

IRS Warns Tax Professionals of New e-Services Email Scam

The Internal Revenue Service today issued an urgent alert to tax professionals who use IRS e-services to beware of an email asking them to update their accounts and directing them to a fake website.

The subject line for the fraudulent email is “Security Awareness for Tax Professionals.” The “From” line is “Your e-Services Team.” It has both an IRS logo and an e-services logo that hyperlinks to a URL verified as a phishing site. The spoofing site poses as an e-services registration page.

The scammers are attempting to exploit current IRS efforts to strengthen the e-services authentication process and its ongoing communications with tax professionals about their accounts. Scammers are attempting to steal e-services usernames and passwords or additional personal data through a registration page.

If e-services users have already clicked on the fake logo and provided their username and password, they should contact the e-services help desk to reset their accounts. If the same password is used for other accounts, these should be changed as well. As an extra precaution, users should perform a deep security scan on their computers, re-evaluate their security controls and be alert to any other signs of identity theft or data compromise.

Tax professionals should always go directly to IRS.gov to access e-services and never click on any links provided in emails.

Tax professionals who receive a suspicious email should send it as an attachment to Phishing@irs.gov and then delete it. Recipients should not click on any links.

The scammer email tells recipients that information was stolen from certain user accounts in 2015 from a state-sponsored actor. It says users are being asked to upgrade their e-service account to ensure protection of their information. It asks them to click on the login to access their accounts for security upgrade.

The IRS is in the process of upgrading e-services security and has been in communication with tax professionals about updating their accounts.

The IRS, state tax agencies and tax industry partners working together through the Security Summit have an awareness campaign underway called [Protect Your Clients; Protect Yourself](#). The objective is to remind tax professionals they increasingly are the targets of identity thieves seeking ever larger amounts of taxpayer data to file fraudulent tax returns.

Security Summit partners recommend tax professionals:

- Always use robust security software
- Use encryption software to protect taxpayer data
- Use strong passwords and change them often
- Learn to recognize phishing emails attempting to steal data
- Never click on links or download attachments from suspicious emails
- Beware of any communications claiming to be the IRS that are outside normal channels

Review [Protect Your Clients, Protect Yourself](#) for various steps you can take to protect your customers' information and your business.