

Güvenli bankacılık için .bank alan adları



ÇETİN KAYA
KOÇ

Ortalama bir kullanıcı
Internet bankacılığı
oltacılarından
günde 3-5
tane e-posta alıyor.

Internet bankacılığı oltacılarından hiç olmazsa günde 3-5 tane e-posta alıyorum: “Şu noktaya tıklayıp abc bankasındaki hesabınıza ulaşabilirsiniz” Tecrübe ve bilgi birikimi nedeniyle böyle saldırıların bana zarar vermesi olası değil, ancak her kullanıcı da aynı değil. Yüzlerce belki binlerce banka müşterisi şifrelerini bu oltacı web sayfalarında kaybetti ve zararlarına uğradı. Türkiye’de Internet bankacılık mağdurları içine düştükleri durumu kamuya anlatmak ve zararlarının telafisi için web sitesi bile kurdular. Adliye, bankacılar, avukatlar ve kullanıcılar arasında geçen bu tartışmalar sürmeye devam edeceğe benzer.

Problem şu: Kullanıcı tıkladığı URL’in kendi bankasının URL’i olup olmadığını dikkat etmezse, kendi bankasının sayfası yerine (örneğin, <http://abc-bank.com.tr>) bambaşka bir noktaya yönlendirilmiş olur (örneğin, <http://abc.tc/abc-bank.com.tr>). Bu benzerliğe yanılıp, abc bankasının Türkiye’deki web sitesi yerine, özel olarak hazırlanmış “Turks & Caicos Islands” ülkesi adına kayıtlı abc.tc sitesine ulaşıyor ve bu sitedeki login sayfası da kendi bankasının login si-

tesine çok benzer (görünüş olarak tamamıyla aynı) olduğu için login name, şifre ve PIN numarasını giriyor. Bu bilgileri elde eden balıklı hacker’ler bir kaç dakika sonra, kullanıcının abc bankasındaki gerçek hesabına girip, para havaleleri veya başka ödemeler yapıp veya kredi kartı ve kimlik bilgilerini elde edip, kullanıcıyı zarara sokuyorlar.

Aldanmamak için nereye tıkladığınıza ve nereye bağlandığınıza dikkat edin. Ancak bilgi güvenliği uzmanlarının böyle saldırıları önlemesi söz konusu olmaz mı? Yakın zamanda bir öneri yapıldı: Bir .bank alan adları kategorisi yaratılmalı ve bir banka kurumsal kimliğini ispat edip, böyle bir isim alsın ve bu isimler başkalarına kesinlikle verilmesin. Örneğin İş Bankası veya Akbank’ın siteleri, şu andaki gibi is-bank.com.tr veya ak-bank.com.tr yerine is-bank.bank veya ak-bank.bank (veya kısaca is.bank veya ak.bank) olsun. Bu basit alan adları kolaylıkla tanındığı için, kullanıcılar hemen farklı noktalara çekildiklerini fark ederler ve avlanılmazlar. Bu çözüm yeterli olacak mı acaba? Devamı iki hafta sonraki yazımızda.

koc@krip.to