The University of Texas Rio Grande Valley

Information Security Office

Look out for tax scams

2/9/2018

What is Happening?

This year, the Internal Revenue Service (IRS) announced on Jan. 04, 2018 that the nation's tax season started Monday, Jan. 29, 2018, and that the nation's tax deadline will be April 17 this year.

We encourage that you stay aware for suspicious electronic mail that can potentially be dangerous email scams.

How does the scam works?

Cybercriminals use various deceiving techniques to:

- Disguise an email by making it appear as if it is from an organization executive or legitimate agency (e.g., IRS, FBI, Payroll Office, etc.)
- Trick you into replying sending sensitive information such as:
  - Social Security Number (SSN)
  - Banking information (e.g., Account number, routing number, credit card information)
  - Your W-2 form in order to monetize their theft
- Trick you into clicking on a fake link where you'll be redirected to a fake website asking for your bank's username and password
- Ask you from a [fake] "Executive" that a wire transfer be made to a certain account due to "errors" in the W-2 form
- IRS [fake] "agent" calling you because you are being investigated for tax fraud, and you need to provide your information (e.g., SSN, date of birth, address, direct deposit information, etc.)

What to look for?

Did you know that the IRS doesn't ***initiate*** contact with taxpayer by email, text messages or social media channels to request personal or financial information. Any contact from the IRS will be in response to a contact initiated by you. Cybercriminals, when they learn of a new IRS process, often create false IRS web sites and IRS impersonation emails.

Please remain alert to cybercriminals trying to trick you into giving them your W-2, or other sensitive information by following these tips:

- Beware of links in suspicious emails! **NEVER** click them
  - Hover over the link: Simply place your mouse over the link to see the web address. (Links might also lead you to .exe files. These kinds of file are known to spread malicious software.)
- Scam artists use logos or photos in emails that appear to be connected to legitimate websites.
- **NEVER** download or open any attachments from suspicious emails
- Be cautious of scam phone calls

Steps to take if you become a victim

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, please visit the IRS website and search for the IRS:

- **Taxpayer Guide to Identity Theft**

Do you suspect you might have received a fake email?

Please reach out to our office in order for us to assist you with your incident.

We can be contacted via:

Telephone: (956)665-7823

Email: is@utrgv.edu

Information Security Office