**Here are the seven principles of influence and how I believe they translate to phishing:**

**1) Reciprocation**– This is simply “give and take”, a version of “you scratch my back, I scratch yours.” An email promising to give access to confidential information if a certain attachment is downloaded or a link is clicked is a classic example of this principle being leveraged in phishing.

**2) Scarcity** – People want what is difficult to get. Phishing emails that stress that a certain benefit is accessible only if action is taken within a short period of time (“download this attachment to continue having access to your email”) is an example of this principle at play.

**3) Authority** – People defer to authority. That’s why many phishing emails seek to impersonate senior executives / Human Resources / Information Technology / Finance. An email from the CEO (supposedly) asking the Finance department to immediately wire $300,000 to an account unknown to the department is an example scenario that has occurred many times in the past.

**4) Consistency** – You must have heard the expression “creature of habit”. In some way, all of us are creatures of habit in that we like to go about our lives in set ways. Phishing emails that look like official communications exploit this fact, hoping the recipient overlooks the unusual request that is included in such an email. An email with the Amazon logo saying a shipment is held up and asking the recipient to confirm their home address may not raise red flags even if no shipment is expected; that’s the power of a recognized brand.

**5) Consensus** – We have all seen the power of the crowd, from frenzied fans at a rock concert or the mad mobs in riots. People have a tendency to follow other people. A phishing email that mentions something like “544 of 800 employees have updated their software, click this link to download” seeks to exploit this fact.

**6) Liking** – This is an extremely obvious principle of influence, and something that we use daily. If people like you, they will say “yes”. Conversely, if people want to be liked, they will also say “yes”. This is exploited by phishers when they target eager-to-please new employees. An email from HR (supposedly) asking a new employee for their SSN to update in payroll is one such common ruse.

**7) Unity** – This was not in the original list but was added later by Cialdini. The idea is that the more we identify ourselves with others, the more we are influenced by them. A phishing email supposedly sent by someone who shares the same interests as the recipient, information that can easily be sourced through social media, has a high chance of success. For example, if a person loves dogs, an email from another dog-lover (supposedly) with an attachment of cute dog pictures (supposedly) has a high chance of being opened.