The Art of Hacking Humans: Intro to Social Engineering

Phishing

Phishing is a deceptive technique used to gain unauthorized access using communication channels by imitating a known genuine source. It is quite similar to pretexting as both make an appearance of being from a genuine source, but the most common way of propagating it is through email. Phishing is usually used to steal sensitive data like login credentials, online banking details or payment card details. Phishing messages usually come with a link or an attachment. The link could be made to appear from a genuine source, like your bank, and clicking may result in a webpage that is an exact clone of the website it claims to be (like your bank's online banking logon page); the page would include the space for username and password, which if entered gets you compromised. The link may also open to an error page or not even open at all making it appear as though there was an error, but the result of the clicking is installation of malware on the system; attachments also have a similar result. The malware can be used for various attacks, like stealing login credentials, taking over logical access, adding the compromised system and/or network to a botnet and so on.

Phishing can come in various forms other than through email messages like SMS messages or social media messages and so on. Phishing carried out through SMS is known as **smishing** and can get a mobile device compromised or lead you to a fraudulent site to steal your data. Another form of phishing is **vishing**, which is carried out using voice messages that can direct to fraudulent URLs or get systems infected. Phishing phishing is usually directed towards random targets, but those targeted towards a specific set of people, like high net worth customers of a specific bank, is known as **spear phishing** – we had mentioned in the brief historical overview section that the letter from Jerusalem could be seen as a precursor to spear phishing.

Phishing takes advantage of human gullibility and lack of awareness. Some phishing messages may state that someone's account will be blocked if necessary action is not taken by clicking a link or following instructions in a attachment; these type of attacks also take advantage of fear – fear of losing something. Below is an example of a phishing email claiming to be from a bank requesting a link be clicked to complete an upgrade:

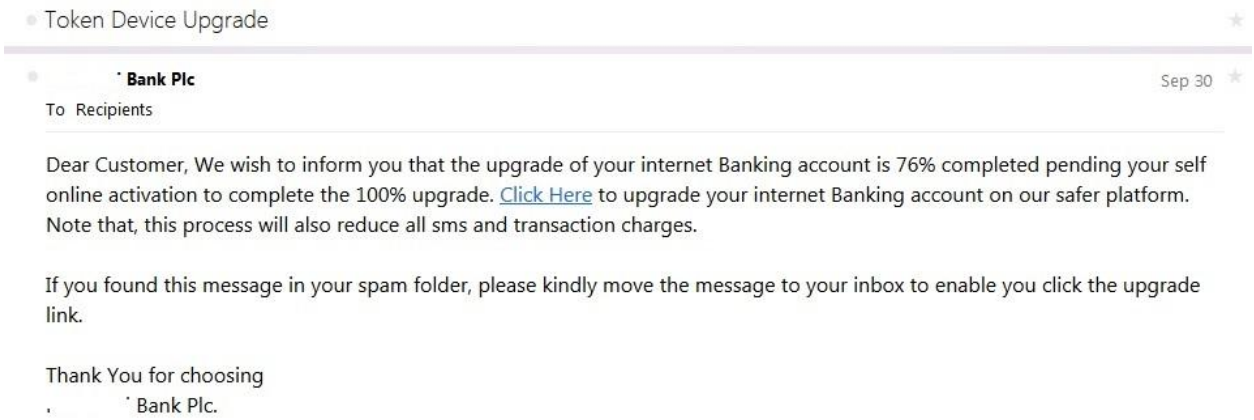

Figure 1: Sample phishing email

Avoid clicking on links or opening attachments from unknown sources, and even those apparently from known sources without some level of confirmation; hover your mouse cursor over a link to show you the actual URL. The wording of messages would likely not be that used by the person the message is supposedly from, but even if you cannot decipher the wording you can contact the apparent sender to ensure whether the person sent such message. Bottom line: phishing can bested be tackled with awareness. Organizations should educate their employees and customers on phishing to help them avoid falling victim. Organizations in the financial sector, like banks, usually send messages to their customers to avoid clicking links sent to them for banking transactions, but rather to go straight to the bank's website and initiate any transaction from there; they also notify their customers that they would not send messages requesting sensitive data to them.