Şifre Güvenliği

İnternet ortamında belirlediğiniz şifrelerimiz genelde aynı ve basit şifrelerden oluşmaktadır. Ayrıca, bir sosyal ağ üyelik şifremiz ile e-posta şifremiz ve hatta banka kartlarımızın şifreleri aynı olabilmektedir. Basit şifreler olarak günlük yaşamda kolay hatırlayabileceğimiz kişisel bilgilerimiz; doğum tarihimiz, doğduğumuz yer, telefon numaramız ve '123456' kombinasyonlarından oluşan ve kırılması oldukça kolay şifrelerden oluşabilmektedir.

İnternet ortamında farklı hesaplar için aynı ve tahmin edilmesi kolay şifreler belirlenebilmektedir. Bir sosyal ağ üyelik şifresi ile e-posta şifresi ve hatta banka kartı şifresi aynı olabilmektedir. Tahmin edilmesi kolay şifreler; doğum tarihi, doğum yeri, telefon numarası, yakınlarının isimleri gibi kişisel bilgiler veya '123456' gibi sıralı rakamlardan oluşmaktadır.

Güçlü şifre nasıl oluşturulur?

- En az 8 karakterden oluşmalı
- Harf, rakam ve özel karakterler içermeli (@,#,$,%,^,&,!).
- Küçük ve büyük harfler bulundurmalı (k, B)
- Kişisel bilgiler, sözlükte olan kelimeler ve sıklıkla kullanılan kolay tahmin edilebilir bilgilerden oluşmamalı
- Bütün hesaplar için farklı şifreler belirlenmelidir.

Hatırlaması kolay güçlü şifre önerileri için tıklayınız.

Basit ve aynı şifreleri kullanmak niçin tehlikeli?

Basit şifreler kişi hakkında bilgi içeren ve tahmin edilmesi kolay şifrelerdir. Mesela 1974 doğumlu, Antalyalı bir internet kullanıcısının şifresini "antalya07" veya "antalya1974" olarak belirlemiş olma ihtimali rahatlıkla düşünülebilir.

Yakın zamanda yapılan bir araştırma, birçok internet kullanıcısının, internet ortamında '123456' gibi sıralı rakamların kullanıldığı şifrelerle internet aktivitelerini yürüttüğünü ortaya koymuştur. Unutulmamalıdır ki, sosyal ağların da gelişimine paralel olarak insanlar çok daha büyük bir siber dünyada birçok kişisel bilgisini (resimleri, videoları, kendi hakkında bilgileri, doğum yerini, doğum tarihini, okulunu, işini vs.) artık rahatlıkla doğrudan veya dolaylı yönden internette paylaşabilmektedir.

Nasıl mı?

Dayı ve dayıoğlunun Facebook'ta etiketlendiği varsayıldığında, kişinin 500 arkadaşı varsa, bu 500 arkadaşla da anne kızlık soyadının paylaşıldığı düşünülmelidir. Hatta Facebook'ta gizlilik ayarları yapılmadıysa tüm internet coğrafyasında bu bilgiler paylaşılmaktadır. Böylelikle, fazla çaba harcamadan bankacılık işlemlerinde kullanılan çok kritik bir bilgi olan anne kızlık soyadına ulaşılmış olacaktır. Üstelik doğrudan paylaşılmadığı düşünülen bir kişisel bilgiye ulaşılmıştır. İşte şifre tahmini de bu böyledir. Basit şifreler, internet ortamında, sosyal medyada paylaşılan birtakım kişisel bilgiler aracılığıyla tahmin edilebilmektedir. Tahmin edilmesi zor şifreler belirlense bile internette farklı hesaplar için aynı şifrelerin kullanılması büyük bir güvenlik açığına sebep olmaktadır. Çünkü bu şifrenin bir şekilde öğrenilmesi durumunda diğer hesapların da kötü amaçlı kişilerin eline geçmesi muhtemeldir.

ETİKETLER

#ŞifreGüvenliği