


## It's Tax Time...Yay?

### Before Filing Your Taxes

- Update your Software - be sure that all internet-connected devices are running the most current versions.
- Update your Passwords before you begin
- Include Multi-Factor Authentication wherever you can

### Watch Out For Scams

Learn how to recognize a scam with the following Red Flags:

- Be highly suspicious of any phone calls, emails, or texts claiming to be from the IRS or other government agencies.
  - Requests for Personally Identifiable Information (PII) refers to any data that could potentially identify a specific individual. For example:
    - » Bank account information, Social Security numbers, login credentials, mailing addresses
  - Urgency. The sender uses an abnormal sense of urgency, or other scare tactics, to obtain information.
  - Attachments. The message includes an attachment, such as a PDF.
-  Never open attachments from a suspicious or unknown email address. It may download malware or viruses onto your device.



### Securely Sending Documents to Tax Preparers

- Encrypt your files before sending them via email - available on most major email platforms.
- Use a secure portal to upload documents - they encrypt documents during transfer and storage and limit access to only approved individuals.

### Finish Up by Backing Up

Protect your valuable documents by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.



### REMEMBER...

The IRS will not call you out of the blue. If there is an issue, you will receive information in the mail first.

The IRS will also never ask for credit or debit information over the phone.