CPA
Practice Advisor

beware of their inbox – specifically the successful email scams dubbed spear phishing that identify themselves as a friend, customer or company.

Jul. 07, 2017

The IRS is warning tax professionals to increase their computer security and to beware of their inbox – specifically the successful email scams dubbed spear phishing that identify themselves as a friend, customer or company.

As part of the Security Summit effort, the IRS, state tax agencies and the tax industry next week will kick off another series in the Protect Your Clients, Protect Yourself

campaign called “Don’t Take the Bait.” It’s critical that tax professionals remember

scams.”

Phishing scams use bait or lures to trick preparers into opening an infected link or attachment or disclosing usernames and passwords to critical accounts. Falling for the phishing bait means exposing taxpayer data to theft. Thieves also are interested in stealing preparers’ e-Services passwords, Electronic Filing Identification Numbers (EFINs), Centralized Authorization File (CAF) numbers and Preparer Tax Identification Numbers (PTINs.)

From January through May, there were 177 tax professionals or firms who reported data thefts involving client information involving thousands of people. The IRS currently is receiving three to five data theft reports a week from tax practitioners. Not all data losses are due to phishing scams but stopping this commonly used tactic by cybercriminals would do much to lessen the current losses.

“We’ve been warning tax professionals that they are increasingly the targets of national and international cybercriminal rings. These syndicates are well-funded, knowledgeable and creative. It’s going to take all of us working together to combat these identity thieves,” Koskinen said. “But doing nothing or making a minimal effort is no longer an option. Anyone who handles taxpayer information has a legal responsibility to protect it.”

The Security Summit will focus the “Don’t Take the Bait” series on security awareness, emphasizing the various types of phishing scams – a common and successful tactic used in data breaches. The 10-week series of news releases, which begins July 11, also will focus on what steps tax professionals can take to protect their clients and their business from these attacks.

This effort is part of the Summit’s “Protect Your Client, Protect Yourself” education series aimed at tax professionals. The IRS and Summit partners also have been

encouraging individual taxpayers to increase their security awareness through the

The Anti-Phishing Work Group (APWG), a not-for-profit industry association focused on eliminating the identity theft and fraud resulting from phishing, reported seeing a significant increase in phishing activities in 2016.

APWG reported that the total number of unique phishing attacks in 2016 was 1.2 million – a 65 percent increase over 2015. APWG now sees 92,564 unique phishing attacks per month – a 5,753 percent increase over the last 12 years. Each phishing attack may involve millions of emails.

Phishing.org reports there are more than 100 billion spam emails sent each day; more than 85 percent of all organizations have been targeted by phishing attempts and phishing damages exceed $1 billion.

Verizon, which publishes an annual data breach investigations report, warns that 1 in 14 users are tricked into opening a link or attachment from a phishing email. A quarter of the victims have been duped more than once.

Verizon's 2017 report found that 95 percent of successful phishing attacks include some sort of malware software installation that allows thieves to export data or take control of the systems. It found most hacking efforts – 81 percent – used either stolen passwords or accessed weak passwords.

The number one goal of phishing thieves is to monetize their stolen information. As the IRS, states and tax industry have made inroads into tax-related identity theft, criminals need even more information to better impersonate taxpayers. This is why tax professionals, who hold sensitive financial data, are critical targets.

Tax return information stolen from practitioners enables the thieves to better masquerade as legitimate taxpayers and make it harder for the IRS and states to identify a suspect return. It is critical that tax professionals experiencing a data loss

immediately notify the IRS and states so that they may take action that prevents

Nationwide Tax Forum at Orlando, Fla., and ends September 12 with the final Nationwide Tax Forum at San Diego.

The IRS, working with its partners in the tax community, will focus on tax professional security issues as part of the five-city Tax Forum series. Tax professionals are encouraged to attend.

Advisory • Technology