Internet Scam Alert

The Internal Revenue Service never contacts taxpayers by e-mail to alert them of refunds or of problems with payments or to request personal or financial information. Be alert for "phishing" e-mails sent by scammers in an attempt to obtain your information. Do not reply to, open any attachments, or click on any links from suspicious e-mails purporting to be from the IRS or EFTPS (Electronic Federal Tax Payment System).

If directed to a website for additional information, DO NOT CLICK ON THE LINK, as the website contains malware that will infect your computer and steal account numbers, user names and passwords to your accounts at financial institutions, as well as spread itself to the computers of everyone in your address book.

REMEMBER: THE IRS DOES NOT INITIATE E-MAIL CORRESPONDENCE WITH TAXPAYERS ABOUT THEIR ACCOUNTS.

Also, be wary of e-mails from Federal Express, UPS, EBay, PayPal, Amazon.com, credit card companies, and financial institutions. They may claim a package cannot be delivered, there is a payment issue, or information is needed about your account. In some cases, just opening the e-mail will cause malware to infect your computer, without your having to click on the link provided.

As technology changes, the scam artists find new methods of reaching you. Text message scams involve sending you a text message that appears to be from a credit card or other financial institution about your account, with either a phone number to call or a website to go to. A similar scam is a text message offering you a bargain if you call a number or go to a website and download a confirmation.

Social networking sites like Facebook and Twitter have also become targets for hackers and scammers. One method they use is to send you a message that tricks you into clicking on a link that takes you to a fake login page, where you enter your password, giving the scammer access to your account. They can then use your account to reach your network of contacts. As a result of an account being compromised, a message may seem to come from a regular follower or friend, but by clicking on the accompanying link, you can infect your computer with a virus or malware.

TIPS FOR PROTECTING YOURSELF:

- The IRS and financial institutions will never e-mail, tweet or text you for personal information, so never reply to an e-mail, tweet or text message requesting confidential information.
- Pay close attention to messages referring to financial transactions to make sure that the sender of the message is legitimate. Check that the subject line references your account number or other identifying information. Scammers will generally not have your personal information.
- Be careful about clicking on links to websites, even if they appear to be from people or institutions you know. Instead, go to the official website by typing the address in your browser.
- Avoid calling phone numbers provided in an e-mail, text message or tweet. You can check your credit card, statement from a financial institution, phonebook, or the legitimate website of the institution for the correct contact information.

more...

Kranz & Company LLP
taxes@kranzandco.com

Internet Scam Alert

- If it sounds too good to be true, it probably is. You have not won the lottery, will not make thousands of dollars working from home, and there is no prize – although if you call the phone number provided, you may be charged an outrageous amount for the call.

- Change your passwords often. If you think your security has been breached, change your passwords immediately.

- If using a public computer, make sure to clear the history, close the browser and log off. If possible, you should reboot. Avoid visiting financial institutions or entering credit card numbers on public computers.

- KEEP YOUR INTERNET SECURITY UP TO DATE. Run virus and malware scans at regular intervals. Make sure Windows Update is set to automatic in order to fix the latest security issues.

- If your browser has a setting for "phishing filter", make sure that it is turned on to automatically check for suspicious websites. (In Internet Explorer, it is in Tools/ Internet Options/ Advanced tab/ Security/Phishing filter.)