



NCCIC

National Cybersecurity & Communications Integration Center

NCCIC ADVISORY

TARGETED TAX FILING PHISHING ATTACKS

April 18, 2011

SUMMARY

This advisory provides general guidance to public and private sector organizations and individuals about potential targeted phishing attacks, or spear phishing. During the tax filing time of year, the US-CERT sees increased spear phishing activity with respect to the income tax filing deadline. The objective of these types of attacks is to lure people to click on links or an attachment within the body of an email; leading that person to malicious computer code. This advisory offers some suggested methods that may minimize the likelihood of an attack becoming successful. We encourage anyone receiving this advisory to widely distribute it

OVERVIEW

Today is the due date for filing US federal income tax returns. As such, it is not uncommon for malicious actors to take advantage of citizens filing taxes electronically to execute phishing attacks via email. Public and private sector organizations and individuals should keep close watch for the following indication that an email may be malicious:

- The sender of the email or initiator of the phone call is your first indication as to whether an email or phone call is legitimate. Be cognizant of how you file, whether electronically or via the mail and whether through a third party tax service or the IRS directly.
- If you file a paper copy but receive an email notification, there is a good chance this is malicious. One should ask how the IRS (or other third party tax support provider) got your email if filing a paper copy. The IRS and third party tax providers do not tend to arbitrarily send notifications via email.
- If you file directly through the IRS online, but you receive emails from third parties stating you are eligible for a bigger refund, or there was an error on your return, treat these emails as suspicious and do not open. Notify the IRS or the third party filing service as to what is happening.
- If you file electronically via the IRS directly, be aware of emails seemingly from the IRS stating there is an error or you are eligible for a bigger refund. Emails can easily be 'spoofed' and can appear to originate from anyone.
- Be aware of extension deadlines. Malicious actors will attempt further emails around the time extensions are due or several weeks after filing deadlines when refunds are expected.

PREVENTATIVE STRATEGIES

The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into 'clicking the link' or opening attachments to seemingly real websites regarding tax filing status. The following represents some best practices to follow but is not an exhaustive list:



NCCIC

National Cybersecurity & Communications Integration Center

- **NEVER click on links in emails.** If you do think the email is legitimate, whether from a third party tax service or the IRS, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- **NEVER open the attachments.** Typically, notifications from the IRS will come via postal service. If there is any doubt, contact the IRS directly and ask whether the email with the attachment was sent from them. This applies to third party tax services as well. It is not typical for providers to send attachments regarding taxes; again, if there is ever any doubt, contact your tax provider directly prior to opening any attachments.
- **Do NOT give out personal information** over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be the IRS or your third party tax support provider, do not give out your personal information. Ask them to provide you their name and a call back number. Contact the IRS (or your third party tax provider) to verify the authenticity of the phone call and then call them back on the provided number.

To learn more about the tax filing process or if you have any questions regarding electronic filing, feel free to contact the IRS directly at:

www.irs.gov

The National Cybersecurity and Communications Integration Center (NCCIC) encourages the public to use safe, common sense cyber practices, such as not opening emails from unknown individuals or organizations, using spam filters and firewalls, running anti-virus and anti-spyware software and keeping them updated regularly. For more information regarding computer security, visit the United States Secret Service (USSS), the United States Computer Emergency Readiness Team (US-CERT) or the Federal Bureau of Investigation's (FBI) 'Be Crime Smart' website at:

www.secretservice.gov/fraud_email_advisory.shtml

http://www.us-cert.gov/reading_room/emailscams_0905.pdf

<http://www.fbi.gov/scams-safety/>

POINTS OF CONTACT

Please direct questions concurrently to the NCCIC and its appropriate component listed below:

NCCIC

NCCIC@HQ.dhs.gov
(703) 235-8831

US-CERT

SWO@US-CERT.gov
(703) 235-8832/8833

NCS/NCC

NCS@HQ.dhs.gov
(703) 235-5080

ICS-CERT

ICS-CERT-SOC@dhs.gov
(877) 776-7585