IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Whale Phishing is Sinking Businesses

Howard Frear

Howard Frear
Director
Sales & Marketing
EASY Software

Biography

Howard Frear has been at the forefront of major trends in the software industry for close to 18 years. He joined EASY Software (www.easysoftware.co.uk) in 2001 and during that time he has been instrumental in developing and overseeing a highly successful strategic partnership with SAP, a relationship that today accounts for more than 50% of EASY UK's software sales. Howard is also credited with many of EASY's largest customer wins including Serco Group, Cable & Wireless and Barclays Capital.

Howard is a very successful and experienced sales and marketing professional and is the driving force behind EASY Software UK's go-to-market and business development strategy. Day-to-day Howard is charged with managing the direct sales force, directing key marketing activities and overseeing strategic partner liaison.

Keywords CEO fraud, Whale phishing, Document Management (DM), Enterprise Content Management (ECM)
Paper type Opinion

Abstract

Fraudsters are using legitimate executive names and email addresses to dupe unsuspecting employees to wire money or sensitive documents to their accounts. CEO impersonation fraud, also known as 'whale phishing' is the latest scam being used by cybercriminals to steal company data – and it is hitting businesses hard. According to the author of this article, control backed by full digital access to relevant information is the way forward.

Introduction

Cybercriminals are now impersonating the 'big fish' – CEOs and other C-level executives – who have access to financial and other sensitive company information into transferring funds, revealing bank details, passwords and other valuable data via email.

Cases are on the increase and the sums of money involved are large. Last year, for example, a member of toy maker Mattel's finance team wired more than $3 million to a fraudulent account in China, after he was spoofed by a message he thought was from the newly appointed chief executive.

In another case, an accountant at French industrial equipment company Etna Industrie was tricked into wiring $542,000 to unknown foreign bank accounts – believing it was rubber stamped in an email from the chief executive as part of a company acquisition.

Unlike traditional phishing scams, these CEO fraud emails are carefully targeted, so do not end up in spam filters and swiftly bypass security. Neither do attackers interact with the victim's bank directly. They cleverly get the victim to do that for them. In addition, these cybercriminals do their homework. They read up on public information about the company and use social media to track employees, so they know who in the company handles money transfers. They ensure they know the organization and its workings extremely well before they trigger an attack.

So how do Whale Phishing emails work? Simple, they play a psychological mind game. Employees do not question them as they are from senior executives. They also come with a sense of urgency, which puts more pressure on employees to act quickly.

Whale Phishing is rising fast. The US Federal Bureau of Investigation (FBI) said that since January it has seen a staggering 270% increase in identified victims and exposed losses from CEO impersonation fraud. The FBI estimates these scams have cost organizations over $2.3 billion in losses in just the past three years.

How to guard against whale phishing

With these kind of scams escalating, companies must not be so naïve as to think it will never happen to them. Remember it only takes one member of staff to be caught off guard. Senior management and CIOs need to look at their operations and work out where they are vulnerable and take the appropriate security steps.

The main area to attack when it comes to any kind of fraud is the so called information gap. The big challenge here is to close that information gap for good. Control backed by full digital access to relevant information is the brick in the wall here. While email security policy should be part of all employee training, senior executives also need to be briefed on how to keep company data safe.

Any kind of unusual behaviour should be red flagged automatically with the support of an anti-fraud system, ideally integrated into a robust contract management system. Most companies, banks and agencies, for example, never put in a request for personal information via email. Any employee who suspects an email might be part of a whale phishing attack should immediately report it to the IT department.

It is the role of information management experts everywhere to ensure that these kind of scams come off the tracks. Whale phishing isn't going to disappear, but companies can mitigate risks to keep cyber thieves out. That means acting now and not when the CFO realizes sizeable funds have been wired from the company bank account to unknown sources!