Suspicious Emails

Why do we need to be on the lookout for suspicious emails?
Email is used by various people and organizations to involve total strangers in actions against their own interests, such as:

(a) Obtaining money by subterfuge
(b) Taking control of their computer to send spam
(c) Infecting their computer with a virus
(d) Encrypting all their files

We are protected from most of this by the 'border guards' at our email providers, such as Microsoft, Google, Yahoo, Telstra, and by security (anti-virus) programs on our own computers. But occasionally risky email gets through to our inboxes, so we need to be alert, and aware of the clues that warn us that a message may not be what it seems.

What makes a message suspicious?
(a) The sender is not familiar to you.
(b) Your personal name is not used.
(c) The standard of English is poor; the message contains bad grammar, spelling mistakes etc.
(d) The message offers large sums of money (appeals to greed), contains warnings or threats of imminent disaster (appeals to fear, tries to cause panic).
(e) The message claims to alert you to a delivery of a parcel that you ordered.
(f) It invites you to click on a web-link included in the message (a reason may be offered: to claim your reward, to regain access to your account).
(g) It invites you to Reply giving personal information such as a login name and password. (Reputable organizations will NEVER ask you to do this; MelbPC and Microsoft are reputable organizations.)
(h) It invites you to open an attachment. (Especially dangerous: attachments that are 'executables' [programs that run when you open the attachment]; Word files [which may also contain executable code]. Be careful if you cannot read to the end of the name of an attached file.)

There's some useful advice on this website:
http://www.techrepublic.com/blog/10-things/10-tips-for-spotting-a-phishing-email/
Also in this Word file at the MelbPC Yammer service (requires your MelbPC account login):
https://www.yammer.com/melbpc.org.au/#/files/67455503

What to do if you receive a suspicious message

(a) Take your time! Dangerous messages often contain language designed to get you to act quickly without thinking first.

(b) If it's obvious the message does not concern you (eg it's directed to clients of a bank that you don't bank with, or promises a delivery you know you did not order) just delete it. (There's a note below on the 'delivery' scam.)

(c) If you have no personal interest in any rewards or threats contained in the message then just delete it.

(d) Do NOT click on any web-links in the message. Check the link behind any web-links or 'hot words' within the message by hovering your computer mouse over them (or, on a touch-screen, holding your finger down on the link). In a computer browser window the link will pop up bottom-left; on a touch-screen, it will be at the top of the little window that pops up. If the address is very different from the link in the text, and/or seems to bear no relation to the (claimed) sending organization, then delete the message.

(e) If you're still uncertain whether the message is genuine, then contact the organization (or individual) who (apparently) sent it, by other means: login directly to their website (NOT using the link in the message) or phone them. (Read the organization's own web advice first - the reference list below may include your organization's advice.)

(f) If you're using webmail, mark the message as Junk, which helps to prevent more spam from that source getting through to you and others.

(g) If the message seems to you particularly dangerous, eg because the imitation of the organization's official site is of good quality, report the message to the organization. (See the reference section below for advice from some leading organizations including their spam-reporting addresses.) This is a public service but not obligatory.

(h) You are encouraged to report suspicious messages to other MelbPC members using our Yammer chat-room (requires MelbPC login) where there is a group dedicated to Security Alerts. It's worth joining and following that group because other members post warnings there about current threats. You can find examples of scam emails there. This link will lead you to it:
https://www.yammer.com/melbpc.org.au/#/threads/inGroup?type=in_group&feedId=9197709

(i) You can reduce the risk of future harm by taking the advice of the Australian Signals Directorate (summarized in the ZDnet article in our list of links below). You can reduce the risk from theft of your email password by enabling 'multi-factor authentication' (also known as '2-step verification) for your email login. This is available on demand to members using MelbPC email at Office 365 (send a message to ihelp@melbpc.org.au to request it). It is also available from the other major email providers, including Google (Gmail) and Microsoft (Hotmail, outlook.com).

Note on the 'delivery' scam:
A common and very dangerous sign to be VERY careful of is a notification from Australia Post or some other similar organisation such as FedEx or TNT that informs you that an attempt was made to deliver a package to your home but you were out. It says you need to print the documentation in order to collect your package from the Post Office, depot etc. The attached file is a Zip file.

Zip files in themselves are not dangerous but these contain an .exe file that will be extracted. These embedded .exe files can be very dangerous as they often contain a 'Ransomware' program that will encrypt ALL your data.

You should never try to open one of these files. Stop and think. Why would someone include a compressed executable file in order for you to print something? It would be much simpler and easier to include the required text in the body of the email.

Unfortunately, because very many people buy on-line and are expecting parcels, they click on something that is actually very hostile. Think before you click!

Websites of major organizations with advice about suspicious emails

Microsoft:
https://www.microsoft.com/en-us/safety/online-privacy/phishing-scams.aspx/

Google (top menu):
https://support.google.com/mail/topic/3394657/

Google (Advice on avoiding, and reporting, phishing emails):
https://support.google.com/mail/answer/8253/

Apple :
https://www.apple.com/legal/more-resources/phishing/

Telstra/Bigpond:
https://www.telstra.com.au/support/category/email/manage/phishing-or-hoax-email-scams

Australian Taxation Office (ATO):
https://www.ato.gov.au/general/online-services/identity-security/verify-or-report-a-scam/

Australian Federal Police (AFP):
https://www.afp.gov.au/what-we-do/crime-types/cybercrime/online-fraud-and-scams

Scamwatch (an Australian Government service):
https://www.scamwatch.gov.au/
Also from Scamwatch: If you click the graphic (red magnifying glass over blue envelope) on the right of this page…
https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing
…you will see a helpful visual guide to risks in email messages.
Australian Signals Directorate (via ZDnet):
http://www.zdnet.com/article/block-adverts-delete-flash-kill-java-asd/

HL Feb 2017