

Phishing E-mails

What to do with them!

1. Don't open them, if possible.
2. Forward them to the following: spoofof@millersmiles.co.uk
reportphishing@antiphishing.org – the subject line may be left blank.
3. Email users that access their emails via an email client (e.g., Outlook Express, Windows Live Mail, Thunderbird) should forward the phishing email *as an attachment*. Attaching the email to a new email message preserves vital email header information that helps to identify the phishing email source.
4. There are several methods of attaching one email message to another:
 - a. Without opening it, right click the phishing email in the inbox and select 'Forward As Attachment' (Outlook Express), or
 - b. Open a new email message and then 'drag and drop' the phishing email from the Inbox to the new email message window. You may need to resize the email application window to avoid obscuring the new email message window.
5. Email users that access their emails via a web browser (e.g. Hotmail, Yahoo, Google Mail) should forward the phishing email using the 'forward email' feature in the usual way.

Further information can be found here: <http://www.millersmiles.co.uk/submit.php>

