Mullin's Business Service LLC

312 South Grand Street * Schoolcraft, MI * 49087 * (269) 679-5536 * FAX (269) 679-2206 * e-mail: cmm@mbs312.com

To all of our clients;

We take several precautions here in our office to protect your information. However, we also need to remind you that what you do on your devices and how you protect them is just as important.

We are writing to caution you about several email scams that are targeting taxpayers this filing season. Cybercriminals use these scams to obtain names, social security numbers and addresses, which they then use to file fraudulent returns.

In one version of the scam, cybercriminals trick payroll personnel into disclosing sensitive employee information. Cybercriminals pose as executives and send emails to payroll personnel requesting copies of Forms W-2 for all employees. Criminals use the W-2 information to file fraudulent tax returns, or they post it for sale on the Dark Net.

In another version of the scam, cybercriminals pose as the IRS, the IRS Taxpayer Assistance Center, a professional tax organization, a tax software company, or IRS Refunds. They trick people into opening a link in an email. This link takes people to a fake page where thieves try to steal information. In some cases, these links or email attachments also secretly downloaded malware to your device that can give the thief control of the computer or allow the thief to track keystrokes to determine passwords or other critical data.

A new scam targets senior citizens; they get a phone call telling them that their Social Security deposit will be held unless they verify their information. Once the person verifies their information the thieves have everything they need to either sell that information or use it for their own purposes.

You should always use security software with firewall and anti-virus protection on your home computers. If you store your tax records on your computer make sure you encrypt the information. Your cell phones, tablets & computers should all have password protection on them.

Consult with your information technology (IT) consultant about the best way to protect your sensitive data and systems. Learn to recognize and avoid scam emails that may be nothing more than an attempt to steal personal information. Do ***not*** click on links or download attachments from unknown or suspicious emails.

Remember that the IRS will never initially contact a taxpayer via email or by telephone about a bill or tax refund. No legitimate agency is going to ask you to pay your alleged tax bill using gift cards, iTune cards or any other type of non-cash payment. No one is going to throw you in jail if a tax bill isn't paid in the next 8 hours. If you get a pop up on your computer screen that says you are infected with a virus and need to click on the link below or call a phone number for help DON'T DO IT! Shut your computer off immediately and get help from a legitimate source.

If you have any questions about your tax account, if you receive a suspicious email, or if you think that you have been the victim of identity theft, please do not hesitate to contact us for assistance.

Mullin's Business Service LLC