Online Trust Alliance

TIPS FOR KEEPING SAFE DURING TAX SEASON

Keep your identity and personal information secure and private

❑	**The IRS Does Not Call.** A common scam involves a fraudster calling, claiming to be the IRS and asserting the taxpayer owes money and must pay immediately. The IRS never asks for personal or financial information by email, phone, text or social media nor does it ever call to demand payment. Cyber criminals have learned how to spoof phone caller ID to display "Internal Revenue Service." Report suspicious calls to the IRS at 1-800-366-4484.
❑	**The IRS Does Not Email; *Block Spoofed & Forged Email – Be Skeptical*.** Do not respond to an unsolicited email that requests your private or sensitive information or asks you to click on a link. For information, type www.irs.gov directly into your browser. Only use email services which provide complete email authentication checks. Leading consumer services including Yahoo! Mail, Gmail and Outlook / Hotmail support these standards. All business inbound email should validate the sender. Cybercriminals can make messages and webpages look authentic. https://otalliance.org/eauth.
❑	**Ask Before You Share.** If you are asked for something sensitive such as a Social Security Number (SSN), ask why it is needed and what systems are in place to protect it.
❑	**Less is More; Check Default Settings.** Privacy is not the default setting on social sites, which typically make most of your information widely accessible unless you specify otherwise. Change the settings to the privacy level you feel comfortable with. Also, do not share too much – just because a form has blanks, it doesn't mean you have to provide that information.
❑	**Protect your Device (PC, Mac, Tablet & Phone).** Keep security software on your devices, and keep it updated. Think of it like locking your home's doors and windows to protect everything inside. Activate auto-locking on your phone, requiring passwords.
❑	**When Free Wi-Fi Costs.** Criminals set-up look-a-like hotspots to eavesdrop on unprotected data, and capture user passwords. Consider using a virtual private network (VPN) or tether your computer to your mobile device. Make sure connections are encrypted (https). https://otalliance.org/aossl.
❑	**Look For The Green.** The IRS and leading organizations now mandate the use of Extended Validation SSL Certificates. Look for the green trust indicator in your browser to help validate that the site you are visiting is legitimate. https://cabforum.org/about-ev-ssl/.
❑	**Passwords**. Strong passwords are not enough. Use unique passwords and two-factor authentication where possible. Reusing passwords expands the impact of a compromise.
❑	**File Tax Returns As Soon As Possible.** When filing taxes, putting it off to the last minute increases the risk of someone filing a bogus return in your name. File as early as you can.
❑	**Check your credit history.** Free credit reports are available at annualcreditreport.com. Reports can help indicate use of your identity for nefarious purposes. We recommend ID theft monitoring services and checking your reports monthly. https://otalliance.org/breach.

 For Updates visit https://otalliance.org/taxfraud