## Multi-layered phishing mitigations





The following real-world example shows how implementing layers of defences can help organisations (in this case a financial sector company of around 4,000 staff) defend themselves against phishing attacks. Reliance on any single layer would have missed some of the attacks, and cleaning infecting devices is costly and prohibitively time consuming.

1,800 **50** 1,800 malicious emails 14 emails were 1 instance of malware 50 emails reached sent to the company in users inboxes. clicked on, launching installed this campaign. malware.

1.750

1,750 emails were stopped by an email filtering service that identified that malware was present

36 emails were ignored or reported by staff, using a button in their email client.

25 were reported in total, including some after having been clicked on.

This was the first indication that the attack had got through the initial layer of defences.

13 malware installations were unsuccessful because a patching regime had ensured that nearly all devices were up-to-date.

The malware's call home to its operator was detected, reported and blocked. I device was seized, investigated and cleaned within a few hours.

## How was the organisation attacked?

A financial sector company of around 4,000 employees received 1,800 emails which contained a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.







