

Security & Privacy

Phishing Scams & Hoax Emails

To maximise your safety online, we have developed a 'how to' guide on pinpointing and reducing your exposure to phishing scams.

MessageMedia will never request you to confirm or disclose your confidential account information. If you receive an email you believe may be a hoax, please send a sample to MessageMedia Support at:

support@messagemedia.com.au

Phishing emails are scam communications sent by a third party assuming the look and feel of a real organisation. The main aim of a phishing email is to trick you into revealing your personal information and user account details which will then be used for illegal purposes.

Identifying Phishing Emails

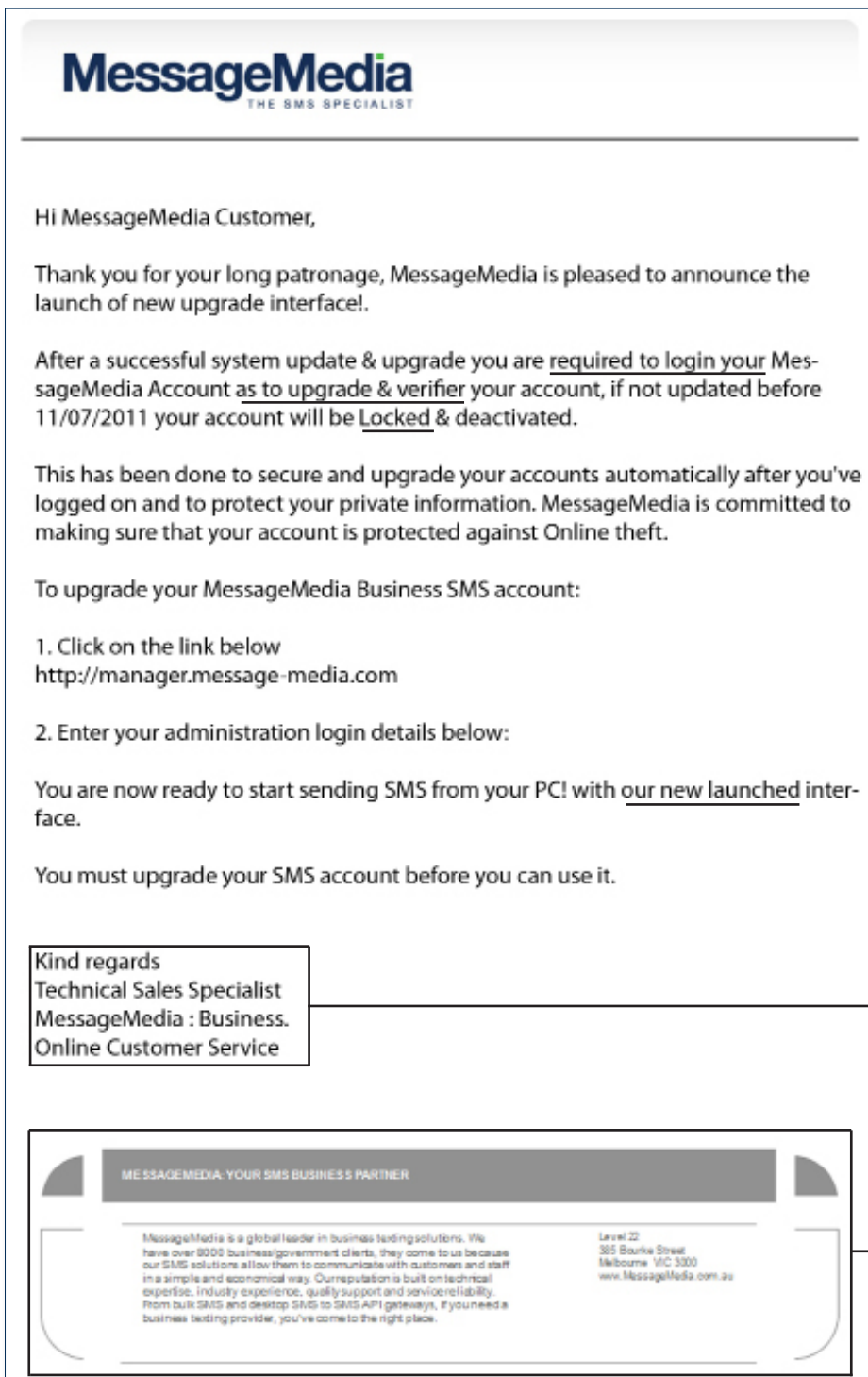
Phishing emails are often poorly written and attempt to recreate the graphical nature of a companies brand by copying logos and headers from official websites.

What are the signs of a phishing email?

Use of bad grammar throughout the email

Non specific signoff to email

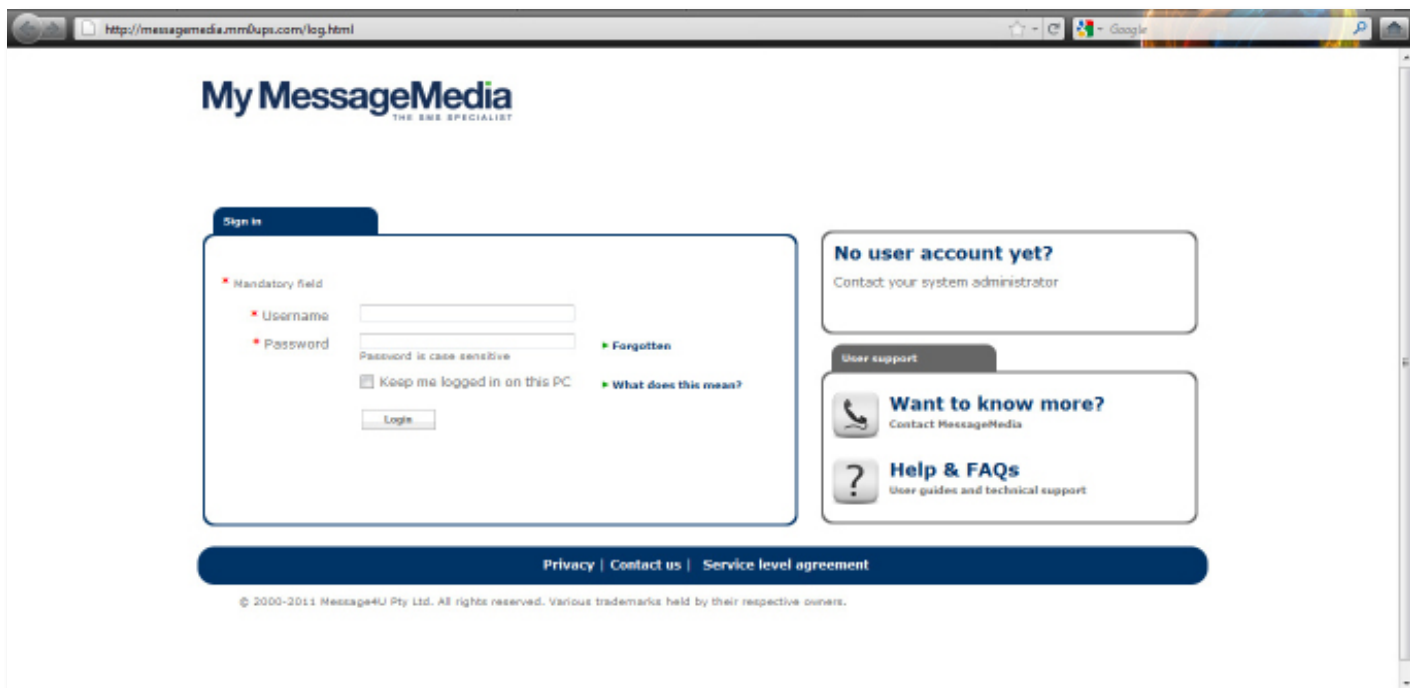
Poorly formatted headers/ footers



Identifying Phishing Websites

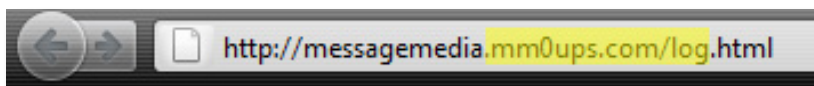
Phishing emails often link directly to convincing replica webpages. These pages are not privacy protected and store the information you enter for illegal use at a later date.

Example of a replica webpage:

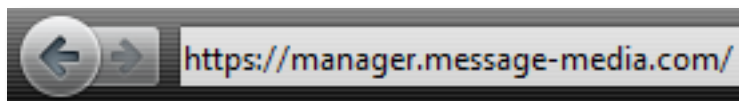


To ensure you are entering your confidential information on the correct website, make a note of the destination URL.

A URL with irregular conventions is often a sign of an unprotected, illegal phishing scam:



The correct MessageMedia URL is as follows:



What to do if you receive a scam or hoax email

If you receive a scam or hoax email send a copy to the MessageMedia Support team through

support@messagemedia.com.au

To minimise the chance of opening the email and exposing your computer to malware, send the hoax email as an attachment - avoid forwarding the email and do not open any attachments.

After sending the email to the MessageMedia Support team, delete the original email from your inbox, sent items and deleted items folder immediately.

If you have responded to the email or entered confidential information on a website linking from the email contact MessageMedia Support on 1800 155 228 immediately.

How to avoid Phishing Scams

Phishing scams can be avoided by using common sense and looking out for the telltale signs.

It is important that you are aware of spam emails, illegitimate SMS messages and phone calls from unknown parties attempting to data mine your information. Do not give your personal account details or copies of important documents to anyone other than for legitimate purposes.

Keeping your anti-virus software and firewalls up-to-date and performing regular scans of your computer will also minimise your chances of being a victim of phishing scams.

Further Information

For further information on phishing scams please visit the Australian Competition & Consumer Commission website.

ACCC Scamwatch

<http://www.scamwatch.gov.au/>

ACCC Scamwatch - Phishing Emails

<http://www.scamwatch.gov.au/content/index.phtml/tag/RequestsForYourAccountInformation>