Few Professionals Are Fully Confident in Ability to Assess the Effectiveness of Their Phishing Defenses

New guide highlights findings from ISACA phishing survey and offers best practices for improvement

Sydney, NSW, AUS (21 March 2019)— Findings from a recent ISACA survey about strategies for phishing defense showed that only 12 per cent of the roughly 1,5000 respondents were completely confident in their ability to assess the effectiveness of their phishing awareness efforts. In the new paper, Phishing Defense and Governance, released in partnership with Terranova Security, ISACA outlines key takeaways from this phishing research that reached security, assurance, risk and governance professionals, including: Only a slight majority (63 per cent) regularly monitor and report on the effectiveness of their activities. 38 per cent of respondents reported that their organisations develop security awareness collateral and anti-phishing materials internally. 85 per cent of enterprises measure and regularly report on the effectiveness of their phishing awareness programs There is still a divide when it comes to organisations employing awareness activities such as email newsletters and online and in-person training, when compared to assessments of what employees have learned, through simulations and other knowledge-based tools. Simulation is not a common component of phishing awareness and training, with only 57% of those surveyed saying they perform phishing simulation, and 25% reporting they use other active knowledge-based assessment of employee phishing behavior. "Current phishing defense strategies and implementation are clearly not hitting the mark," said Frank Downs, director of cybersecurity practices at ISACA. "Strengthening these defense activities and improving outcomes is within reach, but requires careful planning and execution, and eliminating any gaps in managing and implementing these security awareness initiatives internally and externally." Phishing Defense and Governance also examines the potential correlation between joint internal and outsourced collateral development and the increased ability to report and measure on effectiveness, as well as the ways in which external service providers can be used to help support phishing defense. The white paper also provides some main areas of improvement where professionals should focus their attention when seeking to improve their phishing defenses, including: Ensuring the organisation has the capability to validate user behavior modification (such as through a phishing simulation) Evaluating the outsourcing or co-sourcing relationships in place and determining where the organisation has gaps in the quality of information it is receiving Setting clear goals for improvement and tracking to them "Phishing attacks continue to grow each year both in number and in cost to organisations globally and countless new phishing scenarios are created every day," said Theo Zafirakos, CISO at Terranova Security. "While human error continues to prevail as the leading cause of all breaches and security incidents, security professionals agree the most effective way to reduce human risk is with security awareness and phishing simulation training." The Phishing Defense and Governance whitepaper can be downloaded for free at www.isaca.org/phishing. For another perspective on phishing, read this ISACA Now blog post, "The C-Suite is the New Main Target of Phishing," by Harold Walker, CISSP, Phishing Awareness Evangelist, Terranova Security. About Terranova Security Terranova Security is a global leader in security awareness training, recognised by Gartner®, with 1000+ successful phishing awareness and security awareness training programs spanning over 6-million users. Terranova Security is committed to partnering with CISOs and security professionals to help reduce human risk and support each organisation with a personalised and consultative approach for phishing and awareness training needs. Uniquely positioned to support security leaders govern, manage and measure changes in behavior, Terranova Security provides true flexibility and delivery models for phishing and security awareness training. Learn more: terranovasecurity.com About ISACA Now in its 50th anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organisations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China. Twitter: www.twitter.com/ISACANews LinkedIn:www.linkedin.com/company/isaca Facebook: www.facebook.com/ISACAHQ Instagram:www.instagram.com/isacanews/ Contact: Julie Fenwick, 0468 901 655, jfenwick@daylightagency.com.au Lauren Graham, 0432 614 401, lgraham@daylightagency.com.au

Contacts

Julie Fenwick
The Daylight Agency
mailto: