RE: Keeping you and your loved ones safe online

2/4/2022
Good Moring
As we enter tax season, is this a good time for a reminder of how to protect yourself when using email and web. Please discuss these topics with your family, especially teens and older relatives. Together we are stronger.

Last week 49,297 emails were sent to CSH email boxes. 12,333 messages were prevented from reaching staff by our filter due to the emails being classified as Spam, who the sender was, content and the like.

1. Don't get phished
    a. Please report suspicious emails to the tech department and exercise caution before clicking on a link or attachment.
2. Don't share your passwords. (**We will be requiring all staff to change their network password after the February vacation. Passwords require 12 characters or more, and include, upper- and lower-case letters, numbers and special characters**.
    a. Use strong passwords. Using a Password Phrase (i.e. Hockey/17/csh/Carol) allows you to make a long, complex password that is rememberable to you but hard to crack. Test the strength of passwords here
    b. Example: (i.e. Hockey/17/csh/Carol)
    c. (**Hockey** = my favorite sport, **/17** = house number a grew up at, **/csh** = where I work, **/Carol** = my mother's name. This password will take 496 centuries to Crack.
    d. If I add an **asterisk** to the end of the phrase (Hockey/17/csh/Carol*****) the time to crack increases to 47,193 centuries.
    e. If you think that a password may have been compromised, contact the Tech Team and we will help you change your password.
3. This link will take you added information on Cyber Security and Privacy Reminders

Suggestion to keep you and your loved ones safe during tax season CPA Practice Advisor

Text message scams
Last year, there was an uptick in text messages that impersonated the IRS. These scams are sent to taxpayers' smartphones and have referenced COVID-19 and/or "stimulus payments." These messages often contain bogus links claiming to be IRS websites or other online tools. Other than IRS Secure Access, the IRS does not use text messages to discuss personal tax issues, such as those involving bills or refunds. The IRS also will not send taxpayers messages via social media platforms.

Unemployment fraud
As a new tax season begins, the IRS reminds workers to watch out for claims of unemployment or other benefit payments for which they never applied. States have experienced a surge in fraudulent unemployment claims filed by organized crime rings using stolen identities. Criminals are using these stolen identities to fraudulently collect benefits.

Email phishing scams
The IRS does not initiate contact with taxpayers by email to request personal or financial information. The IRS initiates most contacts through regular mail delivered by the United States Postal Service.
Phone scams
The IRS does not leave pre-recorded, urgent, or threatening messages. In many variations of the phone scam, victims are told if they do not call back, a warrant will be issued for their arrest. Other verbal threats include law-enforcement agency intervention, deportation, or revocation of licenses.

Be well
Joe