*Risk*MATTERS

Social Engineering Fraud

WHAT IS SOCIAL ENGINEERING FRAUD LOSS?

There have probably never been as many threats to a company as there are today. Everything from "old fashioned" employee initiated dishonesty to sophisticated "cyber" style hacking is or ought to be on the radar of every company and their Board.

An old threat has recently reemerged and criminals are finding success with it at alarming rates. This new scam has many names but is generally called Social Engineering Fraud or Impersonation Fraud.

The scam quite simply involves a third party impersonating a key individual, be they a fellow employee, an executive, customer or supplier of products/services and through trick or artifice, they get an employee to voluntarily part with something of value. The target is either money or valuable information.

Their methods are varied but contain common themes. The medium of choice these days seems to be email, but can include phone calls or more brazenly, impersonating someone in person.

The level of sophistication is usually quite startling and will likely involve an intimate knowledge of the company, a specific transaction or the clients/suppliers with whom the company conducts business. There will nearly always be a sense of urgency associated with the request or will play on various emotions (pride, sympathy, fear) – or both.

What is most alarming for many companies is that no matter what protocols or safeguards are in place, because the target is always a human, there is no certain defence that can be implemented or fix that can be purchased. Because of this, many are left awake at night wondering if, or more accurately when, they will become a target of these fraudsters.

The bright side to all of this however, is that with a little training and a strong sense of awareness within the company, most of these types of losses can be avoided.

In addition to this, for those companies that can demonstrate an active awareness and have a plan in place to avoid these types of losses, The Guarantee is responding to this ever evolving threat and can help to transfer some of this risk away from the company.

We strongly urge you to read the accompanying loss examples and tips to avoid being the victim of social engineering fraud to help raise your awareness of the problem and to use these tools to create a starting point in making your organization less attractive to these types of fraudsters.

SOCIAL ENGINEERING FRAUD LOSS EXAMPLES

Consider Some Examples Of Social Engineering Fraud Losses:

1 VENDOR IMPERSONATION FRAUD

An employee of ABC Manufacturing receives an email from a long standing vendor advising them that they have recently changed banks and sends the correct form to change the wire instructions. The employee updates the file. Several months later the vendor advises ABC's accounts payable department that they have missed the last three payments and are over $100,000 in arrears.

When ABC advises that all payments have been made and the vendor confirms they never received them, red flags go up.

During the review it is discovered that the email with the wire change instruction was fraudulent – two letters were inverted and the employee did not notice. The police are called and the new wire information leads them to a bank in Asia. No proceeds were recovered.

2 EXECUTIVE IMPERSONATION FRAUD

A mid-level employee, John, in the finance department, received an email from the CEO in which he says he is overseas on business and in urgent need of getting a payment out to a new IT vendor quickly to avoid missing a key deadline. The CEO said he was told by the head of finance that John was the person "that could get it done". The CEO provided an invoice for some IT consulting work in the amount of $47,500 and advised it had to be paid by the end of the day. The CEO thanked him in advance for helping the company avoid "looking foolish", noted he would get confirmation from the IT firm once payment was received and commented that John had a bright future with the company, noting the head of finance had "lots of good things to say about him".

John promptly wired the funds and left for the day feeling good!

During the next review the audit team contacted John as they were unable to locate the matching invoice. It was only when he forwarded the CEO's email that it was discovered the CEO's email address had been hacked and the instructions were fraudulent.

No proceeds were recovered.

3 CLIENT IMPERSONATION FRAUD

The CFO of a relatively new client of the Insured, a service provider, calls and advises that they have lost a key contract, their usual contact person had been laid-off and they need to cancel their agreement with the Insured. The client makes an emotional appeal, advising that unless they're able to recover some of the money they had paid up front for the contract, the company might go bankrupt. They explained they were embarrassed and having to call many of their service providers; gratefully most were agreeing to help them out. They'd also moved offices to downsize and lessen their rent payments. The Insured considered the contract to be pretty small and agreed as a good gesture to refund the $17,000 that was unearned on the contract to the client.

Within a few weeks, the Insured starts to get complaints from the client that service calls were going unanswered. Shocked that their contract had been cancelled, the client shows up at the Insured's office and it is then that the fraud is uncovered. They had never moved offices and were in excellent financial shape. By then, the $17,000 cheque had been cashed and the PO Box which was used as the 'new office' had been vacated. An investigation is still ongoing but it was discovered that the PO Box was rented with a fraudulent ID.

TIPS FOR EMPLOYEES TO MITIGATE EMAIL-BASED SOCIAL ENGINEERING FRAUD

While social engineering fraud is certainly increasing in sophistication and frequency, implementing the following basic controls will help mitigate the fraudster's chance of success:

1 SLOW DOWN AND BE APPROPRIATELY SKEPTICAL

One of the most common themes in social engineering fraud is that the fraudster creates a sense of urgency. The target is often asked to move quickly in order to avoid missing a deadline or upsetting a client/vendor/manager/executive.

When it comes to transferring funds or sharing information, there is always a case for moving at a measured pace.

It isn't required that you look through life expecting the worst of people, but a healthy level of skepticism is a good thing.

2 CHECK THE ADDRESS AND AVOID USING 'REPLY' TO ACCEPT OR RELAY SENSITIVE INFORMATION

More and more social engineering frauds are taking place through forged or altered email addresses – amended to look very similar to authentic addresses. When responding to requests that ask for confidential or sensitive information to be disclosed or altered, closely verify the address and start a new email chain to the known address to carry on the communication. You should, however, whenever possible, avoid using email to complete these types of transactions. Remember though, if the email address is correct, it doesn't mean it is a legitimate email. Continue to be vigilant.

3 VERIFY WITH A KNOWN SOURCE

Given that fraudulent emails may originate from a legitimate email address (the account may have been hacked) whenever you are asked to make changes that involve sensitive or confidential information (payment/banking info, contact information, primary contact person, mailing address etc.) always verify with a known contact that the person who contacted you is authorized to make those changes or is who they say they are. Pick up the phone or when possible meet in person to confirm.

4 BE UP FRONT IF YOU THINK YOU'VE BEEN A VICTIM

It happens more than we'd like. If you think you may have been the target of a social engineering attack, successful or not, tell your manager so that they can act early. Sometimes it is only through hindsight when you may realize something was off. Often a quick response can minimize the damage. Hiding it, avoiding it or hoping it goes away will only ensure that the potential loss is bigger and/or harder to recover.

5 CREATE AN ENVIRONMENT THAT PROMOTES CAUTION AND HAVE ESTABLISHED PROTOCOLS

If you are in a position where you give instructions to others or have people report to you, encourage them to verify important or atypical requests and offer praise when they do. Often people don't verify because they don't want to risk upsetting a busy manager or executive within the company.

Create internal protocols that address making changes to or disclosing sensitive or confidential information, so that employees don't have to make it up as they go. Give them the tools to protect themselves and the company.