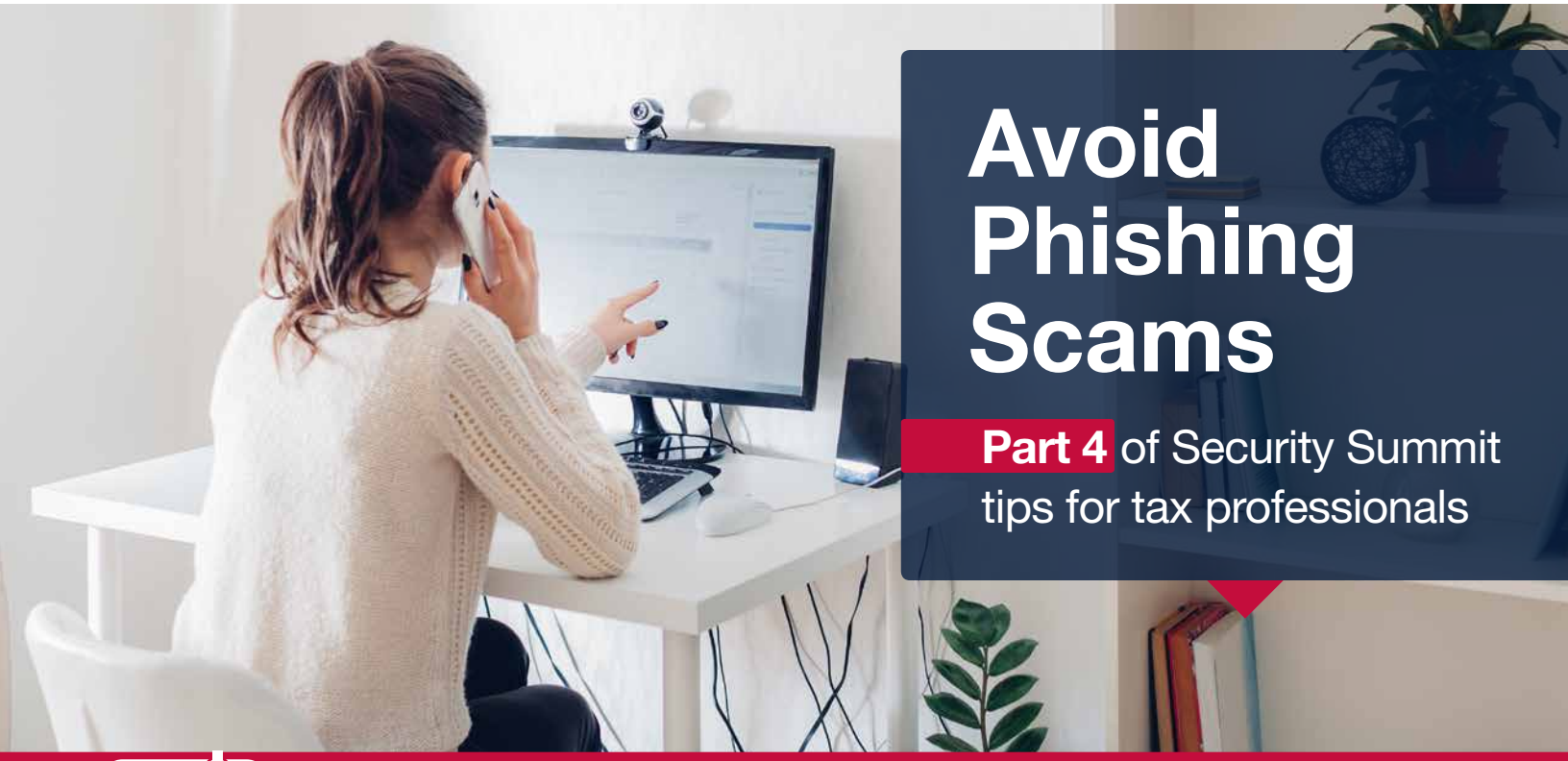
www.irs.gov/securitysummit

Working Virtually: Protecting Tax Data at Home and at Work

A five-part series from the IRS and Security Summit partners



Avoid Phishing Scams

Part 4 of Security Summit tips for tax professionals

As tax practitioners increasingly turn to telework, they must be alert to email phishing scams, especially those taking advantage of COVID-19 and Economic Impact Payments. Creating a data protection plan is critical as cybercriminals step up efforts to steal client tax information.

Here's what tax professionals should know:

- Most data thefts start with a phishing email trick.
- Identity thieves pose as trusted sources – a client, your software provider or even the IRS – to lure you into clicking on a link or attachment.
- Remember, don't take the bait. Learn to recognize and avoid phishing scams.
- Create "trusted customer" policies; contacting potential clients by phone or video conference.

Generally, phishing emails:

- have an urgent message, such as your account password expired.
- direct you to an official-looking link or attachment. The link may take you to a fake site made to appear like a trusted source to steal your username and password.
- or the attachment may contain malware, which secretly downloads and allows thieves to eventually steal all the tax pro's passwords.

Taxpayers and tax preparers can report suspicious emails posing as the IRS to phishing@irs.gov.

Publication 5433-C (8-2020) Catalog Number 74832E Department of the Treasury **Internal Revenue Service** www.irs.gov