Cybercrime Prevention Flyer

CPF 0006-2022-CID361-9H **30 March 2022**

Tax Season Cyber Fraud

It is tax season. That time of year when people's thoughts turn to settling their tax obligations and when cybercriminals thoughts turn to stealing your money, your information and maybe your identity. The Internal Revenue Service (IRS) warns that cybercriminals committing tax scams are more active during tax season.

How Do Cybercriminals Get my Personal Data?

Cybercriminals use phishing and smishing techniques to deceive someone into divulging personal data such as banking and credit information, usernames and passwords, and other personal and private details.

In a phishing scheme, a cybercriminal embeds malicious links or attachments in an email and tricks the recipient into clicking the link or opening the attachment. A smishing attack is similar to a phishing attack, with links and sometimes attachments, except that the source is a message received on a smartphone as a Short Messaging Service (SMS) message also known as a text or text message. Smishing is simply a combination of SMS and phishing.

What Happens When a Link is Clicked or Attachment is Opened?

Clicking a link or opening an attachment might install malware on the user's system. Malware infects a computer and allows a criminal actor to access user information stored on the computer. Malware sometimes allows cybercriminals to take complete control of the compromised system and use that system as a launchpad for further criminal activity.

Clicking a link might take the user to a very real looking but entirely fake IRS website that asks the user to log in using their credentials – username and password – in order to address an IRS tax issue. With those credentials and other information easily found on the internet, the cybercriminal can access a taxpayer's online IRS account and redirect a legitimate tax refund or even file a completely fraudulent tax return on the victim's behalf, directing the refund to an account or mailing address the cybercriminal controls.

How do I Recognize an IRS Tax Scam?

There are several telltale signs an email or text message is not genuinely from the IRS.

- Initial contacts from the IRS arrive by United States Postal Service They do not come in emails or text messages.
- Communications from the IRS do not have misspellings or grammatical errors.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

- The IRS will not demand immediate payment or threaten to engage local law enforcement authorities.
- The IRS will not call unexpectedly about a tax refund.

What Should I do if I Receive a Fraudulent IRS Communication?

If you believe a communication that purports to be from the IRS is fraudulent:

- Do not open it or any attachments, or click on any link.
- Do not call any telephone numbers listed in the communication.
- In the case of a text message, forward the text message to the IRS at 202-552-1226.
- In the case of an email, forward it as an attachment to phishing@irs.gov.

What Should I do if I Fall Victim to an IRS Tax Scam?

If you believe you are the victim of a tax scam and have suffered a loss, have found an unauthorized or fake IRS website, or been contacted by someone falsely purporting to be from or representing the IRS, report it online to the Treasury Inspector General for Tax Administration, or by telephone at 800-366-4484, or by U.S. mail to Treasury Inspector General for Tax Administration, Hotline Team, 1401 H Street NW, Suite 469, Washington, DC 2005.

Simple Steps to Increase your Online Safety

- Keep antivirus software up to date.
- Keep computer operating system up to date.
- Consider setting virus definition and operating system updates to automatic.
- Do not use the same password for all accounts. That way, if one password is compromised the risk to other passwords is minimized.
- Block phone numbers and emails of suspected fraudulent callers.
- If you need to contact the IRS or any other taxing authority, find the number or email on their official website. Do not rely on the number in an email or text message.

Additional Resources

Tax Scams May Cost You Money this Tax Season
Tips for Avoiding Tax Season Fraud
Tax Scammers Work Year-Round
Taxpayers beware: Tax season is prime time for phone scams
Avoiding Tax Scams this Season
Six IRS Scams to Watch Out For

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF