**Don't Fall For The Same Old Tricks**

Respondents to a Cloudmark survey released last month said that 28 percent of spearphishing attacks are getting through their organization’s security defenses. Of those that suffered a spearphishing attack, 32 percent said they had financial losses and 29 percent had damage to company reputation.

"Unfortunately, a particularly message doesn’t need to be the worst, sneakiest, or most clever in order to be successful," says Angela Knox, senior director of engineering and threat research at Cloudmark.

Amy Baker, vice president of marketing at Wombat Security Technologies agrees. “Unfortunately, phishing scams don't always need to be sneaky to have a big impact on an organization."

"An email that elicits an emotional response is a sneaky way that we hear of people falling for phishing attacks," says Baker. "Criminals are gleaning a lot from things that we post on social media like trips that we are taking and what we did while we are there, allowing them to craft spear phishing emails that strike a chord because of the personal details that they know. A good example would be an email telling you that you received a speeding ticket in a city that you just visited."

"A sense of urgency," says Knox, "is useful for 'hacking the human' and getting the person to act quickly, which gives them less time to think and recognize that the message might be a fake."

Knox also points out that users can be tricked by "reply-to" email addresses. "The from line looks like a person that the user knows, but the reply-to email can be different. ... Most email clients do not show the reply-to in the initial message. ... Note that in many email clients, particularly on mobile devices, the Reply-To isn’t visible."

How to prevent your organization from being next? Remind your users that what they say on social media can be ammunition for the phisher. Remind them that a phisher will prey on your emotions just as much as she'll prey on your filtering technologies.