 2FA in the following priority order.

    a. FIDO Security Keys. Use security keys whenever possible because all other forms of 2FA are phishable. We recommend Yubikeys and Google Titan Keys. Make sure your security keys support NFC (or Apple's lightning port) so that you can use them with your phone. In some cases, your phone can also be used as a hardware security key.

    FIDO security keys are built on a standard called web authentication and are designed to mitigate real-time phishing. Other commonly-used methods generate a time-bound or single-use code. These codes can easily be exploited by attackers and used remotely with stollen username and password.

    b. Authentication App. We recommend using Authy since it allows for backups in case you lose, misplace, or get a new phone.

    c. Email is the next best option.

    d. Avoid SMS/text message/phone as your 2FA unless it is the only option. Ensure you have a long, random, unique password if so.

★ If you ever send 2FA/MFA codes to your phone, ensure your mobile phone provider (E.g., Verizon, AT&T) also have secure settings like MFA and strong passwords. Mobile phone providers are targets for adversaries who wish to gain access to your accounts. These are often known as "SIM-swap" attacks and can result in an adversary taking over your phone number.

★ CTA supplies FIDO Security Keys to partners located in the United States. These keys are manufactured by Yubico, a leader and long time provider of 2FA hardware.

📨 Secure Messaging and Device Choices

Many of the tools we use every day to communicate (such as standard email and text messaging) are not secure from eavesdropping or interception. Furthermore, even when using a platform like Slack or Google Chat, you should consider that all messages

including direct messages can be retained and subject to litigation holds. Only type things you would not be embarrassed about if they ended up on the front page of The New York Times.

If you need to send sensitive data or have sensitive communications, we recommend using messaging apps that are encrypted in transit and at rest and support disappearing messages. Some examples are Signal and WhatsApp, though each has limitations, so use the application best for your organizations' needs.

Finally, avoid SMS (text messaging) whenever possible, especially when dealing with sensitive data.

📈 Data Security

As data practitioners and infrastructure folks, we work with a lot of data daily! Even when that data doesn't contain PII (personally identifiable information), it is still our responsibility to keep that data safe and secure.

CTA employs industry-standard access controls and security monitoring and logging, but the safety of your data is a joint responsibility. We will provide up-to-date security information to your team where applicable. We recommend that you familiarize yourself with Google BigQuery security best practices.

CTA is always happy to consult with you and your team on security best practices. Please just email us at security@cta-tech.app to schedule time with us.

✔️ Secure These Accounts

It is likely that you and/or your organization use the services below. Use this checklist to confirm that you've added a strong password and enabled 2FA/MFA on each.

Account	Personal	Work
Apple (Apple Business Manager)	☐	☐
Google Workspace, Microsoft Office 365, Yahoo!, AOL	☐	☐
Facebook and Instagram	☐	☐
Twitter	☐	☐
LinkedIn, Pinterest, Snapchat, TikTok, WhatsApp, Skype, Slack	☐	☐
File Storage, like Box and Dropbox	☐	☐
E-commerce sites, like Amazon and CDW	☐	☐

★ CTA also recommends that you check any other sites that contain your personal or business information. These include, but are not limited to:

- Bank, investment, and other financial institutions
- Health insurance and HR applications
- Streaming and media services, like Hulu, Netflix, and HBO Max
- Travel sites, such as Airbnb, Booking.com, Lyft, and Uber
- Other corporate services, like Salesforce and SAP

📄 Additional Information

1. We strongly recommend using a hosted email service and productivity suite such as Google Workspace for your work email. Don't run your own server if you need to send bulk email; instead, use a trusted sender like Mailchimp or a transactional email offering like Amazon Web Services SES.

2. Community Tech Alliance doesn't offer or use a VPN (Virtual Private Network), and we recommend you don't either. While having secure access to cloud services is important, we recommend that you leverage new practices like zero-trust networking.

    a. On your personal devices, to ensure that you have a secure connection, CTA recommends leveraging secure DNS and only visiting sites over HTTPS/TLS. If you have privacy concerns over your ISP's ability to monitor your traffic, you can use a tool like NextDNS and Google Chrome, which force-upgrades connections to HTTPS.

3. Your CTA-provided Google account will give you access to both Google services and, in some cases, third-party services. We leverage Single Sign-on (SSO); for example, using our Google account to log into independent services, like Atlassian products. We recommend that your team also leverage SSO wherever possible. For example, Slack administrators can require their users to log in via Google accounts. If your Google account already has 2SV/MFA, then there's no need to add *an additional* 2SV/MFA to your Slack account–you just use your Google account!