****

INSERT LOGO HERE

INSERT LOGO HERE

**ANTI-PHISHING POLICY**

**Internal Use Only**

Reference: ACME-GAPP-v1

|  |  |
| --- | --- |
| **POLICY APPROVER:** Chief Information Security Officer | **DATE:** October 18, 20XX |
| **POLICY CONTACT:** Information Security Manager  **SCOPE:** Global | **LAST REVISED:** October 18, 20XX  **APPLICABILITY:** All Employees |

1. **INTENT**

The policy outlines how ACME Corporation defends itself against Phishing attacks resulting from the use of social engineering techniques. This may occur via phone, text messages, social media channels or emails. Aside from the theft of information, attacks can install malware (such as ransomware), sabotage our systems, steal money through fraud or it could be the first step in a targeted attack against our company, where the aim is something much more specific, like the theft of sensitive data.

This policy is in line with ACME Corporation’s purpose, values, and principles. If you have any questions about this policy, please consult the Policy Contact listed above or your local HR representative.

1. **ABIDING BY THIS POLICY**

Violating this policy may result in disciplinary action, consistent with local laws, up to and including termination. Employees affected by this policy are expected to read and follow it, directing any questions to the Policy Contact.

1. **POLICY**

ACME Corporation adopts a multi-layered defense to combating Phishing attacks which incorporates a combination of technological, process, and people-based approaches. By widening our defenses, we can improve our resilience against Phishing without disrupting the productivity of our users. It also offers multiple opportunities to detect a Phishing attack, and then stop it before it causes harm.

**The approach splits our efforts into four areas on which we can build our defenses:**

**1**. Making it difficult for attackers to reach our users

**2.** Help users identify, and report suspected phishing emails

**3.** Protect our organisation from the effects of undetected phishing emails

**4.** Respond quickly to incidents

* 1. **MAKING IT DIFFICULT FOR ATTACKERS TO REACH OUR USERS**

We filter or block Phishing emails as much as possible before it reaches our users using a variety of techniques including IP addresses, domain names, email address welcome/block list, public spam and open relay block lists, attachment types, and malware detection. We also honour anti-spoofing policies of the sender's domain.

Attackers 'spoof' trusted emails, making their emails look like they were sent by reputable organisations. These spoofed emails can be used to attack our customers, or people within our company. We employ specific anti-spoofing controls (such as DMARC, SPF and DKIM3) to make it harder for email from our domains to be spoofed.

Attackers use publicly available information about our company and users to make their Phishing (and particularly spear phishing) messages more convincing. This is often gleaned from our website and social media accounts (information known as a 'digital footprint').

**All staff need to conscious of the impact of:**

* Information shared on our company websites and social media pages (i.e., what do visitors to your website need to know, and what detail is unnecessary but could be useful for attackers?)
* What our partners, contractors and suppliers give away about our company online
* How sharing personal information has the potential to affect both them and the company
  1. **HELP USERS IDENTIFY, AND REPORT SUSPECTED PHISHING EMAILS**

We utilise the following mechanisms to ensure that our staff understand the nature of the threat posed by Phishing and how best to deal with them.

* Succinct learning videos incorporating real examples and case studies to make the threat tangible, without overwhelming
* Online interactive learning activities (e.g., quizzes, gamification) which are both engaging and informative
* Provide additional guidance to business areas more vulnerable to Phishing such as customer-facing departments or staff authorised to access sensitive information, manage financial assets, or administer IT systems
* Monthly simulated Phishing campaigns coupled with ‘on-the-spot’ learning

It is important for us to have a good reporting culture where our staff are willing “ask out loud” for support and guidance when something feels suspicious, unexpected, or unusual. This provides the company with vital information about the types of Phishing attacks are being targeted at our company and situations where legitimate emails are getting mistaken for Phishing.

**Our monthly simulated Phishing campaigns are supported by in person reinforcement as outlined below:**

* An initial click sees the staff member receive ‘on-the-spot’ notification and a short learning video
* On a second click, a pre-drafted informal letter is sent to the staff member
* Upon a third click, the staff member will receive a detailed training video along plus a session with their Supervisor to ensure that they fully understand the need for vigilance
* For the fourth click, the employee will receive more extensive education plus a meeting will be held with their Line Manager
* A fifth offense will result in a formal written warning
* All additional clicks will lead to further formal disciplinary action

Whilst we make every effort to support and encourage our staff to employ secure behaviors by way of recognising and dealing with Phishing attacks, where staff members demonstrate consistent unsafe behaviors evidenced as part of simulated Phishing responses, the Company feels it no choice but to enact formal disciplinary procedures.

* 1. **PROTECT OUR ORGANISATION FROM THE EFFECTS OF UNDETECTED PHISHING EMAILS**

As Malware is often hidden in fake websites that a user is directed to as part of a Phishing attack, it is critical that we have well configured devices and good end-point defenses can stop Malware installing, even if the email is clicked. Our software and devices are always kept up to date with the latest versions from software developers, hardware suppliers and vendors to prevent attackers from leveraging known vulnerabilities.

Passwords are a key target for attackers, particularly if they are for accounts with privileges such as access to sensitive information, handling financial assets, or administering IT systems.

**We make our login process more resistant to Phishing by:**

* Limiting the number of accounts with privileged access to the absolute minimum
* Using two-step/two-factor verification whenever practical so that an attacker cannot access an account using just a stolen password
* Only providing privileged access to people who need it for their roles and regularly reviewing users that have been provided with privileged accesses to ensure that they are still needed
* Remove or suspend accounts that are no longer being used
  1. **RESPOND QUICKLY TO INCIDENTS**

We recognise that all organisations will experience security incidents at some point, so it is crucial that we are in a position to detect them quickly and respond to them in a planned way to limit that harm caused.

We have technical security monitoring capabilities in place to pick up on incidents that users are not likely to become aware of. This incorporates proactive monitoring against known threats. We keep our monitoring capability up to date to ensure it remains effective.

In addition to monitoring, we have detailed incident response plans in place which are practiced on a regular basis to ensure that everyone is familiar with their roles and knows who to call for further support.

1. **CONTACT INFORMATION**

**General Enquires:** For general enquiries, please contact the Policy Contact listed above or the Service Desk.

**Reporting Potential Policy Violations:** If you feel this policy has been violated, you have many resources available to help you, including your immediate manager, your HR representative and the Policy Contact listed above. We will follow the Company’s Incident Response Guidelines for any reported violation.

1. **ADDITIONAL INFORMATION**

**Future Modifications of This Policy:** ACME Corporation reserves the right to modify this policy as needed, for example, to comply with changes in laws, regulations or Company practices and procedures.

1. **DEFINITIONS**

**Phishing:** Fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

**Malware (malicious software):** Any program or file that is harmful to a computer user including computer viruses, worms, Trojan horses, and spyware.