marketscan
data you can trust

WHAT YOU CAN LEARN FROM SPAM CON ARTISTS

If scammers can make millions of dollars annually from their emails, they must be doing something right...

WHAT YOU CAN LEARN FROM SPAM CON ARTISTS

If scammers can make millions of dollars annually from their emails, they must be doing something right...

Although the goal of the scammer is to defraud his/her victim, their techniques have lessons for any business using email marketing within legitimate campaigns.

THE ADVANCE FEE SCAM

Perhaps the best known email fraud is the "Advance Fee Scam". Also known as the "Nigerian 419 Scam", because many of these messages appear to originate from Nigeria, this fraudulent use of email marketing generates *millions* of dollars each year.

HOW IT WORKS

The Advance Fee scam operates on a scattergun, fire-and-forget basis to thousands of unrelated recipients at a time.

- The recipient is encouraged to make contact with the sender under the pretence of getting a share of a large sum of money.
- Once a reply has been sent, several more emails will follow asking the dupe to help bribe officials or put other plans in motion to help move the money by sending "cash advances".
- As long as the scammer keeps receiving cash, the emails continue to arrive.
- The dupe, however, never receives anything in return.

There are a number of common indicators for these spam email messages:

- The message usually has an attention-grabbing subject line designed to encourage the recipient to open it
- The message often appears to come from an authoritative source, such as an African government official
- There are often dozens of other email addresses in the recipient list
- There is always a time limit specified in the message body by which time the reader must act
- The message always promises a share of an unimaginably large amount of money
- There is always the suggestion that the promised transfer of money needs to remain secret because it is illegal, hence the need to use unofficial channels.

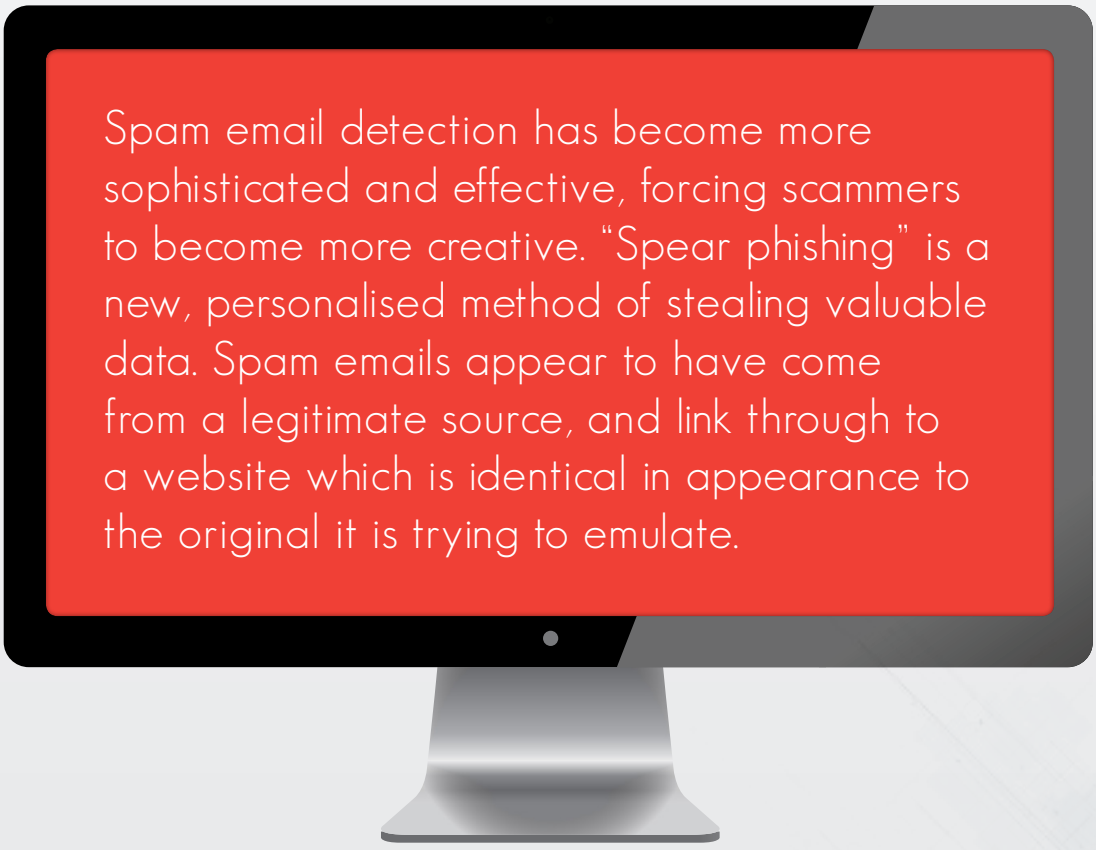
THE RETURNS

A single "bite" on one of these spam emails can yield several thousands of pounds for the scammer.

The last official estimate from the US Government revealed that Advance Fee scam victims parted with **$5,100 each on average**

Here in the UK, the government estimates that spam email scams cost the UK economy **£150 million annually and each victim an average of £31,000**

SPEAR PHISHING



HOW IT WORKS

Rather than relying on a list of general addresses, Spear Phishing uses a list that more closely resembles finely targeted marketing data.

- The scammer sends a message to a targeted list of people encouraging them to visit a website to resolve an urgent issue such as an unexpected payment or security breach.
- The dupe clicks through the link provided and completes an online form which requests several personal details
- The scammer collects this information and later uses it to empty the dupe's bank account or to create fake identities for use in other fraudulent activities.

"Spear phishing attacks generally yield 2 victims for every 1,000 targeted users. Overall, the attacker can expect a 150,000 dollar profit from a spear phishing attack as opposed to netting 14,000 dollars for a mass phishing campaign"

Jeff Orloff, Internet Security Expert, All Spammed Up

WHY IS SPEAR PHISHING SO EFFECTIVE?

Spear Phishing is effective because:

- Messages are highly targeted
- Branded messages appear to come from legitimate organisations
- The content is relevant to the reader. Fake messages apparently from a particular bank are sent to known account holders, for instance.

It is also worth noting that Spear Phishing targets businesses as well as consumers:

"Half of all respondents (51%) believe that, in the past year, their organization was targeted by a phishing email designed specifically to compromise their own users."

Spear Phishing & Info Security Trends, July 2012

LESSONS FOR YOUR OWN EMAIL MARKETING EFFORTS

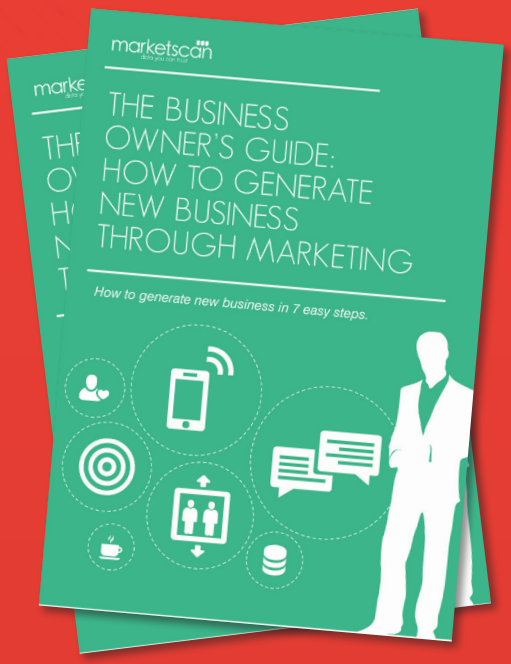
1. The choice of subject line for successful email marketing is critical. Get the subject line right and you can convince your recipient to open your message. Get it wrong and the message goes straight in the bin.

2. The Advance Fee scam makes clear promises to the reader and raises their expectations. If your own email marketing is unclear, or does not give the recipient a reason to read more, you should not expect a great response rate.

3. Both the Advance Fee fraud and Spear Phishing spam email technique rely on urgency to prompt the reader into action. Promises of greater rewards (or dire consequences) ensure that the recipient ignores other indicators and makes an immediate response. The legitimate equivalent would be to offer time limited discounts, for instance.

4. The Spear Phishing spam email method is extremely effective because it uses targeted mailing lists. Messages are tailored to the interests of their recipients, massively boosting the chances of the email being read and acted upon.

5. Spear Phishing relies on accurate data, which is why the scammers spend time compiling and updating their email marketing lists. Your business also needs to ensure that marketing data is up-to-date and accurate for the best chance of creating a significant Return on Investment.



For more great tips, download our free eGuide

THE BUSINESS OWNER'S GUIDE: HOW TO GENERATE NEW BUSINESS THROUGH MARKETING now!

DOWNLOAD FREE EGUIDE NOW!