NEWS
CYBER SECURITY
Vol. 7 | Issue 3 March 2022

Welcome to the TXDPS Cyber Security Newsletter!

Tax season is upon us! A time of year when the scammers go into overdrive. Be extra careful while online, and avoid activities that could put your identity and finances at risk.

Let's explore some common tax scams and steps you can take to protect yourself, your identity, and your finances.

Scammers using these tactics generally attempt to create a sense of urgency, or have a good story that would tend to compel you to disclose personal information such as such as your date of birth, social security number, driver's license number, or even usernames and passwords to your accounts.

Common Tax Scams (via CIS):

- **Refund Calculation Scam**: "The IRS recalculated your refund. Congratulations, we found an error in the original calculation of your tax return and owe you additional money. Please verify your account information so we can make a deposit."
- **Stimulus Payment Scam**: "Our records show that you have not claimed your COVID-19 stimulus payment. Please provide us with your information so we can send it to you."
- **Verification Scam**: "We need to verify your W-2 and other personal information. Please take pictures of your driver's license, documents, and forms and send them to us."

How to Protect Yourself:

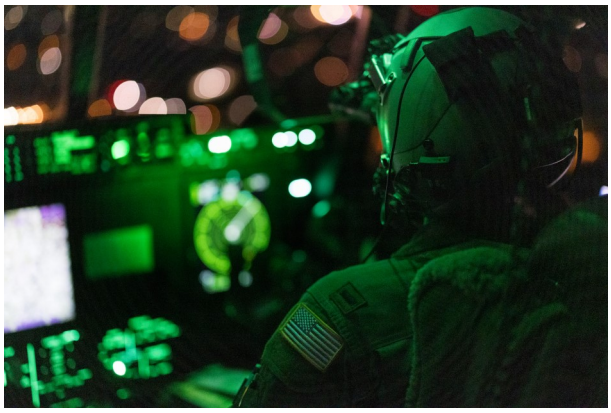
- Remember that *IRS.gov* is the only genuine website for the Internal Revenue Service. All Internet and email communications between you and the IRS would be through this site.
- Never send sensitive information via email. If you receive an email from an unknown source or one that seems suspicious, do not reply.
- The first point of contact by the IRS is typically via postal mail. The IRS will not contact you via email, text messaging, or your social network, nor does it advertise on websites.
- Get An Identity Protection PIN (IP PIN) from the IRS to prevent someone else from filing a tax return in your name.

For more tips: https://www.cisecurity.org/insights/newsletter/Fraud-Alert-Beware-of-Common-Tax-Scams

In the News

'Russian state-sponsored cyber actors' cited in hacks of U.S. defense contractors

(Joe Warmisnky | February 16, 2022)



For more than two years, "Russian state-sponsored cyber actors" have targeted the emails and other data of U.S. defense contractors that handle sensitive information about weapons development, computer systems, intelligence-gathering technology and more, the federal government warned Wednesday.

The alert from the Cybersecurity and Infrastructure Security Agency said cleared defense contractors (CDCs) are the primary victims of the breaches. Those companies are authorized by the Department of Defense to access, receive and store classified information as part of their contracting work. The alert does not say whether classified information was accessed.

The attackers, however, have been able to "acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology," the alert said, by focusing on "enterprise and cloud networks, prioritizing their efforts against the widely used Microsoft 365 (M365) environment."

"The acquired information provides significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and information technology," CISA said. "By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment."

CISA Director Jen Easterly and Bryan Vorndran, the assistant director of the FBI's Cyber Division, urged contractors to use good cyber-hygiene and report suspicious activity as the government works on the case.

Full Story: https://www.cyberscoop.com/russian-state-sponsored-cyber-actors-cited-in-hacks-of-u-s-defense-contractors

A Few More Cyber News Stories:

As Russia invades, Ukrainian government networks suffer high-profile DDoS disruption
https://www.cyberscoop.com/ukraine-government-networks-ddos-disruption-russia-invasion/

White House Denies Mulling Massive Cyberattacks Against Russia
https://threatpost.com/white-house-denies-mulling-massive-cyberattacks-against-russia/178658/

Top senator warns Putin cyberattacks could trigger bigger war
https://www.axios.com/mark-warner-putin-cyber-attacks-ukraine-40c5e959-5093-4d79-bf24-8d4731edb293.html

CYBER CHALLENGE

Don't Get Hooked

This Month's Challenge

For this month's challenge, let's keep those eyes sharp and see if you can avoid getting hooked by a phishing email!

You'll be presented with 8 emails. Look them over and decide whether they are a Phish or a Genuine email.

Please share your results with me as well as your thoughts on the ones that tripped you up, if you miss any that is!

Good luck! (~10 minutes to complete)

https://www.egress.com/resources/cybersecurity-information/phishing/spot-the-phish