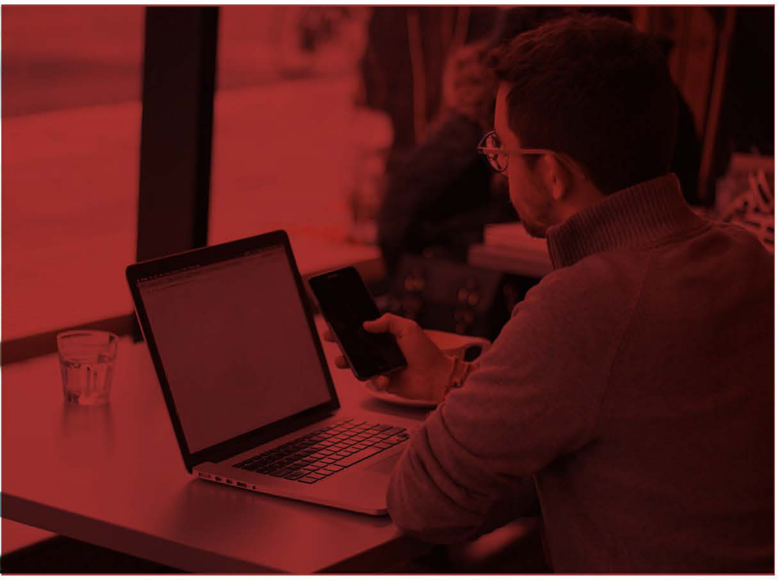
Lancashire
Cyber Foundry

What is Social Engineering?

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

When people think of a hacker, often they picture someone in a dark room with their hood up frantically typing on a keyboard, but often the most dangerous hackers are the ones who operate under everyone's noses. Social Engineering, or human hacking, is one of the most common ways people have data and information stolen. Social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes." As security software keeps improving many hackers have realised that the weakest link in the security chain is the person already behind the security system.



The social engineer will manipulate people who already have access to sensitive data to give that to them without ever having to use a computer themselves. Sometimes the information that the manipulator will receive is harmless on its own, but it may be one piece of the puzzle that the social engineer is building. Social engineers will extract any information that they can which will be used to destroy a company's reputation and in some situations will cause monetary damage. Even if a company's cyber security is up to date it is important to know how to ›revent social engineers.

European Union
European Regional Development Fund

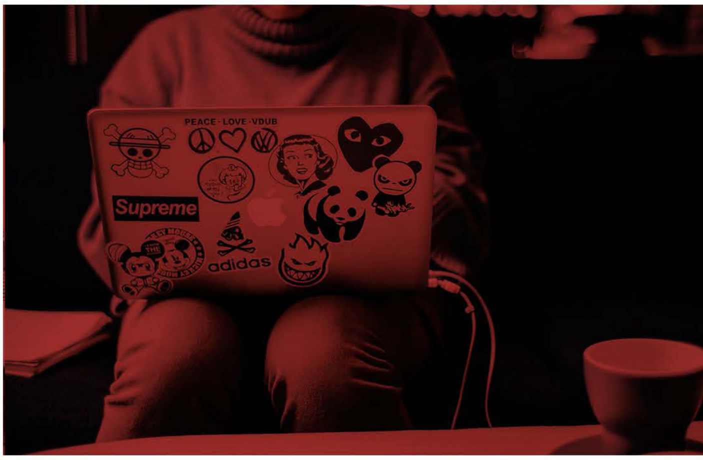
NORTHERN POWERHOUSE HM Government

Lancaster University

'ACT NOW OR LOSE YOUR ACCOUNT'

There are many different types of 'attacks' a social engineer will carry out but fundamentally they all focus on aspects of psychology and how to use that to manipulate people into giving up sensitive information. The most common and well-known type of attack is phishing. This is when a target receives an email that often contains a malicious link asking the user to submit sensitive data. These attacks often trigger the fight or flight instinct with threatening titles such as "ACT NOW OR LOSE YOUR ACCOUNT!" This is done as people do not think as logically when they are acting on instinct, instinct is easier to predict and are less likely to view links with distrust.

In the past phishing emails were easy to detect as often they were sent to mass mailing lists and would often contain many grammatical mistakes, although most people avoided them it would only take one person to click a false link to bring the system down. Recently, phishing attacks have become more sophisticated, being professionally written and the target has been better researched resulting in more convincing emails making them harder to detect. There are several distinct types of attacks used by social engineers and these will be covered in more detail in a following article.



Thankfully, social engineering is extremely easy to prevent simply by having a well-trained team and procedures for verifying and authorising data transfer. The simplest way to prevent social engineering attacks is to verify where the request for information is coming from. If an email says a bank account has a problem, visit the trusted website of the bank using the browser and not clicking on any links in the email or call the trusted number for that company. The trusted website or phone number would then be able to confirm or deny if the bank account in question has a problem. It may take a few moments longer than just clicking a link but is significantly more secure and has the potential to save a company from monetary and reputational damage.

ABOUT THE AUTHOR

Alexander Lee

Alexander Lee is an analyst developer on the Lancashire Cyber Foundry. A recent graduate from Lancaster University with a Masters in Physics he has always been interested in programming and coding, making sure to use it throughout his degree. With experience in developing physics software and simulations Alexander now works to provide support to businesses through research and development for technical projects.