TB.2

# Best Practices for Cyber and Data Security

It's easy to understand the impact of a physical robbery at your home. However, **data theft can be just as, if not more, damaging,** and often goes unnoticed until significant harm has been done.

Data thieves can:

- **Steal your identity** and use it to take out credit in your name
- **Access your bank accounts** and steal your money
- **Access your cell phone number** and hold your cell phone hostage and use it to get into all of your accounts

## California's Commitment to Data Protection

The State of California has some of the strongest protections in the country to make sure that organizations like California FarmLink or bookkeeping and tax preparation firms keep your data safe. There are steep fines if we fail to follow best practices in protecting your data. This is why we ask you to **transmit data to us using secure links and not using e-mail or text messages.**

What to Know About Secure Systems:

- **Encryption**: Data is made unreadable to outsiders. Look for systems or files marked as "encrypted" or "secure."
- **Storage Security**: Use trusted platforms (like Google Drive or Dropbox) with strong passwords and two-factor authentication (2FA).
- **Transmission Security**: Avoid sending documents over plain email. Use **encrypted file portals** (like ShareFile, Dropbox with password protection, or your bookkeeper's secure portal).

## Secure methods of Storing and Transmitting Data

1. **Verify the Recipient Before You Send Anything:** Before sending data, call or text your CPA, tax preparer, bookkeeper, or Community Development Financial Institution (CDFI) to verify their email or portal details. Scammers often impersonate trusted professionals to steal data.

2. **Use Strong Passwords and 2-Factor Authentication (2FA) for storage**: Create unique, 12+ character passwords (mixing letters, numbers, and symbols, phrase) for your accounts. Here are a few tips for how to create passwords you will remember: .
    - ***Use a phrase***: CABerryFarmersAreBEST!!9753
    - ***Use a combination*** with the name of a favorite town or place, the number of children, cousins, siblings or friends you think of most often, and a symbol that makes sense to you: Patzcuaro&4, ElTepozteco3!
    - ***Use an abbreviation***: Make a password from the first letter of each word in a sentence.
        - Sentence: I Love Farmering, Ranching, and Fishing in California!
        - Abbreviation: ILFR&FIC!!25
3. **Securely Store Your Passwords:**
        - Multi-Factor Authentication (MFA): A security method requiring you to verify your identity in multiple ways before you're granted access to an online account, app, or system.
            - Something you have: A code sent to your phone via text message, an authenticator app that generates a constantly changing code, or a physical security key.
            - Something you have: A biometric scan, like your fingerprint or facial recognition.
        - Google Keychain: This is built into your Google Account, Chrome browser, and Android devices, securely storing and syncing your passwords and passkeys across all your signed-in devices for easy access and autofill.
        - iCloud Keychain: securely stores and syncs your passwords, passkeys, credit card info, and Wi-Fi passwords across all your Apple devices.
4. **Limit Access:** For bookkeepers using software like QuickBooks, provide temporary access with limited permissions. Revoke access once their work is complete.
5. **Monitor:** Regularly check accounts for unusual activity. Set up bank alerts for transactions over $500 to spot issues early. We will help you do this with your business accounts, you need to do this for your personal accounts -  and don't forget your kids if they have savings accounts!

## Questioning Data Security Practices

If you are working with a service provider who does not use a safe method of storing and transmitting data and does not ask you to do so, you should question if your data is secure.

## Warning Signs and Easy Actions:

- **Lack of encryption**:
    - ***Example:*** Your bookkeeper, tax preparer or CPA e-mails you financial reports and asks you to email tax documents to their personal e-mail account instead of using a secure portal like ShareFile.
    - ***Easy Action:*** *Verify the email with your* bookkeeper, tax preparer or CPA. Ask "Do you have a secure client portal for sharing files?" If they say no or suggest email, request a secure alternative or consider a different provider.
    - **FarmLink Clients:** We use Dropbox for this.
- **Requesting excessive data**:
    - ***Example:*** Your bookkeeper asks for your full bank account numbers to process payroll, even though they only need payment totals.
    - ***Easy Action:*** Ask, "Why do you need this specific data?" If their reason isn't clear or necessary, redact sensitive details before sharing.
- **Suspicious behavior or urgency:**
    - ***Example:*** A bookkeeper or tax preparer emails from a new address, pressuring you to send tax data urgently without verifying their identity, or asks you for more banking account information than they need. (They need to view your bank accounts, they do not need to have access to your accounts.)
    - ***Easy Actions:*** Call their known phone number to confirm the request. If the contact is unfamiliar or unverified, don't share data and report the suspicious activity. Do not provide anyone with direct access to your bank account unless you know you are working through a secure portal such as a payment gateway.
    - **California FarmLink Clients:** we will only email you from an email ending in @cafarmlink.org and you can always give us a call to confirm it is a relevant FarmLink staff person requesting information

No legitimate business, government agency or other non-profit organization will ever ask for your personal financial information or other sensitive data via text, phone call, or e-mail. If you get any phone call test or e-mail demanding payment (or offering to pay you!) and requesting access to your financial accounts, it is a scam. A legitimate request will happen:

- In the context of a relationship you already have
- With a person you already know

- Using a secure platform - but even then verify with the person you are working with so you are certain that you are being directed to the correct platform

If you get a text, e-mail, or phone call and you are not sure, do not respond to what you received. Instead find the last legitimate communication you had with that person or organization and initiate contact with that person or organization and ask if the communication you just received is legitimate. If they say it is legitimate, be sure that you understand what they are asking for and why.

Note: The IRS will only contact you via the US Postal Service.

*Authored by Samantha Estrada*