



5 Ways to Proactively Guard Your Email Programme Against Phishing

Toshiaki Onishi, Delivery Manager Asia Pacific, Epsilon International

➔ [E-Marketing Tips](#)

Keywords : Phishing protection, spoofing, email authentication

Date : 7-10-2009

[Newsletter](#) > [Asia Pacific](#) > [2009](#) > [Jul](#) > [E-Marketing Tips](#)

Whenever a new round of phishing attacks arise in the banking sector, the immediate knee-jerk reaction from the industry tends to be – to stop all email communications with their customers for an indefinite period. While it may be felt as a necessary step, the sudden suspension of email communications doesn't in any way help protect customers from phishing attacks at the time or in the future; not to mention it adds no value to building consumer confidence in your brand, service, or marketing communications. What's more, this unexplained suspension of email messages can easily trigger complaints from security-aware customers expecting to find time-sensitive communications from the bank in their inbox.

Instead of shutting down your email channel, the most effective approach to protect customers that rely on your online services and communications, and to safeguard your brand from continued phishing attacks, is a strategically built and carefully executed integrated communications programme that fights back. Don't wait till the next phishing attack. Take action now:

1. Educate your customer on how to distinguish your legitimate emails. This is the only long term solution to protect your customers from erroneously responding to phishing emails. You need to provide your customers, and remind them regularly, about the style and content of your emails from design, to sender name, to the scope of your regular email communications.

Phishing emails also often mask their fraudulent link in an image or in a forged URL with the spelling of a legitimate domain. This deception however can only be successfully implemented in an html format email. To protect customers from such links, an increasing number of financial institutions and e-commerce operators are using text emails, to allow their customers to see the real domain behind each URL, and so help consumers to easily recognise fraudulent email activities.

Encourage your customers to type your website address in a new browser window whenever they are in doubt of the links presented in the email received.

2. Employ a single-domain URL strategy. All customer-interacting URLs should only come from one domain (e.g. www.ABCBank.com), and avoid promoting or referring a sub-domain as the primary landing page (e.g. http://myaccount.ABCBank.com). As you start presenting more than one URL as the official access point, you are encouraging your customers to accept variations on your URL, and they also become more vulnerable to phishing attacks.

3. Don't behave like a phisher. Your emails should never ask customers for their personal or financial information, and avoid wordings that may be interpreted as asking for such information in the content or subject line. Phishing subject lines are often about online security, followed by a request for confirmation of personal and financial details.

4. Establish and manage your sender reputation. First and foremost, set up a dedicated IP for your email campaigns, so that you can establish a reputation record of your own and have complete control over your sender reputation - a critical factor to your email deliverability. An absence of a sender reputation or a low IP score is often associated with spam or phishing scammers by ISPs, resulting in email blocking. [Read here to find out how to build and maintain a high sender reputation for your email campaigns.](#)

5. Enable as many email authentication technologies as possible to allow ISPs and filtering software to verify the legitimacy of your email and you as a sender. ISPs use various authentication methods in combination to block identified or potential phishing, spoofing and spam senders from reaching their email users. Some of the common email authentication solutions include reverse DNSⁱ, domain keys identified mail (DKIM)ⁱⁱ, sender ID and sender policy framework (SPF)ⁱⁱⁱ.

- i. Reverse DNS: during this process ISPs will look up an IP address by searching the domain name registry or registrar tables to verify the association of a given IP address with the domain name.
- ii. Domain Keys Identified Mail (DKIM): this authentication technology encrypts a digital signature of the sender in an email in a way that can be verified by recipients.
- iii. Sender ID and Sender Policy Framework (SPF): both authentication solutions allow software to identify and reject messages with forged addresses. ■