



Be in the Know: Computer Tech Support and IRS Scams

Release Date: October 9, 2015

Media Contact: Jerad Albracht, 608-224-5007
Bill Cosh, Communications Director, 608-224-5020

MADISON – Tech support and Internal Revenue Service scams target victims randomly and regularly. Both are old scams, both involve threats and demands for money, and neither is showing any signs of slowing down.

Over the past four weeks, the Consumer Protection Hotline at the Wisconsin Department of Agriculture, Trade and Consumer Protection has received at least nine calls about tech support scams and more than 120 calls about IRS scams.

The criminals behind these scams are experts at preying on fears of crashed computers and lost data or back taxes and jail time, and people fall victim every day. The best defense is to know how these scams work and to share this information with friends and family.

Computer tech support scams:

You receive a call out of the blue claiming that your computer has a virus and that the caller can help you get rid of it. The callers often falsely claim to represent Microsoft or a local tech support company to gain your trust. They tell you that they can remove the (non-existent) virus from your computer for a fee. The caller asks you to download software from the internet that grants them remote access to your system.

If you allow these scammers to access your computer, they can load any number of malicious software programs onto your machine and they may access your files as well. If you give them your credit card number to pay for their “services,” you can expect to get ripped off there too. This is typically a phone-based scam, but also shows up in online pop-up messages saying you have a computer virus and telling you to call a specific phone number for help.

What to do:

- Hang up the phone or close the pop-up.
- A tech support representative (Microsoft or otherwise) will never contact you to tell you that your computer has a virus.
- If you question whether your computer is actually infected, run a system scan using the antivirus protection software on your computer. Keep your antivirus software updated in order to protect you from the latest malware.
- If you need additional help, take your computer to a local, trusted tech support business.

IRS scams:

A scammer who falsely claims to be with the Internal Revenue Service contacts you by phone or email. He claims that you owe back taxes. He demands immediate payment and may threaten you with legal action, jail time, deportation or revocation of your driver’s license.

In other versions of IRS scams, the scammer may email you requesting your IRS e-services portal username and password or may request personal or banking information in order to “update” your e-file records.

These are “government impostor” scams – a type of criminal operation that uses the names or “look-alikes” of government agencies in the hopes of adding legitimacy to their ploys. None of the communications mentioned above are actually from the IRS.

What to do:

- Hang up the phone or delete the emails.
- The IRS communicates with taxpayers by traditional mail. The IRS does not initiate contact with taxpayers by phone or email to request immediate payments or to gather personal or financial information.
- Never click a link or open an attachment in an unsolicited email.
- If you question the legitimacy of a communication from a governmental agency, contact DATCP’s Consumer Protection Hotline (800-422-7128) or call the misrepresented agency directly to inquire.
- The IRS has a webpage that describes and debunks the various tax scams that have been reported to the agency. The page provides a wealth of tips, news releases, and video and podcast links to help you stay informed on these threats: <http://www.irs.gov/uac/Tax-Scams-Consumer-Alerts>.

For additional information or to file a complaint, visit the Consumer Protection Bureau at <http://datcp.wisconsin.gov>, send an e-mail to datcphotline@wisconsin.gov or call the Consumer Information Hotline toll-free at 1-800-422-7128.

Connect with us on Facebook at www.facebook.com/wiconsumer.

###