NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0012-NCCIC 090020120202

DISTRIBUTION NOTICE: THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE. PLEASE ENSURE WIDEST DISSEMINATION.

TARGETED TAX FILING PHISHING ATTACKS

EXECUTIVE SUMMARY

This bulletin provides general guidance to public and private sector organizations and individuals about email attacks—phishing and spear phishing. During the tax filing time of year, DHS, IRS, and law enforcement agencies see increased 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 execute malicious computer code on their computer. This advisory offers some preventative strategies that minimize the likelihood of an attack becoming successful. We encourage anyone receiving this advisory to widely distribute it.

The IRS website (http://www.irs.gov) includes a variety of articles related to phishing, such as, "*Don't be scammed by Cyber Criminals*" (http://www.irs.gov/newsroom/article/0,,id=252313,00.html). Additional response steps, common phishing examples, and IRS contact points are also available through this webpage.

BACKGROUND

During the time period leading up to the deadline for filing US federal income tax returns, there is an understandable increase in email and TV advertisements related to tax filing. As such, it is not uncommon for malicious actors to exploit citizens filing taxes electronically by executing phishing attacks via email or social engineering attacks via telephone. Public and private sector organizations and individuals should keep close watch for the following indications that an email may be malicious or the caller on the phone is not who they claim to be:

- 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 mail and whether through a third party tax service or the IRS directly. If being contacted by phone, ask for that person's name and a call back number.

- If you file a paper copy but receive an email notification, there is a good chance the received email is malicious. The IRS and third party tax providers typically do not send email notifications, especially to taxpayers filing a paper return. If you file a paper return yet receive an email notification, contact the IRS or whomever prepared your taxes, directly.

- If you file your taxes online, but receive emails from other 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 them. Notify the IRS and your tax filing service provider about the email.

Also, be aware of extension deadlines. Malicious actors may attempt to send 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 legitimate websites regarding tax filing status. The following list is not exhaustive, but represents some best practices to follow. To minimize the likelihood of a successful attack, users are encouraged to take the following precautionary steps:

- Do not 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 website log on.

- Do not 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 by 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 without properly verifying the other party's identity. 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.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

POINTS OF CONTACT

To learn more about the tax filing process or if you have any questions regarding electronic filing, please contact the IRS directly at:
http://www.irs.gov

Suspicious e-mails, claiming to be from the IRS, can be sent to:
phishing@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 email scams please feel free to visit:
http://www.us-cert.gov/reading_room/emailscams_0905.pdf

Data breaches which involve a monetary loss or include a financial nexus such as a compromise to your financial, credit or debit accounts, or personal information can be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.
http://www.secretservice.gov/field_offices.shtml

U.S. persons and companies interested in pursuing an investigation of a cyber attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page:
http://www.fbi.gov/contactus.htm