Understanding fraudulent instruction

Danger

Fraudulent Instruction is the transfer of funds by an employee, outside of an organization to a third party, as a result of deceptive information provided by a criminal purporting to be someone else, typically a vendor, client or authorized employee.

These social engineering scams have targeted the legal profession and attacks on businesses across industry sectors are increasing in frequency and sophistication.

Even at the best-managed companies employees can still fall victim to these fraud attempts which usually emphasize the time pressure and confidential nature of the transaction. Ultimately if these frauds are successful it is often too late to undo all of their costly implications.

Tips to help spot a fraudulent instruction

- The sender claims to be traveling and available only by email.
- The sender claims to need the information urgently.
- The request is formatted to look like it's sent from a mobile device in order to make it harder for you to recognize that something is off.
- The sender's email address will be similar to our CEO/CFO's – often off by only a character or two. For example:

  CEO@company_xyz.com vs. CEO@company-xyz.com

Therefore it is important for all businesses to be aware of the expanding exposure and to prepare and protect through a variety of defenses.

Advice to protect yourself

Out of Band Authentication A method of challenge and response to the requestor of a transfer, payment or delivery of money or securities by an Insured, via a method other than the original means of request, to verify the authenticity or validity of the request.

Dual Authorisation A method by which third party payments must be authorized by two personnel from the same business, providing an additional level of security.

External Email Tagging A means by which incoming email from outside the organisation are tagged "EXTERNAL" (or otherwise), to prevent deception.

Anti-Virus Software All anti-virus software and firewalls should be constantly updated to defend against the evolving nature of fraud practices and to block incoming specious traffic where possible.

Security Awareness Training All employees, particularly those with an increased risk of being targeted should be kept aware of developing exposures via a security training program, inclusive of fraud detection practices.

Loss scenarios

A law firm representing a client at a real estate closing was to receive a wire transfer of $250,000 representing the sale proceeds. Prior to this, the paralegal's email had been hacked and emails were sent impersonating the client requesting a change of account details. By the time the fraud had been detected the funds had been removed from the overseas account.

An employee at technology company in Massachusetts received an email from what appeared to be the CEO regarding an acquisition that needed to remain confidential and be executed with urgency. This resulted in the transfer of $40,000 to an overseas account held by a third party. When the company finally became aware of the breach, they were only able to recover $8,100 of the stolen funds.

CBSL489_US_03/17