IDAHO State Tax Commission

Emailing **W-2** or **private individual data?**

Stop. Connect. Confirm.

Criminals are targeting **human resources** and **financial professionals** across Idaho with a new phishing scheme. **Don't fall for this scam.**

Stop.

If you get an email asking you to send employee W-2 or other private/sensitive information, stop to confirm if the request is legitimate before you hit send.

Connect. Confirm.

Criminals have perfected techniques to trick you into thinking an email is coming from a person you work with. Don't fall victim to this scam.

- Connect with the person who sent you the request by phone or face-to-face.
- Don't respond to the email to confirm the sender's request. The sender could be a criminal in disguise using a fake email address.
- If you confirm a legitimate request, take steps to protect the information before you send it.

If you've **received a suspicious email:**

- Forward the email to **Phishing@irs.gov** and place *W-2 Scam* in the subject line.

If you **sent confidential information:**

If you sent W-2 or private individual data to an unauthorized third party:

- File a complaint with the Internet Crime Complaint Center (IC3), operated by the Federal Bureau of Investigation, at **www.ic3.gov.**
- Contact **fraud@tax.idaho.gov** and **DataLoss@irs.gov.**

  For more information, go to **https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers.**

Notify any affected employees to:

- Review the recommended actions by the Federal Trade Commission at **www.identitytheft.gov** or the Internal Revenue Service (IRS) at **www.irs.gov/identitytheft.**
- If a tax return gets rejected because of a duplicate Social Security number or if instructed to do so by the IRS, the employee should file a Form 14039, *Identity Theft Affidavit*, with the IRS and the Idaho State Tax Commission.

For more information on identity theft, visit our website at **tax.idaho.gov/idtheft.**

EIS00375 04-19-2017