


Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

take months to successfully remove.

Nov. 19, 2018

 **Internal Revenue Service**
United States Department of the Treasury

This Product Contains Sensitive Taxpayer Data

Tax Return Transcript

Request Date: 11-01-2012
Response Date: 11-01-2012
Tracking Number: 12345678910

SSN Provided: 000-00-0000
Tax Period Ending: Dec. 31, 2010

The following items reflect the amount as shown on the return (PR), and the amount as adjusted (PC), if applicable. They do not show subsequent activity on the account.

SSN: 000-00-0000
SPOUSE SSN:
NAME(S) SHOWN ON RETURN: JOHN Q TAXPAYER
ADDRESS: PO BOX 101
ANYTOWN, ST 00000-0000-000

FILING STATUS: Single
FORM NUMBER: 1040
CYCLE POSTED: 20111201
RECEIVED DATE: Apr. 15, 2011

There's a new tax scam going around, this time relating to tax transcripts.

The IRS is warning of a surge of fraudulent emails impersonating the IRS and using tax transcripts as bait to entice users to open documents containing malware.

The scam is especially problematic for businesses whose employees might open the malware because this malware can spread throughout the network and potentially take months to successfully remove.

This well-known malware, known as Emotet, generally poses as specific banks and

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

These clues can change with each version of the malware. Scores of these malicious Emotet emails were forwarded to phishing@irs.gov recently.

The IRS reminds taxpayers it does not send unsolicited emails to the public, nor would it email a sensitive document such as a tax transcript, which is a summary of a tax return. The IRS urges taxpayers not to open the email or the attachment. If using a personal computer, delete or forward the scam email to phishing@irs.gov. If you see these using an employer's computer, notify the company's technology professionals.

The United States Computer Emergency Readiness Team (US-CERT) issued a warning in July about earlier versions of the Emotet in [Alert \(TA18-201A\) Emotet Malware](#).

US-CERT has labeled the Emotet Malware “among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.”

Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved