

Identify a Phishing Message in Five Steps



From the network breach at RSA to theft of intellectual property in Operation Aurora, it is no secret that some of the most visible hacking involves the use of spear phishing. A targeted form of phishing that is custom-made for a specific organization, a spear phishing email message seeks to elicit a desired action that could result in a Trojan being loaded, or the unintended leaking of confidential or privileged data.

As Paul Mah has written in the past, defending against spear phishing is a challenging task that mandates some amount of user training. To assist organizations on this front, Paul has come up with a simple checklist to help identify a potential phishing message.

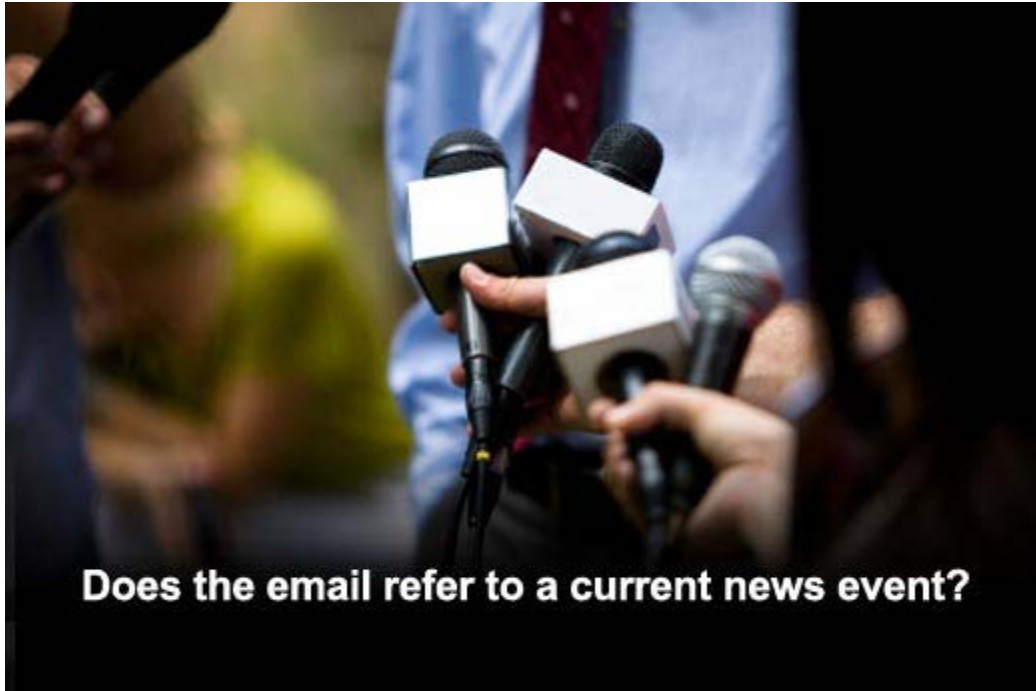


Does the email contain information that could be obtained from social networking sites?

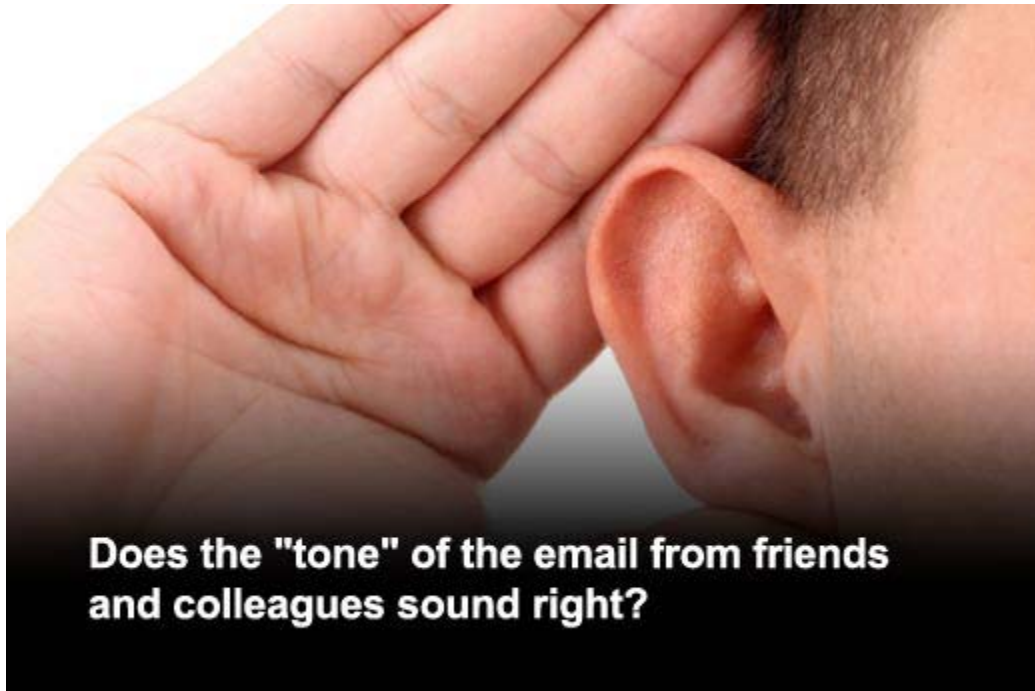
The dizzying amount of information being loaded into social networking sites makes it trivial for an attacker to use them as a source of information to craft a spear phishing message or to gain a victim's trust. With this in mind, private information should always be regarded as belonging to the public domain once they can be found on social networking sites such as Facebook or Twitter. Indeed, a woman in Singapore was arrested recently for allegedly cheating victims of thousands of dollars by masquerading as their cousin. All her information — including their contact number and name of their real-life cousins — was apparently obtained from Facebook accounts.



One predominant objective of hackers entails the loading of malware or Trojans onto their target's PC. Given that executable files are typically blocked in email attachments these days, black hats have evolved their techniques to either trick their victims into downloading the malware over the Internet, or directing them to visit a specially crafted website loaded with a browser exploit. To protect yourself from such scenarios, you should almost never click on a URL link unless it is from a reputable site, and even so you should usually type in the URL manually.



Major news events such as large-scale catastrophes or the death of celebrities are quickly followed by a wave of phishing messages touting the same news events in their subject lines or email body. No doubt, phishers are hoping that confused or overeager users will let their guard down and click on their proffered URL links in their haste for more information. Hence, be on your guard when you see an email that refers to a current news event.



It is trivial for hackers to collect the email addresses and names of colleagues and friends. Larger companies typically publish their staff information on the Internet, while simple social engineering methods could be used to glean details such as the name of one's immediate supervisor or colleagues. The guideline here is to filter such messages based on what we know of the purported senders and how they typically write. Getting a curt "Check out this link" email from a normally verbose colleague or a "Nice babes" from a female boss should set alarm bells ringing.



Is immediate action required?

Phishers want their victims to respond immediately, or soon after reading their phishing message. This prevents them from checking with more knowledgeable colleagues, or to otherwise wise up to the trickery. It is for this reason that a message demanding an immediate response deserves a far greater dose of skepticism, and should hence be scrutinized more carefully.