AMBERSAIL

Cyber Security Awareness Policy

Sample Copy

Companies need to ensure that staff are always aware of the threats posed by cyber security fraud.

Threats are constantly evolving as criminals become more sophisticated and creative.

To help combat the threats from cyber fraud, a company should have policies and procedures to support what it does. This includes staff education.

Threats come in many forms and companies should remain vigilant. Reviewing what steps are being taken to reduce risks and keeping up to date with developments.

This policy document has been developed by Ambersail – a specialist cyber security and penetration testing company. It provides a framework for a company cyber security awareness programme.

Obviously, this is a generic example. Feel free to modify your approach to suit.

More can be found on Ambersail's awareness services here: https://www.ambersail.com/cyber-security-awareness/.

Document Reference	Cyber Security Awareness Policy - Ambersail Sample
Date	31/07/2019
Document Status	Final
Version	1.0
Revision History	1.0 – 31/07/2019: Sample release.

Table of Contents

1. Policy Statement

This document details **<COMPANY>’s** policy in relation to cyber security awareness.

<COMPANY> recognises that there are significant business risks posed by criminals and fraudsters who attempt to capitalise on staff behaviours.

Detailed below are the security standards and procedures required to maintain an acceptable level of staff awareness to counter cyber security and social engineering attacks.

These procedures have been developed according to industry best practice standards such as ISO 27001.

More importantly, the policy is regularly reviewed and maintained to keep pace with the constantly evolving tactics employed by criminals and fraudsters.

- This document should be viewed in conjunction with **<COMPANY>’s** top level security policy. This can be found here **<ENTER REFERENCE DOCUMENT HERE>**.

2. Review and Update of the Policy Statement

The Policy Statement and associated company Policies are reviewed at least annually by **<COMPANY>’s [RESPONSIBLE TEAM]** to ensure:

- The business meets its compliance obligations to **<STATE HERE>**.
- Continually evolving threats are identified, evaluated and recorded. Any defensive actions and countermeasures are adopted.

The **<COMPANY>’s [RESPONSIBLE TEAM]** shall undertake the technical review of this policy statement and associated company Policies.

Any changes to this policy will be communicated to **<COMPANY>’s [RESPONSIBLE TEAM]** and any other necessary 3rd parties.

3. Purpose

Cyber Fraud represents a very real threat to the profitable operation of the company. Fraud attempts are often targeted at both individual staff as well as larger indiscriminate groups

It is very important that people understand the nature and appearance of fraud attempts and how to deal safely with any fraudulent communications.

4. Scope

This document provides operational guidelines for individuals having access to networks and electronic and physical facilities at **<COMPANY>**.

This includes (and is not limited to):

- Permanent members of staff.
- Contract members of staff.
- Third Party Service Providers.
- Site visitors.

5. Policy

5.1. Fraud & Theft Threats

Fraud and theft attempts are continually evolving.

Major threats are currently understood to come from:

5.1.1. Emails

Staff should take great care with all email communications. **<COMPANY>** receives many phishing emails each day.

Phishing emails often appear to be sent from trustworthy sources. However, these emails are crafted to trick the recipient into disclosing sensitive and confidential information.

Phishing emails normally contain plausible subjects with supporting links or attachments. Links will normally take the victim to a bogus site where they are expected to provide confidential details which are then used by criminals. Clicking on attachments can often introduce viruses or malicious software onto the victim's computer, which can quickly spread to the company network.

<COMPANY> makes every effort to screen emails and to filter out harmful messages before the communications reach staff email inboxes. However, plausible emails are often not identified by filtering software and get through to individuals. In addition, fraudulent activity often emanates from legitimate channels which makes a technical solution to the fraud problem impossible.

As a rule, any email that contains instructions or invitations to follow external links or open attachments should be treated as suspicious.

Links or attachments should only be followed when:

- You trust the sender and have verbally confirmed with the sender that the email is genuine. Call the sender on the official contact or support numbers for confirmation.
- If in any doubt as to the purpose or validity of the email, call **<DEPARTMENT / CONTACT DETAILS>**.

Never forward a suspicious email to someone inside or outside **<COMPANY>** unless authorised to do so by your immediate line manager.

Once an email is understood to be fraudulent or malicious, tag the email as spam (if your email client allows this). Then immediately delete the email.

Emails requesting actions for specific job functions are the responsibility of the following people:

Subject	**Team / Person Responsible**
Finance. Company Banking.	**<PERSON'S NAME> Contact Number, Contact Email Address**
Human Resources. Staffing Issues, Payroll, Sickness, Salary.	**<PERSON'S NAME> Contact Number, Contact Email Address**

Subject	**Team / Person Responsible**
Recruitment	**<PERSON'S NAME> Contact Number, Contact Email Address**

If you receive emails requesting action on these subjects that you are unsure about contact these people directly on the numbers provided. **Do not forward the email under question to these contacts unless requested to do so**.

5.1.2. Telephone

This sections refers to voice communications on both mobile telephones and fixed land lines.

Fraud attempts can be made using pressurised requests from callers. These requests might appear plausible with the caller having researched the recipient of the call. Background information being found on social media, general Internet searches or financial history such as company share registers.

In all cases staff must not act on the requests.

Under no circumstances should the recipient of the call provide further details to identify themselves, work colleagues or general company information.

If a pressurised telephone call is received, simply take the caller's name, company name and contact details.

Explain that it is company policy to take these details and to call them back.

5.1.3. Physical Entry To Buildings

This section should be read with **<COMPANY>**'s policy on general physical security to be found here: **<DOCUMENT REFERENCE>**.

Fraudsters can attempt to enter a building without authorisation to access the company network or remove important assets such as devices storing confidential company data.

All staff should have a valid company name badge clearly displayed at all times.

All visitors must sign in at reception where their business will be confirmed and a visitor badge will be issued. This badge must be surrendered when the visitor leaves the premises. All visitor badges must be accounted for.

All visitors to company premises must display a visitor badge clearly at all times. Visitors must also be escorted by a member of staff whilst on company premises at all times.

Staff should be able to easily distinguish between colleagues and visitors.

If a member of staff sees a either a person without a valid name badge or an unescorted visitor, they should (i) politely ask what business that person has in the building. Escort them to **<NAMED TEAM / INDIVIDUAL>** (ii) contact their line manager immediately.

Staff should be alert to the presence of unauthorised people. Fraudsters may appear genuine – and appear to be busy in the building. Staff should not be afraid to challenge people if they do not recognise them or they do not wear correct ID.

Staff must not allow unrecognised people to "tailgate" through doors. Do not hold doors open or otherwise facilitate access for unrecognised people.

5.1.4. Social Media & MessagingApps

This includes mobile apps and web sites such as Facebook and Twitter. These services allow people to share information publicly.

Fraudsters often use profile and news information posted online to help build more plausible stories when attacking companies. Fraudsters may also approach their victims using messaging apps or as connection requests from social media services.

It is very important to understand that any information posted online may quickly become public, and that company information should never be shared over messaging apps

Do not post any company information online through messaging or social media sites unless authorised to do so.

Examples of these sites are:

- Facebook
- WhatsApp
- Tumblr
- Instagram
- Twitter
- Baidu Tieba
- Pinterest
- LinkedIn
- Gab
- Google+
- YouTube
- Viber
- Snapchat
- Weibo
- WeChat

Examples of the types of information not be posted are:

- Company email addresses.
- Company contact telephone numbers.
- Company news and events.
- General company announcements.

Any questions on what can be posted online, please contact: **<CONTACT NAME/DETAILS>**.

5.2. Supporting Materials

<COMPANY> takes the threat from fraud extremely seriously.

Further to following the guidelines set in this policy document, the following assets and training aids are available:

5.2.1. General Guidance

General guidance to be found here:

<DOCUMENT SOURCE>.

Main contact to discuss all matters relating to fraud:
<NAME>, contact **<CONTACT DETAILS>**.

5.2.2. Training & Awareness

All staff must attend fraud awareness training with **[X]** weeks of joining the company. This training is organised as part of standard company induction.

After induction training, staff must undertake fraud awareness at least every **[X]** months. This training is organised by **[TEAM NAME]** and consists of **[DETAILS OF TRAINING]**.

In addition to periodic training, there must be adhoc testing exercises where test fraud attempts will be made. These exercises are designed to enhance the more formal training exercises and to keep staff vigilant against fraud.