



State of Utah

GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

Utah State Tax Commission

JOHN L. VALENTINE
Commission Chair

MICHAEL J. CRAGUN
Commissioner

ROBERT P. PERO
Commissioner

REBECCA L. ROCKWELL
Commissioner

BARRY C. CONOVER
Executive Director

February 8, 2018

Contact: Charlie Roberts (801 556-6318 or charlie@utah.gov)

Utahns warned to hang up when tax scammers call

Just as the tax filing season begins, Utahns are being warned to be aware and defensive about the latest scam to steal innocent taxpayer's money, data and identity.

"If a taxpayer receives a call saying their refund has been deposited into their account in error, they should immediately hang the phone up and contact their bank or credit union to take corrective measures," said Charlie Roberts, spokesperson for the Utah State Tax Commission.

Taxpayers should then contact either the Tax Commission or IRS and report the incident.

Those who receive a direct deposit refund that they did not request are strongly encouraged to take the following steps:

- 1) Contact the automated clearing house department of their bank or credit union where the direct deposit was received and have them return the refund to the IRS or Utah State Tax Commission.
- 2) If an incorrect refund is on a federal return, call the IRS at 1 800 829-4933 to explain why the direct deposit is being returned. If the incorrect refund is from the Utah State Tax Commission, call 801 297-2200 and make the same report.

Although only discovered this week, this new tax scam technique is even more sophisticated than in past years.

For several years, scammers have called taxpayers with threats of criminal action if they did not send money and give identity information,

Cybercriminals now steal data from tax professionals' computers and file fraudulent tax returns. In a new twist, they deposit the fraudulent refund into the taxpayers' real bank accounts.

-more-



State of Utah

GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

Utah State Tax Commission

JOHN L. VALENTINE
Commission Chair

MICHAEL J. CRAGUN
Commissioner

ROBERT P. PERO
Commissioner

REBECCA L. ROCKWELL
Commissioner

BARRY C. CONOVER
Executive Director

2-2-2-2-2

Scammers then contact taxpayers and tell them the refund was deposited into their account in error. They also ask probing questions to obtain identity and sensitive bank information, such as routing numbers.

“The fraudulent caller then gives the taxpayer instructions on how to return the deposit, into what is really the scammer’s account.” Roberts said.

Roberts emphasized that neither the state nor the Internal Revenue Service would ever phone taxpayers demanding identification information to correct such an error.

“We already have individual and business identification information. We communicate personal, sensitive information by either email or regular mail,” he said.

Cybercriminals have evolved from stealing identity to focusing on tax professionals where they can steal client data.

“The vast majority of data thefts of this kind occur because the tax preparer or someone in their office opened a phishing email and clicked on a link that contained malware,” Roberts said.

He explained there are various forms of malware downloaded secretly into computers, allowing thieves remote access to computers.

“These malware allow thieves to steal data stored on effected computers,” Roberts said.

“Unfortunately, this scheme is likely just the first of many that will be identified this year as the State Tax Commission, IRS, and tax industry continue to fight against tax-related identity thieves,” Roberts said.

###