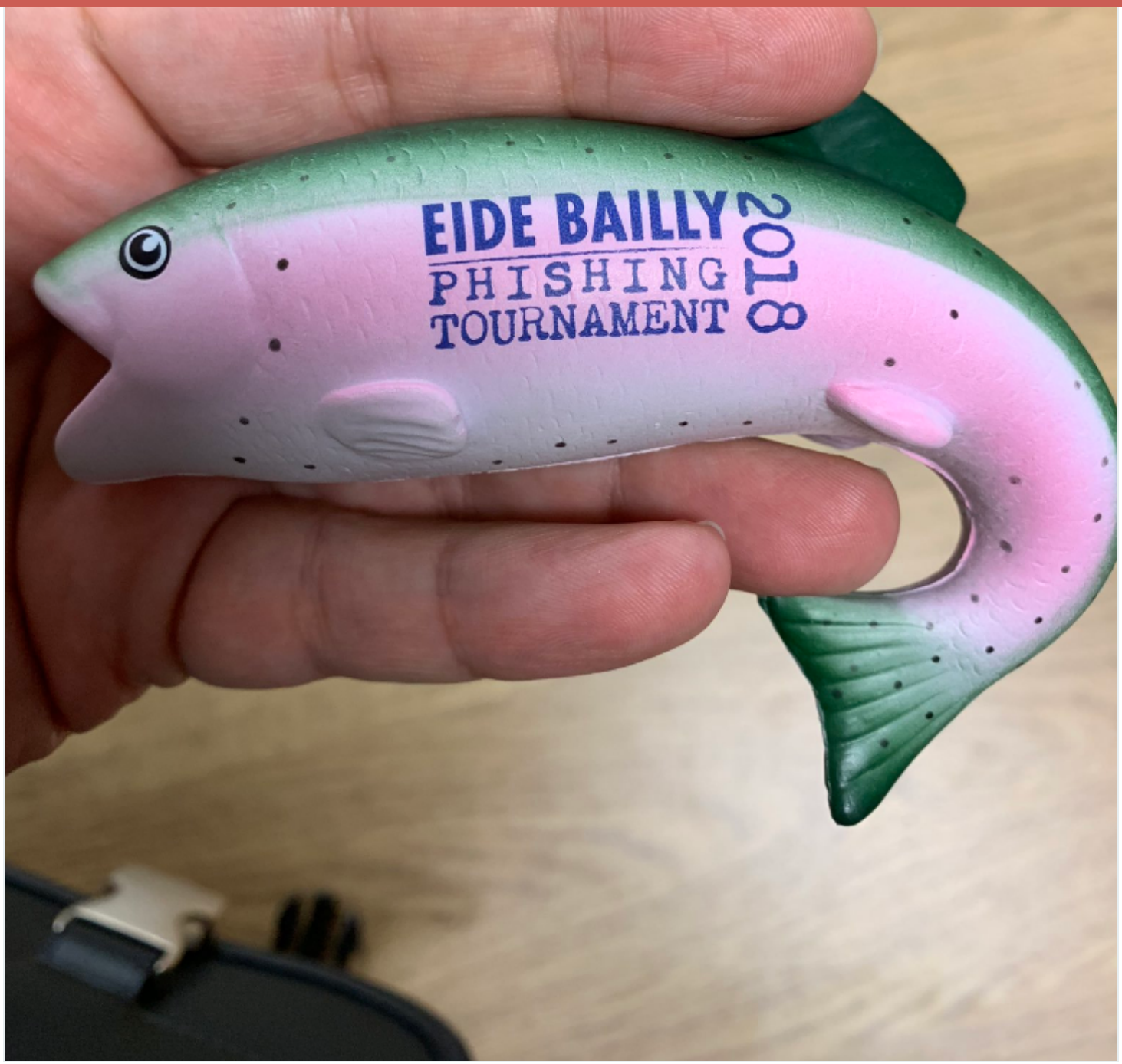
fall, an international CPA firm association commissioned me to create some materials and resources for their firms.

Brian Tankersley • Jan. 16, 2021



This year, we've seen an increase in the number of phishing attacks targeted at accounting professionals and accounting firms. The IRS has been more vocal than usual this year, and all of the tax software companies have tightened up the login

requirements for anyone who has access to electronic filing. Security journalist

more likely to fall victim to the attacks.

E-mail based malware and phishing attacks are frighteningly simple to create. Last fall, an international CPA firm association commissioned me to create some materials and resources for their firms. During the project, I set up the open source hacker tools available to perpetrate such an attack, including GoPhish, several bulk commercial e-mailing services, and free SSL certificates from LetsEncrypt.org on a Microsoft Azure server I rented by the hour. With a small budget and these tools, it was relatively simple to create fake websites, fake e-mails, and tracking servers which stored the legitimate usernames and passwords entered by the victims. While I didn't use the tools on anyone outside my organization, it was interesting to know who clicked on links in messages, and it was eye-opening to show the victims the usernames – and passwords – which they typed into my phishing web server.

All of this highlights the need for ongoing security training – for everyone in your office. Just as many production employees are required to be trained in the safe operation of equipment, office workers should have security awareness training every year. These training sessions can be run internally by your information technology/security staffers, or you can use one of a growing number of services which provide the training and awareness for a monthly fee. These firms usually send their initial phishing test e-mails out unannounced to employees, inform them of their mistake and establish a pre-training baseline.

Your team will then complete a computer-based training, a webinar, or an in-person training class to help them identify common techniques used by scammers. After completing the training, employees are periodically sent phishing messages, and if they fall victim to them, they are assigned additional training and monitoring. Management can review the results of the campaigns, and your IT team can also customize the e-mails to match the kinds of messages received by the firm. You can

learn more about some of these service offerings at the Gartner Group's reviews site

fraudsters figure out that accountants are the information banks of the digital world, they will target our firms more aggressively, and those who do not train their employees will pay a price.

==========

Brian F. Tankersley, CPA.CITP, CGMA (@BFTCPA, CPATechBlog.com) advises firms and companies on accounting technology issues. He has served as the technology editor for a major accounting industry publication, and currently teaches courses in the US and Canada through K2 Enterprises for professional accounting organizations across the US and Canada. Brian and his family make their home in Farragut, Tennessee.

Firm Management • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.