Phising nedir?

Phising yani oltalama saldırısı kullanıcıların şifreleri, kredi kartı bilgileri gibi gizli verilerini ele geçirmek amacıyla yapılan saldırılardır. 1990'lı yıllardan beridir kullanılmaya devam etmektedir. Hala da günümüzde sıkça kullanılan siber saldırı türlerinden birisidir. Kurbana sosyal medya veya iletişim yoluyla bir kurum veya normal bir birey olarak gözükerek belirli eylemleri yapmasını ister.

Nasıl çalışır?

Phising bir e-posta veya telefon yoluyla kurbanla iletişime geçildikten sonra çalmak istediği sosyal medya sitesinin arayüzüne benzer yapıdaki kendi oluşturmuş olduğu web sitesine yönlendirir. Bu site kurbanın yazmış olduğu verileri doğrudan saldırgana verir. Ardından kurban ne olduğunu bile anlamadan normal sosyal medya web sitesine yönlendirilir. Bir çok farklı seneryo ile bu saldırı oluşturulabilir ancak işleyiş her zaman aynıdır.

Nasıl korunulur?

Bu saldırı yönteminden korunmak için bir çok sosyal medya şirketi güvenlik politikaları uygulamaktadır. Verilerimizin korunması için ayrıcalıklı erişim yönetimi, çift faktörlü kimlik doğrulama, merkezi parola yönetimi ve yetkili oturum yöneticisi gibi yöntemler kullanılabilir. Bu yöntemlerin yanı sıra aldığımız e-posta ve aramaların kurumsal hesaplar üzerinden olduğundan emin olmalıyız. Yönlendirildiğimiz linkin https sertifikasının olup olmadığını kontrol etmeliyiz.

Sonuçları:

Bu saldırı için github ve stackoverflowdan instagram html ve css kodlarını aradım ancak bulamadım, instagram bu kodları phising saldırıları yapılmaması için kullanım dışı bırakmış. En sonunda bir tane phising kodlarını buldum domain almak için başvuru yaptığımda domainimi engellediler. Yani bu yöntemi uygulamalı olarak gösteremedim.