Courtesy of
Crendon Insurance Brokers Ltd

CYBERRISKS&LIABILITIES_

Protecting Your Intangible Assets from Social Engineering Fraud

Imagine a couple of men walk into your business with fire service badges, walkie-talkies, proper identification, etc. They tell the receptionist at the front desk that they are there for a routine fire safety inspection. Your receptionist lets them in because they look and play the part perfectly. The two men split up, seemingly conducting different parts of the fire inspection and return to the receptionist 15 minutes later, explaining they have completed their assessment. They walk out the door and are never seen again. Nothing to worry about, right?

Wrong. You've just been the victim of a well-thought out social engineering scam. Days or weeks later, your computer system is compromised, customer credit card numbers are stolen and sales are dropping. So what happened?

What is Social Engineering?
Social engineering is the act of taking advantage of human behaviour to commit a crime. Social engineers can gain access to buildings, computer systems and data simply by exploiting the weakest link in a security system—humans. For example, social engineers could steal sensitive documents or place key loggers on employees' computers at a bank—all while posing as fire inspectors from the nearby fire service, as seen in the example above.

Social engineers don't need to have expert knowledge of a company's computer network to break in to a business—all it takes is for one employee to give out a password or allow the engineers access to an area they shouldn't be in.

Social Engineering Tactics
If you can learn to identify the ways in which a social engineer might try to break into your business, you can stop a threat before it begins.

Social engineers are masters at blending in. They research their target for weeks or even months, learning the smallest details to gain entry into a company. They are often sweet-talkers and their body posture lets others believe they belong.

Social engineers often work in groups of two. In the opening example, the two men split up to conduct a "fire inspection." Keeping them together could have saved the company a lot of time and money. Always make sure there are eyes on visitors at all time.

How to Prevent Social Engineering
Being a victim of a social engineering scam can have a wide range of effects on your business, including:

- Damaged reputation
- Lost sales
- Humiliation
- Lower staff morale
- Losing customer base

All these effects take a lot of time and money to reverse. Because humans are naturally trusting, it can be difficult to identify when we are being socially engineered. However, there are ways to prevent social engineering from potentially ruining your business:

- There should be policies in place at your business that limit or eliminate the amount of sensitive information that is made available to your employees, customers or the general public. Never allow employees to give out passwords or credit card numbers over the phone. If this information is needed by another employee, meet face-to-face.
- Make sure employees never write down their passwords on paper. A piece of paper with important passwords on it can be swiped by a social engineer in the blink of an eye. Make sure your employees' computer passwords expire after a set amount of time, generally three months. Set guidelines for new password creation, but keep in mind that complex passwords are difficult to remember. If passwords are reset too frequently or

Crendon Insurance Brokers

are too hard to remember, employees will end up creating passwords that can easily be guessed.
- Consider installing security cameras around your building. Make sure to keep an eye on areas where security is lax, such as a smoking area or near an unguarded back door.
- All visitors should be greeted and presented a sign-in sheet to fill in.
- Prohibit employees from posting work-related information on social media websites. Often, social engineers spend weeks or even months learning about employees' habits and tendencies before making a move. A simple post about being out of the office for a short length of time could be all a social engineer needs to steal sensitive information. Let employees know that posting otherwise harmless information on the Internet, such as a telephone number or address, could be the final piece of a social engineer's plan of attack.
- Have employees wear badges with their name and picture on them, and have employees swipe their badge to gain access to different areas of the building. Let your employees know that it is not OK to let in employees they don't recognise because they "forgot their badge." This is a common technique to get social engineers in the building.
- Subject your company to penetration testing. Hire an outside agency to act as a social engineer and see how your employees respond. If the test is successful, your employees will be embarrassed. That can lead to extra motivation to be vigilant of social engineers if they were to try and gain access to your company.

Are Your Intangible Assets Adequately Protected?
Social engineering can be a very effective way for a criminal to steal your digital assets. Contact Crendon Insurance Brokers Ltd today to learn more about our resources and cover options to protect your company against losses from social engineering.