**Sosyal Mühendislik saldırısı yöntemlerinden “Sahte senaryolar uydurmak (pretexting)” yöntemine değinelim. Genellikle telefonla veya bire-bir tarzda gelişen saldırı yöntemidir. Hedefin belirlenmesi, hedefe dair bilgi toplanması, hedefle iletişim/ilişki kurulması aşamasından sonra saldırıya geçilir. Amaç, sahte bir senaryo/hikaye uydurarak bu senaryonun içine serpiştirilmiş tuzaklarla hedeften istenilen bilgiyi almaktır. ( ilerleyen aşamalarda kullanmak üzere kişisel bilgiler, şifreler, özel bir sır vs) Telefon üzerinden yapılan saldırılarda hemen her şekilde elde edilebilecek bilgiler sorulur ilk olarak. Ancak yetkinlendirme için gerekli bilgilerin istenmesine sıra gelmesi için sosyal mühendis profesyonellik gereği ağır ağır ilerleyecektir. Sonunda bilgi isteme aşaması hassas bilgiler olan doğum tarihi, kimlik numarası vb bilgilere gelecektir. Sahte senaryolar uydurmak diğer adıyla pretexting yönteminde başarı oranı oldukça yüksektir. Çünkü saldırgan plan dışı olayları/durumları da göz önünde bulundururak kendini herşeye karşı hazırlıklı olarak donatacaktır. Böyle olunca hedefin saldırıyı anlaması ve karşı koyması bilgi çalınmasına izin vermemesi oldukça zor.  
  
Pretexting yönteminde saldırı başlangıcında güçlü ve etkili olabilmek için hedefe dair bazı bilgilerin elde edilmesi gerekir. Bu bilgiler hedefle iletişime geçmeden önce toplanır. İletişim kurulduğunda hedefe hakkında bildiklerinizi ara ara söylenir belli edilir. Bu şekilde güven duygusu oluşturulacak ve ilerleyen aşamadan asıl hedef olan “hassas bilgiye” ulaşmak için uygun zaman kollanacaktır. Saldırgan hedefi ile arasında sosyal mühendisliğin altın kuralı olan “iletişimi” iyi kurmuş ve güven duygusu uyandırmışsa eğer hassas bilgiye sıra geldiğinde elde etmekte zorlanmayacaktır.  
  
Bu kadar bilgiden sonra gerçek hayattan bir pretexting saldırısı ile yazıyı bitirelim.  
  
Bir bilgi güvenliği danışmanlık firması, bir bankanın bilgi güvenliğinden sorumlu müdürünü ziyaret eder ve bankaya bilgi güvenliği testi yapmayı teklif eder. Müdür itiraz eder. Güvenlik firması danışmanı ile arasında şöyle bir konuşma geçer;  
  
Sosyal Mühendislik  
  
- Bizim böyle bir teste ihtiyacımız yok. Yeterince güvenliyiz. En iyi yazılım ve donanımları satın aldık ve piyasadaki en iyi personel bizde. – O zaman biz size bir test yapalım, eğer bir açıklık bulursak ücretimizi alırız, eğer herhangi bir açıklık bulamazsak ücret talep etmeyiz.Bu arada danışmanlık firmasından bir personel lavaboya gitmek üzere toplantıdan ayrılır ve o sırada sekreterin, bilgisayarında film sitelerini incelediğini görür. Hemen yanına yaklaşır ve filmlerle ilgili konuşmaya başlar:- Bu aktörün son filmini seyrettiniz mi? Eğer seyretmediyseniz sizin için DVD’ye çekip gönderebilirim.  
  
- Çok memnun olurum. Tabii sizin için zahmet olmayacaksa. O günkü toplantıdan sonra danışman ofise döner. Zararlı bir yazılım ile birlikte filmi DVD’ye çeker ve kargoyla sekretere gönderir. Zararlı yazılımın sekreterin evdeki değil de ofisteki bilgisayarında çalışmasının garanti etmek için telefon eder.  
  
- Size kargoyla gönderdiğim DVD’yi bir bilgisayarınızda dener misiniz? Bazen kaydederken hata olabiliyor. Sekreter de denemek amacı ile DVD’yi çalıştırır ve filmin çalıştığını söyler, teşekkür eder ve telefonu kapatır.  
Zararlı yazılım ofiste etkin hale gelmiştir ve yaptığı iş bilgi güvenliği müdürünün bilgisayarında, masaüstüne “Sisteminizi ele geçirdik, geçmiş olsun http://www.turkhackteam.net/images/smilies/smile.gif” yazan bir not bırakmaktır.  
  
Gördüğünüz gibi çok basit bir yöntem ile yapılan bu saldırıda elde edilen bilgi saldırının basitliğinin aksine hayati öneme sahip. Neticede bir şirketin dijital ortamdaki tüm bilgilerine erişim söz konusu. Bu yüzden pretexting yöntemi uygulanabilirliği ve başarı oranı en yüksek olan sosyal mühendislik yöntemlerindendir. Önemli konumlarda ve hassas bilgilere sahip olan insanların daima “sorgulayıcı” olmaları gerekmektedir.**