



## Something Smells Phishy – Protection Against Phishing

### What is Phishing?

Phishing is a form of fraud where the “phisher” uses e-mail addresses or websites that appear to be from authentic and reputable organizations in order to lure individuals into sending them personal or corporate financial information (credit card numbers, account usernames and passwords, social security numbers, etc) which the attackers then use to commit identity theft and other crimes. Recent statistics from the Anti-Phishing Working Group indicate that reported unique e-mail based phishing expeditions are growing an average of 50% per month. The largest industries attacked (or spoofed) to fool the consumers are the financial and retail sectors. This means that e-mails or links to websites claiming to be from various banking or credit institutions or web-based retail organizations will be the ones most likely to be “bait” for the unsuspecting consumer.

### How Do You Protect Yourself?

Like many types of fraud, the best protection is awareness, education, and caution with anonymous interactions. Phishing is closely related to “SPAM” (see the Tsunami “Technology 101” paper titled “Protect Yourself from SPAM”) in that it often relies on you giving up confidential information via e-mail. Ask your e-mail provider to ensure that they have adequate “Anti-SPAM” measures in place – this will reduce the amount of phishing expeditions you are potential subject to.

- Be suspicious of any e-mail correspondence you might receive with urgent request for personal or financial information, regardless of who the source of the e-mail appears to be. If in doubt, first contact the organization by phone, but be certain not to use any phone numbers provided in the e-mail – look their number up in the phone book, or from the official corporate web site. The phishers will try and use exciting or upsetting statements in their e-mails to solicit a quick response – they don’t want you to think about what you’re doing, just to react.
- If you suspect the e-mail may not be authentic, do not use any links provided in the email to get to the organizations web site(s). Don’t fill out any forms in the e-mail, nor should you reply directly to the sender or any other e-mail address you are encouraged to contact.
- Finally, regularly check your bank, credit card, and other statements for irregular or suspicious activities, and report them immediately to your financial institution. Each of these legitimate companies has a fraud department who can assist you if you feel you may be a victim of phishing.

For more detailed information on how to protect your corporate environment, please contact Tsunami ([contact@tsunami.ca](mailto:contact@tsunami.ca)).

This document is provided for general information and educational purposes only and is not intended to replace professional advice and services or the maintenance of any systems. In no event will Tsunami Communications Inc. be held liable for any decision made or action taken in reliance upon the information provided through this web site or any published documents.