The Art of Hacking Humans: Intro to Social Engineering

Pretexting

Pretexting involves a malicious attacker deceiving an unsuspecting victim by pretending to be someone else in a bid to gain unauthorized access to sensitive data and information. The social engineer may pretend to be calling from somewhere like helpdesk, IT or pretend to be someone of high authority. The deceit is usually carried out by calls or sometimes through messaging like email or social networks. Email spoofing can be seen as a form of pretexting, it is a kind of social engineering technique where the attacker sends an email that appears to be from a legitimate source to the victim. CEO frauds tend to be perpetrated through pretexting by way of calls or email spoofing.

The attacker would contact a victim (whether through voice calls, email or other messaging applications) claiming to be from IT helpdesk for example, requesting for some sensitive data (like username and password, date of birth, etc) saying that the data is required for an upgrade or something similar. Once such data is acquired, it can be used to access the victim's systems and network, an infiltration to steal more sensitive data and information, siphon funds from bank accounts, install malware or add the compromised systems to a botnet.

Conheady (2014) mentioned a case in which some online brokers used pretexting to compromise Verizon Wireless. This was achieved by the brokers calling customer service and claiming to be from the special needs department of Verizon Wireless (which did not exist) and making a request on behalf of a vocally impaired customer, even using a voice distorting device to make their voice sound impaired when the Verizon Wireless customer service officer asked to speak to the customer. The result was that thousands of private cell phone numbers of Verizon customers were released (Social Engineering, Inc., 2017). CNBC (2015) reported money transfer company Xoom lost $30.8 million to employee impersonation (pretexting), leading to the resignation of the chief financial officer.

Pretexting takes advantage of human gullibility, willingness to assist and zeal to carry out duties. The victims easily trust others so tend to fall for scammers who pretend to be their superiors or help desk or something like that; they respond to such scammers because they are deceived into thinking they are communicating with a genuine source, so respond to the request with ease.

Extra vigilance and awareness of pretexting can help avoid falling victim to the technique. Employees should be educated to be wary of such techniques and to be careful of what kind of information and data they reveal to wrong parties. Customers of organizations should also be enlightened as per pretexting and similar techniques, and should be made to understand what type of information and data they should not disclose unnecessarily. The customers should be educated about the kind of data that an organization will not request for them, of which if they see request for such should not oblige. Clear numbers and lines of communication should be clearly stated to protect against both employees and customers falling victim to communication that is clearly not from such sources.

References:

CNBC (2015) *Xoom says $30.8 mln transferred fraudulently to overseas accounts* [Online]. Available from: https://www.cnbc.com/2015/01/06/xoom-says-308-mln-transferred-fraudulently-to-overseas-accounts.html (Accessed: 23 October, 2017).

Conheady, S. (2014) Social Engineering in IT Security: Tools, Tactics, and Techniques. McGraw Hill Education.

Social Engineering, Inc. (2017) *Vishing* [Online]. Available from: https://www.social-engineer.org/framework/attack-vectors/vishing/ (Accessed: 23 October, 2017).