HOAX EMAILS

‘Best practice’ tips to keep your network safe

BMS
YOUR TRUSTED TECHNOLOGY PARTNER

Cyber-crime is BIG business. These tips will help protect your business from ongoing threats.

1 UPDATE REGULARLY
To make sure you are blocked from new viruses & spyware protect your network with the most up-to-date firewall, anti-virus & anti-spyware software.

2 ACTIVATE SPAM FILTERS
Make sure your IT security software has a SPAM filter and that it is active. This will screen and segregate SPAM and phishing emails.

3 ESTABLISH AUTO-UPDATES
Ensure your software has automatic program & anti-spam rule updates so your protection is always prepared for current threats.

4 EDUCATE YOUR TEAM
Educate your team members and make sure they are always alert & cautious. Hackers work full time to try and break down IT security walls, so collectively you must never be complacent.

5 TRUST YOUR INSTINCT
If you are even slightly suspicious, do NOT open an email. Trust your instinct. You are probably right and the email is likely to be a hoax.

6 PREVIEW YOUR EMAILS FIRST
Format your inbox with a reading pane so you can read new emails without clicking to open them. (Outlook: View tab - Reading Pane - Right or Bottom)

7 THINK BEFORE YOU CLICK
If you accidentally open a suspicious email, DON’T click on any links or images, download files or open attachments.

8 CONFIRM AUTHENTICITY
Phone the person the email is from first before you open it. It’s the safest way to find out if they really sent it. If they didn’t you can alert them that it’s a hoax.

9 BACK UP, BACK UP, BACK UP
If your network is affected by a hoax email, you can revert to your last data backup and get back to business sooner with minimal information loss.

thebmsgroup.com.au | 02 4254 5444 | askus@thebmsgroup.com.au