Phishing Overview

2019
**Phishing**
Phishing is common cyber-attack that uses fraudulent emails to trick recipients into believing they are receiving a legitimate message with the hopes of an individual clicking a link or downloading an attachment. These scams are an attempt to obtain confidential information such as financial or personal information or to gain device or network connectivity through malware or stolen credentials.

**Our Strategy**
At McAfee, we regularly “phish” the entire enterprise, by sending out training phishing emails to all employees. Employees are never warned about when these emails will come in. The structure and difficulty is changed on every occurrence and timing of these tests always varies.

Employees are trained to report any suspected emails, including these training phishes, via an accessible phishing button. All metrics are fed back to our Information Security Team to investigate.

At McAfee, we understand that the sophistication of these attempts can vary and come in a range of different forms depending on the target, and that certain departments are more at risk of being targeted than others. Along with regularly phishing the entire enterprise, we prioritize higher risk departments with extra testing.

Once tests are completed, all metrics of phishing attempts are gathered. These include all emails which were opened, those who clicked on attachments or links, and those who reported the attempt to our dedicated investigation team. After these have been gathered and organized, we share phishing stats with our business units to emphasize the importance with the goal of increased reporting and decreased clicking.

Through continued education, and investigation, McAfee is ensuring that awareness amongst employees is kept at a high level for attempts like these. We understand these types of attack can come in many different forms, at any time, and through any employee, so we ensure that our staff are trained and prepared to deal with any attempt which come their way.

**Types of Phishing**
**Spear Phishing:** Targeted phishing emails that are carefully designed to target a specific user. Most commonly used type of phishing attack. Phishers research about the targeted user or an organization through social media or a company website.

**Whaling:** Similar to spear phishing but the targeted user is more specific such as CEO, CFO, COO or another other type of senior management.

These cyber-attacks are getting more sophisticated and harder to detect if an email is real or fake.

**Vishing:** A phishing scam that is done over the phone. Voice + phishing = vishing

**SMiSHing:** A phishing scam that is conducted through text or SMS messages.
FRM: 18443693848
MSG: Your card has been put on hold. CALL now free: 1-844-369-3848 and follow instructions to resolve this issue.