How can spammers send email using my domain name?

If you have received SPAM email from your own domain name, it can be disconcerting. But it does not necessarily mean you have been hacked. Most often, it is another reason altogether. Here are the two main methods:

1. Changing the display name to match yours

This is the simplest method of phishing. Anyone can easily change the name displayed to be whoever without verification. This is also easily discerned as the name does not match the email.

Bill Gates
<spammer@yahoo.com>

2. Address Forging or "Reply-To Spam"

This is how most spam is sent. Any server can send emails and code can make the reply address say anything. A few lines of code could send an email from bill.gates@microsoft.com.

Most SPAM is sent using the above method. So a quick line of code and they can send an email that looks like it was sent from your domain, but had nothing to do with your domain.

Bill Gates
<BillGates@Microsoft.com>

Why would spammers send email from my domain?

The main reason is to bypass spam filters. You might also easier trust an email sent from your domain. So when a spammer has your email on a list (e.g. steve@apple.com), they write code to send email "from" another account @apple.com. This helps the spam email make it past a spam filter as well as seem more familiar to the you, the recipient.

Is there a way to tell where the email came from?

There sure is. Every email contains a header, which your email program hides from view. This header contains all sorts of information about where this email came from and how it was sent. It is often very easy to confirm that the reply address with your domain did not actually originate from your server.

As always, if you're not sure you can forward your spam to support@bitp.com.au

View message headers in Outlook on your desktop

1. Double-click an email message to open it outside of the Reading Pane.
2. Click File > Properties.
3. Header information appears in the Internet headers box.
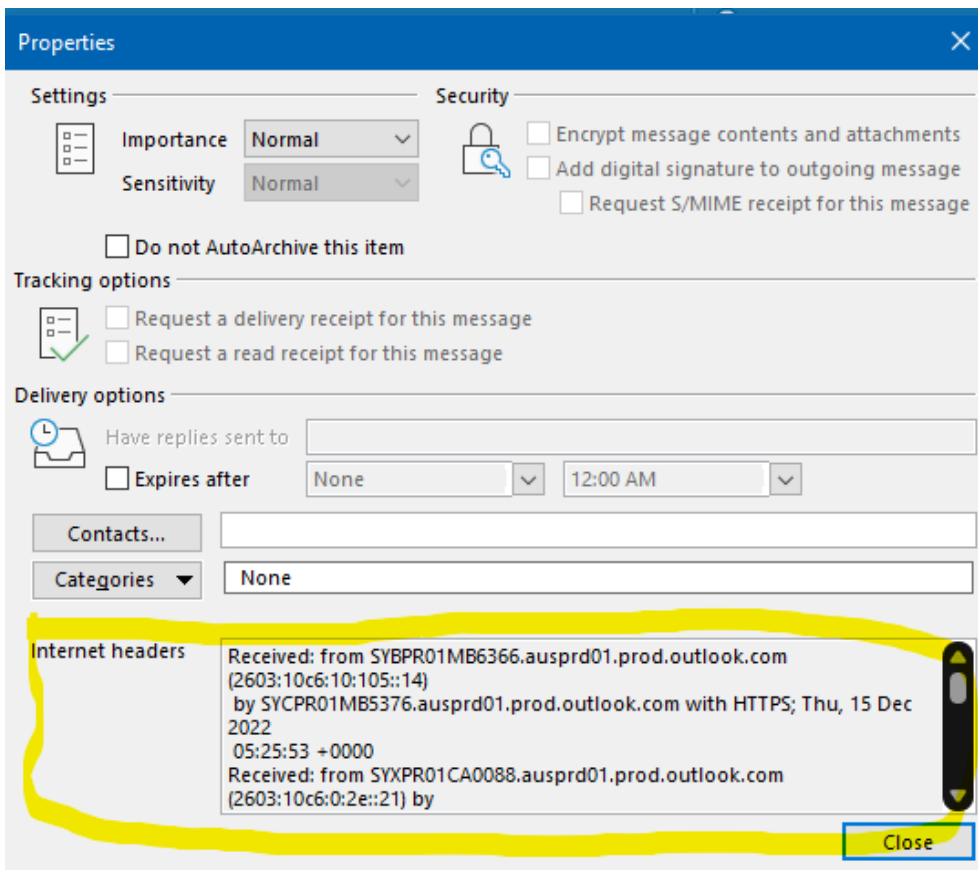
4. Towards the bottom you will find a section that says Reply-To and/or from. Below is an example of what you may see from a scammer. This does not however apply to all attacks of this type. But shows how the scammers disguise their real email.

Reply-To: Bill Gates spammer@yahoo.com
From: Bill Gates BillGates@microsoft.com