GİZLİ VE GÜVENLİ - GÜÇLÜ ŞİFRE

Dijital ortamda güvende tutmamız gereken bilgilerin ve bu bilgilere bir başkasının erişmesi durumunda ortaya çıkabilecek olumsuzluklardan dolayı birçok insan mağdur olmaktadır. Bu olumsuzluklara dolandırıcılık, hakaret, sahte evrak düzenleme, veri silme - kopyalama - hırsızlık, banka hesaplarına erişme gibi mağduriyetler olabilir. Kişisel bilgilerimizin bir başkası tarafından ele geçirilmemesi için şifre oluşturmanın çok önemli olduğunu, oluşturulacak şifrelerin güçlü ve tahmin edilemeyecek kadar zor olması gerekmektedir. Bu durumlarla karşılaşmamak belirli önlemlere e-posta kullanıcı adı ve şifresi oluşturulurken de dikkat edilmelidir. Kötü niyetli kişi veya kişilerin e-posta hesabımızı ele geçirmesi durumunda sizler adına başkaları ile iletişim kurabilecekleri ve arkadaşlarımızın güvenliğini tehlikeye atabilecekleri unutulmamalıdır.

Güçlü bir şifre oluşturmak için aşağıdaki adımlara dikkat edilmelidir.

1. En az 8 karakterden oluşmalıdır.
2. Basit bir kelimenin içindeki harfleri ve rakamları değiştirerek kullanabilirsiniz. (Örneğin B yerine 8 kullanılabilir.)
3. Şifre içerisinde büyük-küçük harf, rakam ve özel semboller olmalıdır.
4. Şifre belirlemeden önce unutulmayacak bir cümle oluşturularak şifre oluşturulabilir.
5. Sözlükten alınan bir sözcüğü direk olarak kullanmayın.
6. Hiçbir özel kimlik bilgisi kullanmayın. (TC No gibi)
7. Kolayca tahmin edilebilecek bilgileri kullanmayın. (Okul adı, sınıf no gibi…)

Güvenlikle ilgili önemli kurallar:

1. Parolanızı 6 ayda bir değiştirin.
2. Arkadaş listenizi ve bilgisayarınızı koruyun.
3. Başkasının bilgisayarında, internet kafede, okulda “Beni Hatırla” Seçeneğini kullanmayın.
4. Oturumunuzu kapatmayı unutmayın.
5. Başkaları tarafından şifrenizin kullanıldığını düşünüyorsanız, güvenli doğrulama seçenekleri ile şifrenizi değiştirin.

SİBER TUZAKLARI NASIL ANLARIM?

1. İnternette **kimlik bilgilerini** isteyen web sitelerine karşı **dikkatli ol**.
2. **Bedava** hediyelerden, programlardan ve **kazanacağını söyleyen yarışmalardan uzak dur.**
3. Eğlenceli gibi görünen testler, **senin hakkında bilgi toplamak** için hazırlanmış olabilir. **Bir kez daha düşün.**
4. Unutma! Bilinen markalar veya kurumlar e-posta yoluyla senden **parola, kimlik bilgileri gibi kişisel bilgiler istemez.**
5. Açılır pencerelerle **(pop-up)** gelen yarışma ve anketlere **katılma.**
6. **Şüpheli bulduğun e-postaların** içindeki bağlantıya (linke) tıklama ve gönderilen dosyayı **açma.**
7. **Tanımadığın kişilerden** gelen e-postaları açmadan önce, **tekrar düşün.**
8. **İçeriği arkadaşlarına da göndermeni isteyen e-postalar**, seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını **uyar.**
9. **İsteğin dışında** bilgisayar kameranın açılmaması için, kameranı **kontrol et.**
10. Oyun oynamak için, **üye olmanı isteyen siteleri** önce **dikkatlice incele.**