

Don't Click on that Email from the IRS!

Written by Kathleen Vinehout, State Senator 31st District
Tuesday, 21 June 2016 10:48 - Last Updated Tuesday, 21 June 2016 11:07

<http://newiproggressive.com/images/stories/S5/identity-theft3-s5.jpg>



The IRS has witnessed a significant increase in email scams using the IRS name to lure people into giving up important personal information. Sen. Kathleen Vinehout shares information about what the IRS won't do and how to report a scam.

ALMA, WI - In my inbox was an official looking email from the "Internal Revenue Service".

The subject line was: "Tax return request submitted". Without thinking, I clicked on the attachment to the email.

"Did you file our taxes by email?" I asked my husband. It was a silly question. He would no more send our tax return by email than bank by email. The computer was a dragon to be tamed. You only woke the dragon when absolutely necessary.

"NO!" came the answer from the other room. "Delete it! It's a scam!"

I hurriedly clicked "cancel" on the downloading email attachment. Then I noticed the attachment was a .zip file – a big file zipped-up. "Oh, dear," I muttered under my breath.

Even though tax season is over, scammers are still using official looking emails to lure unsuspecting, honest taxpayers into their evil web. I did some research and learned that scammers have many ways to use the IRS name to lure unsuspecting people into their net – phone calls, faxes, emails, fake websites, and even text messages and Short Message Services (SMS).

Scam phone calls are familiar to many people. If you receive a call from the IRS, document the

Don't Click on that Email from the IRS!

Written by Kathleen Vinehout, State Senator 31st District
Tuesday, 21 June 2016 10:48 - Last Updated Tuesday, 21 June 2016 11:07

caller's badge number, name, call back number and caller ID. Then call 1-800-366-4484 to determine if the person is a legitimate IRS employee and really needs to talk with you about your taxes.

IRS email scams are becoming much more common.

The IRS witnessed a 400% increase in email scams this year. A February 2016 IRS alert warned, "The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information."

The IRS also noted there are more email scams seeking personal tax information. When an unsuspecting person clicks on the email, it takes them to official looking websites that masquerade as IRS.gov. These sites ask for personal information like social security numbers. The emails also contain malware or nasty programs that track your keystrokes and allow criminals to impersonate you on-line.

It is important to know that the IRS does not initiate communication with taxpayers by email. Unless that first communication with the IRS is a letter, you can be certain that email message or phone call is a scam.

In a recent new release, IRS Commissioner John Koskinen stated, "We continue to say if you are surprised to be hearing from us, then you're not hearing from us."

Commissioner Koskinen listed a few of the actions the IRS will NEVER do: call to demand immediate payment; threaten to send local police or other law enforcement to arrest or deport you; require you to use a specific method to pay your taxes (like a debit card); ask for a credit card or debit card over the phone.

The real IRS warns that an email claiming to be from the IRS is a phishing attempt and should

Don't Click on that Email from the IRS!

Written by Kathleen Vinehout, State Senator 31st District
Tuesday, 21 June 2016 10:48 - Last Updated Tuesday, 21 June 2016 11:07

be reported at phishing@irs.gov

In Wisconsin, the hardworking consumer protection specialists at the Department of Agriculture, Trade and Consumer Protection (DATCP) protect us from scammers. A few weeks ago, they released a warning about the IRS scammers.

"Fake IRS callers are hitting Wisconsin residents hard," the summer 2016 alert reported. Aggressive callers are "demanding immediate payment for (fake) back taxes."

In a strange twist, telephone scammers in Wisconsin are accepting payment for fake back taxes with PayPal, Amazon and iTunes gift cards. In addition, the scammers will try the usual methods of asking you to wire money through Western Union or MoneyGram.

DATCP officials remind Wisconsinites the IRS will never call you demanding payment or making threats. They will always send a letter by postal mail – not email or phone.

Don't be fooled. If you do receive an email, fax or phone call demanding payment, make sure to report it by calling 800-366-4484 or at IRS.gov. You can contact the Wisconsin Consumer Protection staff at the Consumer Protection Hotline at 800-422-7128.