What government shutdown? If it's W-2 time, it's scam time, too

As of Jan. 8, 2019, about 25% of the federal government, including most functions of the IRS and the Federal Trade Commission, is closed. If you think this will stop scammers, think again. Scammers will jump into this vacuum, because the IRS and the FTC are the two principal federal agencies that handle identity theft.

Now that it's W-2 time, you should anticipate that someone somewhere is trying to get your data. Let's take a look at how the tax scam landscape is shaping up this W-2 filing season.

Old scams in new clothes

The IRS has pretty much nailed the W-2 spear phishing ploy, where scammers impersonate a CEO, CFO or some other executive with "Chief" in their title and ask for employees' W-2 data to be emailed to them.

You know enough about this one by now to not respond and to alert your C-suite that any requests for this data must be made in person. If that's not possible, requests must be made in writing and verified before responding.

But if scammers can't get in one way, they'll try another.

We wrote last February about a direct deposit scam. In the latest variation, employees email Payroll, tell you they've changed bank accounts and request corresponding changes to their direct deposit details. To make it more authentic, the tag line—"Sent from my iPhone"—appears in these emails.

Before making any changes to employees' direct deposit details, tell them they must provide you with voided checks. That will take care of any phony emails and you'll also get the routing numbers and checking account numbers right.

If/then

Remember, the IRS doesn't contact taxpayers by email or text. So set up these if/then scenarios for you and your staff to follow:

- If you receive an email claiming to be from the IRS that contains a request for personal information, then you should:
  - Not reply
  - Not open any attachments (they could contain malicious code)
  - Not click on any links
  - Forward the email as-is to the IRS at phishing@irs.gov
  - Delete the original email.
- If you receive an unsolicited text message claiming to be from the IRS, then you should:
  - Not reply
  - Not open any attachments
  - Not click on any links

    - Forward the text as-is to the IRS at 202-552-1226 (standard text messaging rates apply)
    - If possible, in a separate text, forward the originating number to the IRS at 202-552-1226
    - Delete the original text.

Alert the proper authorities

If you have been phished, you should take the following steps immediately:

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide contact information. The subject line should read “W2 Data Loss.” That will guarantee that your email will be can be routed properly. Don’t attach any employee personally identifiable information.
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
- File a complaint with the FBI’s Internet Crime Complaint Center. You may be asked to file a report with your local law enforcement agency.
- Notify employees, so they can protect themselves from identity theft. The Federal Trade Commission’s identitytheft.gov provides guidance on general steps employees should take.
- Forward the scam email to phishing@irs.gov.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002