Combatting CEO Fraud Email Scams

Fraud and cyber crime—which includes any criminal act dealing with computers and networks—are the most common criminal offences in the United Kingdom, according to the most recent data from the Office for National Statistics. In fact, in 2015, approximately 8,000 people and companies each month reported being the target of a phishing scam, which involves fraudsters accessing valuable personal and company data—such as usernames and passwords.

While there are several types of cyber attacks that are considered to be phishing scams, the CEO fraud email scam (also known as 'bogus boss', 'whale phishing', 'insider spoofing', company exec spam and business email compromise) can be the most expensive. Although the average loss is £35,000, it can vary widely with some UK companies reporting losses of up to £18.5 million, according to the nation's fraud and cyber crime reporting centre, Action Fraud.

By understanding the risks involved with the CEO email scam, you can boost your defences to better protect your company from cyber criminals.

The Threat of Email Scams
While the CEO fraud email scam is relatively straightforward, it does require that cyber criminals acquire several essential pieces of information in order to be successful, including the following:

- The company's hierarchy to know who reports to whom
- The names and email addresses of anyone in a senior role that is able to initiate payments
- The day-to-day schedule (and any upcoming holidays, if applicable) of the intended target
- The names and email addresses of anyone who is able to issue money transfers—such as someone in the finance department

Once the fraudster has acquired these pieces of information, he or she will then create an email account that looks legitimate. In general, fraudsters will use one of the following two strategies when fabricating an email address:

1. Registering a domain similar to the company's—for example, firstname.surname@example.com (original) and firstname.surname@exaample.com (fraudulent).
2. 'Spoofing' the genuine email address, which is when fraudsters use a genuine email address but their own domain—for example, firstname.surname@fraudsterdomain.com.

Some fraudsters may even go as far as to contact their intended target in order to learn his or her specific email stylings and aesthetics.

After the fabricated email has been created, the fraudster will use it to contact an employee that is able to issue a money transfer and make an urgent request to wire money to a specific financial institution. Since the email address looks legitimate, the employee generally does not have any reason to believe that the senior staff member's request is fraudulent.

Case Study
To help illustrate the insidious and subtle nature of the CEO fraud scam, read the following case study based on a real-life medium-sized French company that fell victim to the scam.

An accountant at the company received a phone call from an unknown source, who told the accountant that she should expect to receive an email from the CEO with explicit instructions to conduct a financial transaction. The accountant then received an email from the CEO that explained that the company was purchasing a business in Cyprus and that the accountant was to expect a phone call from a consultant, who would explain where to transfer the money.

The accountant received several more emails and phone calls, all of which demanded that she act quickly to ensure that the deal did not fall through. Due to the fraudsters repeated urgings, the accountant authorised £372,000 to be transferred to the fraudster's account. While the company's bank held up three of the approved wire transfers, one worth nearly £100,000 was still approved. This all happened within three hours, which is typical of a CEO fraud email scam. Fraudsters will try to pressure employees to act quickly without hesitation.

The Risks of Email Scams
The following risks are associated with the CEO fraud email scam:

- **Loss of funds:** Any amount of money that the fraudsters are able to extract from a company.
- **Loss of sensitive information:** While fraudsters generally use the CEO fraud email scam to target a company's bank account, they could also use it to obtain sensitive information. This could include bank account numbers, private customer information and confidential documents.
- **Loss of credibility:** After a cyber criminal is able to successfully breach a company's cyber security, it is likely that its investors, customers and the public will lose trust in the company. This loss of reputation could then cause fewer investments and slow business, which could contribute to lower-than-average profits.
- **Fines:** If a company is found to have implemented insufficient cyber security, the Information Commissioner's Office (ICO) could fine it for inadvertently creating conditions suitable for cyber crime or mishandling sensitive data.

How to Protect Your Company
In order to protect your company from the potential risks associated with CEO email fraud, your company should consider implementing these four strategies:

1. Verify any payment requests that are unexpected or appear to be unusual either over the phone or (preferably) in person. Do not use the contact details provided in the potentially fraudulent email.
2. Establish a process for requesting and authorising payments that requires two points of contact. This process should include a verification step in order to identify potentially fraudulent requests.
3. Organise a procedure for what employees should do if they receive an unusual or suspicious email asking them to authorise a money transfer.
4. Provide your entire staff—from the directors and officers all the way down to interns—with comprehensive cyber security training to ensure that they know how to identify and manage cyber security threats. In addition, everyone's password should be robust and be comprised of both lowercase and uppercase letters, numbers and unique characters.
5. Choose your social media friends carefully—befriending targets using bogus social media profiles in order to find personal information is a common cyber criminal tactic.

In addition to the strategies outlined above, fraudulent emails generally display at least one of the following characteristics:

- The sender's email address does not match the organisation's website address, or it has been sent from a completely different address.
- There is an unnecessary sense of urgency accompanied by the request, while imploring the recipient to not communicate with others and keep the request confidential.
- The email's text is contained within an image rather than a text box.
- The email requests that you provide a comprehensive amount of personal information, including your username, password and bank details.
- The email implores the recipient to bypass normal accounting processes for the sake of 'expediency'.

Consider Before You Click
CEO email fraud could be devastating, costing you thousands or millions of pounds in lost funds, lost business or fines. Fortunately, with the proper precautions, your company can adequately defend against cyber attacks. Contact GS Group today for more information on the importance of securing robust cyber cover and managing your cyber risk.