JAMES HAMMON & CO.

CYBER SECURITY: PHISHING ATTACK PREVENTION AND EDUCATION

Version 1.0

Project Manager:

Cameron Beveridge

EXECUTIVE SUMMARY

The following project aim to prevent future phishing attacks by informing and educating employees of phishing attacks and how to identify them, to prevent any risks to the company or the employees.

The project will use a fake email account to be posing as a department within the organisation requesting employees to click on a corrupted link.

The corrupted link will provide the company with details of people who click on the link and how many people who clicked don the link. The link will also redirect employees to a government agency to inform employees on cyber-attacks.

Key Objectives

- Educate employees on cyber attacks
- Identify high risk employees
- Create a fake phishing email
- Prevent future cyber attacks
- Improve employee safety
- Improve company safety

PROJECT SCOPE

Scope

James Hammon & Co. has been experiencing issues related to email phishing attacks on employees. The following project aims to identify high risk employees, gather information on the frequency of attacks and educate employees on phishing attacks to reduce security breaches.

This is to be achieved through the creation of a ‘fake’ phishing email created by the company that will be sent to all employees.

Key objectives

- Identify high risk employees
- Educate existing employees on phishing attacks
- Reduce cyber security breaches
- Generate diagnostic email for phishing attacks

TEAM MANAGEMENT

Department

Information and Technology

Task Requirements

- Create ‘fake’ email address
- Provide text within the email requesting employees to click the embedded link
- Generate a false link that redirects employees to a message of warning to phishing attacks and a link to the Australian Signals Directorate (cyber security) for information.
- Embed a click tracker in the link to determine high risk employees and to collect data to reduce the risk of future attacks.
- Collect and deliver data to the director.

Diagnostic Email

The following details the information embedded within the email and the email address to be created.

Email Address

The email address will be created from the company email with a relatively generic email address that uses a departments name.

Proposed email: payroll@bevhawk.com.au

Email Message

The email message will inform employees of changes to their payable account for their salary. The email will then ask employees to complete the form embedded in the email. This will be in the form of a hyperlink.

Proposed message:

Hello Everyone,

The payroll system is currently being updated with a new service. The payroll team requires all employees to complete payroll payable accounts form so that all employees can receive their salary before the next payment.

Please complete the form embedded within the link below.

Payroll payable accounts form

We apologise for any inconvenience you may have experienced.

Kind regards.

Information Site

The proposed site to inform employees of online scams will be an Australian government website.

Proposed site: https://www.scamwatch.gov.au/

URL Click Tracker

Click trackers will determine how many employees clicked on the link and the email accounts associated with the click.

Proposed Click tracker:

- Plerdy Click tracker – Includes a free trial of the tracker.
- Click Tracker.com
- Clickmeter.com

COST ANALYSIS

The following highlights costs of the project.

The project is not expected to create any additional costs to the company. The cost would be covered by the IT departments annual salary.

Item	Cost ($)
Email address	**0**
Click Tracker	**0 (free trial)**
Hyperlink	**0**

PROJECT OVERVIEW

The proposed diagnostic phishing email is not expected to cost the company any additional costs. The project is predicted to be completed within the week of acceptance of the proposal. The email will provide the company with greater awareness of high-risk employees and inform employees of the risks of phishing scams to protect themselves and the company.