Beware of Schemes During Tax Season

It's tax season! Every year, around this time, the Internal Revenue Service (IRS) publishes its dirty dozen – a list of scams criminals use to try and ferret out personal information and/or steal money.[1] For example, if you received an email from a top executive in your company or organization requesting data from IRS form W2 for the 2016 tax year, what would you do?[2]

The right answer is: Don't respond.

Disguising an email to look like it's from your boss or someone higher up in your firm is called **spoofing**. Criminals have been spoofing corporate employees for years, and now they're turning their attention to school districts, tribal organizations, restaurants, hospitals, and non-profits, according to a February 2017 IRS press release.[3] If you receive a suspicious email, contact your Human Resources department.

Spoofing is just one scheme among many. Here are some of the other scams you should guard against:

Phishing. *Merriam-Webster* explains phishing like this, "…A common phishing scam involves sending emails that appear to come from banks requesting recipients to verify their accounts by typing personal details, such as credit card information, into a Web site that has been disguised to look like the real thing. Such scams can be thought of as 'fishing' for naive recipients."[4]

If you receive an email purporting to be from the IRS, remember this: The IRS does not contact taxpayers about refunds or tax bills using email, text, or social media. In fact, the agency cautions Americans not to click on a link in an email claiming to be from the IRS.[1]

In addition, banks and financial institutions typically won't ask for confidential personal information (user names, passwords, personal identification numbers, and so on) through text message, email, or social media. One bank provided examples of fake emails that had been sent to its customers, including this one:[5]

Dear account holder,

Due to concerns for the safety and integrity of your online account, we have issued this warning message. It has come to our attention that your account information needs to be updated due to inactive members, frauds, and spoof reports.

We ask you to visit the following link to start the procedure of confirmation on customer data.

To get started, please click HERE.

Please don't reply directly to this automatically-generated email message.

Instead of clicking on a link in a suspicious email or text, call your local bank branch or IRS office to ask whether they sent the request.

Phone scams. Be wary if you receive a call and the person says they are from the IRS – even if caller ID says it's the IRS and the person on the other end of the line offers a badge number and official sounding title – because it's likely a scammer.[6]

Criminals have been impersonating IRS agents and demanding immediate payment of taxes without giving the taxpayer an opportunity to question or appeal the amount owed. They may threaten the taxpayer with arrest, deportation, or another punishment. The IRS does not do this. Scammers may also require a specific payment method, such as a prepaid debit card, or insist taxpayers provide credit or debit card numbers over the phone. Don't do it.[6]

Instead of engaging, take the caller's information, refrain from giving out any of your information, and tell them you will call back. Then, look up the number for your local IRS office. Call them to confirm if the caller is an actual IRS employee or not. Don't call the number provided by the caller.[6]

Identity theft. Criminals have been using other people's personal information (Social Security numbers, names, addresses, birth dates, etc.) to obtain money or credit for many years. Recently, scammers have also been filing false tax returns. The IRS has implemented measures that appear to be effective.[1] At the end of 2016, *USA Today* reported, "An unprecedented public-private crackdown has helped cut taxpayer identity theft reports in half and prevented millions of dollars in fraudulent refunds."[7]

Regardless of the progress that has been made, the IRS cautioned, "Taxpayers need to watch out for identity theft especially around tax time. The IRS continues to aggressively pursue the criminals that file fraudulent returns using someone else's Social Security number. Though the agency is making progress on this front, taxpayers still need to be extremely cautious and do everything they can to avoid being victimized."[1]

If you discover someone has filed a tax return using your personal data, Intuit.com advises you complete IRS Form 14039 and mail it to the IRS.[8]

Being wary can help protect against scammers, but criminals may find a way to capture your personal information regardless of any precautions you take. If you worry your data may have been comprised, the Federal Trade Commission suggests considering a credit freeze, which lets you restrict access to your credit report and makes it more difficult for identity thieves to open new accounts in your name. You'll still be able to open new accounts or allow credit checks by prospective employers or landlords, but you'll need to specifically unfreeze your account for

that purpose. To learn more, contact one of the credit bureaus: Experian, Equifax, or TransUnion.[9]

Sources:

[1] https://www.irs.gov/uac/newsroom/irs-summarizes-dirty-dozen-list-of-tax-scams-for-2017

[2] https://www.edsurge.com/news/2017-02-07-phishing-season-widespread-email-scam-targets-schools-edtech-companies

[3] https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

[4] https://www.merriam-webster.com/dictionary/phishing

[5] https://www.chase.com/digital/resources/privacy-security/security/suspicious-emails

[6] https://www.irs.gov/uac/newsroom/phone-scams-continue-to-be-a-serious-threat-remain-on-irs-dirty-dozen-list-of-tax-scams-for-the-2016-filing-season

[7] http://www.usatoday.com/story/money/2016/11/03/irs-says-2016-crackdown-helped-slow-identity-theft-tax-refund-fraud/93234624/

[8] https://turbotax.intuit.com/tax-tools/tax-tips/General-Tax-Tips/Identity-Theft--What-to-Do-if-Someone-Has-Already-Filed-Taxes-Using-Your-Social-Security-Number/INF23035.html

[9] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs