INGRAM MICRO CLOUD Cybersecurity

Installing Antivirus on the Brains of Your Users: The Importance of Security Awareness Training

Attackers are more focused on manipulating the human element than ever. How can you "install antivirus on the brains of your users?" With security awareness training! We spoke to Ingram Micro Technology Consultant II, Jacob White, to learn more about security awareness training and how it can help educate users in making the best decisions and keeping company information safe.

Attackers in the modern era have found great success in using social engineering to meet their goals

Social engineering, or the act of psychologically manipulating users into divulging information, has become a major threat to the security of today's organizations. Attackers are very focused on the people element. In fact, according to the Verizon 2021 Data Breach Information Report, the first way hackers got into a network was through phishing attacks, and the second was with stolen credentials (which can be obtained from social engineering methods).

How does the "human element" play a part?

Social engineering capitalizes on humans' natural instinct to communicate. In today's world, we have so many ways to communicate, whether it be traditional methods like phone or email to more modern collaboration tools like Microsoft Teams, Zoom, Slack, and others. For a hacker, these are all opportunities to breach, and humans are often known as the weakest link in a security chain. Security Awareness Training looks at the way that we interact with one another on these platforms/tools and then simulates how one would behave. Through tools and assessments, we can send simulated attacks to our users and see if they fall for it. Follow-up occurs whether the employee "passes" or "fails:" We congratulate the user who successfully identifies the attempt, and we help further educate the employee who may click or divulge information.

How do simulated attacks work?

A simulated attack is most frequently comprised of phishing (email) or vishing (voice). Traditionally, this has been offered as a service – experts craft the phishing messages, perform the attack, and give a report card after the engagement. That's great for "point in time" checks, however you want to ideally run these simulations continuously over time to gauge learning and compliance through multiple campaigns. Intersperse education in between campaigns to ensure employees have enough knowledge to act properly, and over time you will see the metrics of compliance rise.

How should security awareness training be approached?

Over time, users become more resilient to these methods and can identify bad behavior to protect themselves and the organization from attack. Keep running simulations and create a continuous process, measure each round compared to the previous and don't be afraid of failure. Reward those who can see the social engineering elements, and don't punish those who click – provide more guidance and education. Incentivize good performance.

Ingram Micro's Cybersecurity Delta Force is here to help connect you to security awareness training assessments & vendors. Leverage our team to help work through available options that meet your needs! Contact us at cybersecurity@ingrammicro.com to learn more!