

# Corporate Anti-Phishing Policy

## 1.0 Purpose

This document is provided to educate employees about email and Web-based fraud, and define a corporate policy to protect corporate and personal assets. This policy also indicates that individuals are responsible for the unauthorized disclosure of sensitive information.

## 2.0 Scope

This policy covers employee/partner/corporate representative and all associated third parties that have access to sensitive information belonging to the company.

## 3.0 Policy

**3.1 Prohibited Use.** Employees who receive email or Web requests for sensitive information are prohibited from sharing or disclosing any such information to any party outside the firm without a written agreement approved in writing by a supervisor. This eliminates the element of urgency that is a common trait among the different types of Internet fraud.

**3.1b Phishing is an enabler for identity theft, an activity that allows criminals to impersonate individuals or companies for personal gain and theft of assets. Phishing is an activity that relies on the concept of social engineering and abuses an individual's trust to extract sensitive information. By using recognizable names, forging or hiding the source of email addresses, replicating familiar or official Web sites and introducing the element of urgency, criminals send mass emails that seek to convince enough individuals to compromise valuable information such as financial details, PINs, credit cards, passwords and account numbers. In some cases, less sensitive data such as address, date of birth and phone numbers can be used in identity theft attacks.**

Employees who receive such emails at work are required to report it to their supervisors immediately. In most cases, this also applies to telephone contact as well.

### Specific situations that must be avoided include:

- a. Fake ATM (bank machine) keypads most often placed in drive-through banks. Always use indoor ATMs or interact directly with bank tellers.
- b. Never give out banking or financial information unless it is in a branch of the bank or by phoning a listed phone number for the financial institution. SIN/SSNs, PINs or passwords must never be written down or disclosed to anyone. There are no exceptions for sharing this type of information on the Web or by Email.
- c. Urgent email requests from individual client or company contacts that are not directly known by you must never be acknowledged. Links contained within those emails should never be opened. Always ensure by telephone that the person who requests urgent information is who they say they are. For any sensitive, urgent information of a financial or business nature, refer the matter to your supervisor. The only exception is for work directly related to a project, where you clearly know your interlocutor.
- d. Downloading, exchanging or opening executable programs that may contain malicious code such as viruses, spyware or worms is strictly prohibited. Once installed, these programs can gain control over computers and disclose information to unauthorized parties.
- e. Using company resources to propagate chain letters, jokes, programs or any other non-work related materials is strictly prohibited.

**3.2 Individual Guidelines.** The company recognizes that employees can disclose sensitive information from home or from work. Additionally, trend information indicates that fraud is targeted at individuals or consumers. To protect yourself and learn more about phishing tactics, visit:

[http://www.antiphishing.org/consumer\\_recs.html](http://www.antiphishing.org/consumer_recs.html)

Always use different passwords on all sites and situations that require you to select a password. Passwords should be near-impossible to guess but relatively easy for you to remember. A good strategy is to use

Password Safe, an open source program that keeps track of all your passwords in an encrypted database on your computer and suggests complex passwords that you can simply cut and paste when you need them. Find it at: <https://sourceforge.net/projects/passwordsafe/>

### 3.3 Assumptions

Be aware that most victims of fraud, in particular phishing and social engineering attacks, fall prey to these approaches because they assume that the information is accurate, the person requesting the information is real and that they are addressed individually. In effect, these emails are sent to millions of recipients, are often unmonitored by our Internet service provider and may have bypassed our email spam scanners.

### 4.0 Enforcement

Employees are responsible for the protection and secure disclosure of sensitive company information. All approved sensitive data transmissions over the Internet must be documented in writing and transmitted using either encryption or a secure server (look for 'https://' in the Web page address).

For a definition of information considered sensitive with different degrees of confidentiality, refer to our corporate Data Classification Policy.

Remember that you have privileged access to restricted information. Information is a valuable part of our company's and our clients' assets and must be strictly protected. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### 5.0 Definitions

<b>Term</b>	<b>Definition</b>
Spam	Unsolicited commercial email send in large numbers designed to be profitable from a very small number of responses.
Spyware	Software designed to compile usage statistics or take information from the host system and communicate it back to its home server for commercial or criminal purposes.
Virus/Worm	Unauthorized software that multiplies and carries a message, remote control component or destructive payload.
Phishing	An enabler of identity theft activity often carried out through email
Social Engineering	Most common method of gaining and abusing the trust of a stranger, often for the purpose of identity theft and financial gain.
Identity Theft	The theft of personal or corporate data for the purpose of impersonating and defrauding victims.

### 6.0 Revision History