BLUE GOAT CYBER

Phishing Exercise Services

Steps to Schedule Your Phishing Exercise:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

Our email phishing campaign involves crafting scenarios that are delivered via email to entice users to divulge sensitive information, click on malicious links, or open infected attachments. We perform an email phishing campaign using OSINT (Open Source Intelligence) on your user population. OSINT is information that is publicly accessible. We use this information to discover information about your users, including their work email addresses. We then craft scenarios for users, subsets of users, and individuals to maximize the email phishing campaign success. The OSINT allows us to tailor the phishing campaign to your environment and user characteristics.

We provide a list of all user email addresses we are able to discover on the Internet using our OSINT methods. Alternatively, we are happy to test a targeted group of users, based on information you provide to us.

With your permission, we test these email addresses, as well as explicit email addresses, as provided. We use at least two (2) different email messages/tactics against your users. We measure how many users fall for the phishing ploy – click on a link, divulge information, or open an attachment. We determine constraints of the phishing campaign, such as what types of information (usernames, passwords, etc.) we can gather, during the Rules of Engagement process.

If you already utilize an automated phishing training service that takes users that fall for the phishing templates to a phishing training website or CBT, our phishing service will help validate the effectiveness of your phishing training service. Training without validation is useless.

BENEFITS / RETURN ON INVESTMENT (ROI)

Our Phishing Exercise testing services provides an economic way for you to measure the effectiveness of your Security Awareness training. Many attackers use social engineering tactics to take control of your systems. People, processes, and technologies have to work in concert to achieve a secure environment. Our Phishing Campaigns test the people part of this triad.

DELIVERABLE

The **Phishing Exercise Report** covers tactics used for the phishing campaign and analytics will be provided for the email campaign that show how many users "fell" for the tactic used by clicking on a link or opening an attachment. Samples of phishing emails will be included in this section of the report.

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

(307) 317-8884
info@bluegoatcyber.com