Budget airline impersonated by Facebook hoaxer and malware spammers

Budget Australian airline Jetstar is suffering a double dose of cyberpain today.First up was a hoaxer who managed to create a Facebook persona called "Jetstar Australia" and thus to post legitimate-looking comments onto Jetstar's official pages with sniggering disdain.

A customer who had written a lengthy complaint about Jetstar's policy on strollers (pushchairs) was advised:

This is a "comment box" not "write a long story" box. Please shorten it and send to someone who cares.

A lady unloading her frustration when trying to change her flight bookings online was rewarded with:

Thanks for leaving a comment. We have now cancelled your flights as requested.

And one who wondered if there were any good offers on cheap flights to Queensland's Gold Coast got smacked down with:

Dont be such a tight ass and pay the full price. Its cheap anyway.

The comments might seem amusing, but if you've ever been the victim of bogus online postings in your name - something that's hard to prevent and difficult to correct - you'll know how stressful (not to mention costly) it can be.

Jetstar has scrambled to distance itself from the bogus comments, and is advising people to double-check the Facebook profile of posts that look official:

Jetstar's second brush with having its name taken in vain in cyberspace happened this morning.

A malware spam campaign claiming to be a Jetstar flight itinerary started hitting Aussie mailboxes:

Infected emails contain an attachment with a name such as Jetstar Flight Itinerary-nnn.pdf.zip (nnn is a string of digits) that is, of course, no such thing.

The ZIP file contains an EXE file (Windows program) that is zombie malware. Sophos detects it as Troj/Bredo-AEG.

In a sort of double-whammy, Jetstar customers took to its beleaguered Facebook page to blame the company for the malware. One user vented that she was:

NOT IMPRESSED THAT JETSTAR HAS BEEN COMPRIMISED

That's definitely not fair criticism. (It's not terribly good spelling, either.)

There's nothing Jetstar - or any other brand, for that matter - can to do prevent a crook from constructing an imposter email that includes its company name, address, logo or look-and-feel.

Impersonating a company by email takes little more than cutting and pasting from a legitimate message.

In this spam campaign, for example, the marketing links in the email take you off to official pages such as the Jetstar Shop, and the "unsubscribe" link takes you to Jetstar's outsourced mailing list provider.

Inquisitive email users might have looked at the email headers, but even these are mocked up to make it look as though Jetstar sent the message and as if Symantec's "Star Scan" email filter had vetted it:

The real sender is shown in the topmost Received: header - a cable or DSL modem, most likely a home user's PC itself infected with zombie malware causing it to act as a spamming robot:

Rogue comments on social media sites and spams that hijack a brand are almost always outside the victimised company's control.

In this case, delete the email, and remember, don't believe everythingyou read on Facebook!