Projectors and Stagefright

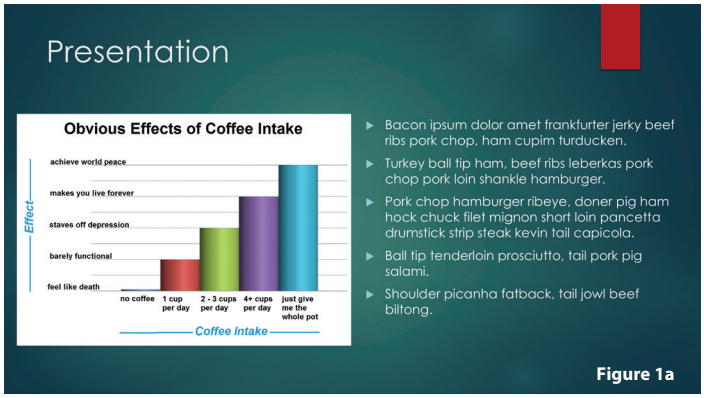

Figure 1a

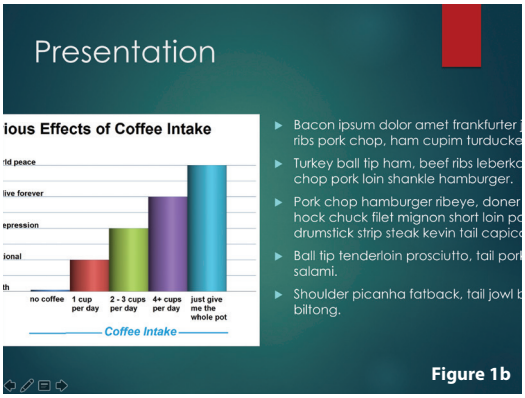

Figure 1b

Choosing the correct aspect ratio for a presentation

There are several mistakes that are easy to make when using PowerPoint. The most common one I see is the failure of a video to play because the video file wasn't copied along with the presentation. There is a new mistake that's easy to make due to the increasing use of widescreen TVs and computers. By default, newer versions of PowerPoint (for example Version 15 on the Mac) will make widescreen presentations (technically called 16:9). The older, more square slide size, is referred to as 'Standard' (or 4:3). If you present via a projector, it's very likely to be square type (standard). On the other hand, if you present on a flat screen it will be the more rectangular, widescreen, format.

Problems occur if you create a widescreen presentation (the default on newer PowerPoint versions) but present it via a standard projector. Have a look at image 1a and 1b to see what happens. 1a shows how the presentation looks when you make it. 1b shows how it looks on a standard projector. As you can see, the sides are chopped off and content is lost.

There are two solutions to avoid this problem. One option is to always use the 'Standard, 4:3' option in PowerPoint. If you present a Standard presentation on a flat screen, you will just have black bars on the left and right side, but no content will be lost. The other option is to ensure you choose the slide size to match your delivery method. To do that you would need to know if you are presenting from a projector or a flat screen. The safest option is clearly to always choose Standard. The location of this setting resides in different places, depending on the version of PowerPoint you are using. Look for the 'Slide Size' option. On version 15 on the Mac, the option is at the far right of the screen, when you are in the 'Design' tab (see Image 2a and 2b).

Stagefright – Android phone vulnerability

A range of bugs have been found in the handling of picture messages (MMS or Multimedia messages) on Android phones. That means all Samsung Galaxy type phones, Sony Experia and other similar phones. The issues don't apply to iPhone or Windows phones. The bugs can result in malicious software being installed on your phone if a special picture message is sent to your handset (which is becoming commonplace). Even if you don't open the message, the malware in the message is still able to run! If you (or friends and relatives) have this type of phone there are a few things worth doing to protect them. Firstly, ensure any system updates are installed. The next thing to do is install a free app that checks the phone for the vulnerability. The best one to use is called 'Stagefright Detector' from 'Zimperium'. Figure 3 shows how it looks in the Play Store. Run the app and allow it to analyse your phone. If you see the result 'Vulnerable' like Figure 4, more action is required.

Disable automatic MMS message retrieval

The easiest workaround is to stop your phone automatically downloading the content of picture (MMS) messages. Once that is done you will still receive notifications of picture messages but you get the choice of downloading or deleting

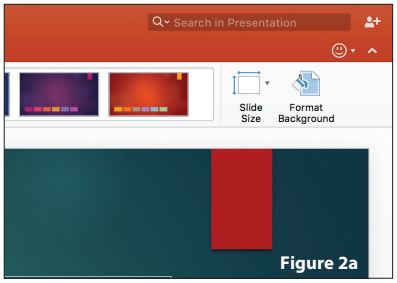

Figure 2a

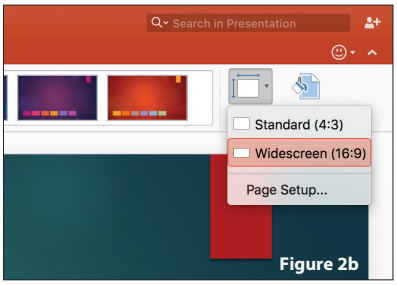

Figure 2b

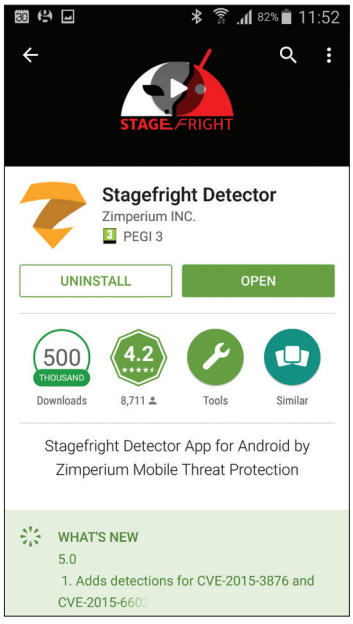

Figure 3

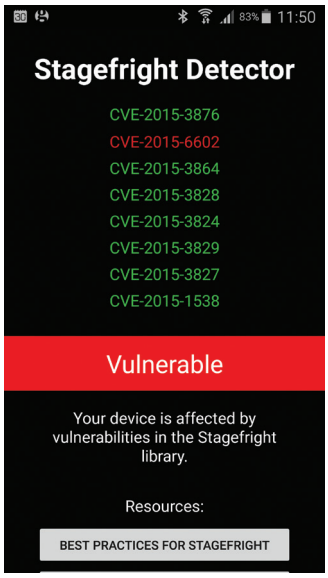

Figure 4

the message. If you get a multimedia message from an unexpected number in the future, you should then delete (rather than download) it. Disabling automatic message retrieval differs depending on which software you use for your messages. A comprehensive set of instructions are provided by the Lookout security firm here: https://goo.gl/U1YvjC

Once you've made this change the phone will still be reported as vulnerable in the detector app. The change just prevents any malicious messages from downloading automatically. Only a system update will completely protect the phone. As most phone manufacturers only keep their phones updated for a year or two, a system update that fixes the problem may never come for many handsets. Please note, this vulnerability does not apply to Facebook Messenger or WhatsApp messages.

Mr David Haider,
Consultant Ophthalmologist and Chief Clinical Information Officer, Bolton Foundation Trust, UK.
E: david@drhaider.co.uk
Twitter: @drdavidhaider