GİZLİLİK VE GÜVENLİK

Durum tespiti ve değerlendirmeler;

2019-2020 eğitim öğretim yılı itibariyle, internet etiği, telif hakkı açık erişim, bilişim suçları, bilgi güvenliği, bilgi yönetimi, bilgi kirliliği, zararlı yazılımlar, dijital yurttaşlık, siber tuzaklar, bilişim ile değişim, gizlilik ve güvenlik, dijital ayak izi, bilgi gizliliği, güçlü şifre gibi konular BTY dersi kapsamında daha ayrıntılı verilmeye başlanmıştır.

Öğrenciler, okul sitelerinde, kendi, arkadaşlarının, hatta ailelerinin sosyal medya hesaplarında, anlık mesajlaşma gruplarında tamamen ifşa olmuş durumdadırlar. Büyük veri, veri madenciliği gibi disiplinlerin geliştiği, manipülasyon, algı yönetimi için teknolojinin ayrı mecralar sunduğu günümüzde bu durum hem mahremiyet ve gizlilik, hem siber güvenlik açısından kaygı verici bulunmaktadır.

Öğrencilerin, velilerin hatta öğretmenlerin güvenlik konusunda gelinen nokta hakkında bilgi sahibi olmadıkları, günümüz teknolojilerini bilim kurgu filmi senaryosu gibi algıladıkları, farkındalığı nitekim yüksek olan küçük bir kesimin de ihmalkar davranış sergilediği gözlenmektedir.

MEB merkez teşkilatında güvenlik farkındalığı ve hassasiyetler nitekim yüksekken, taşra teşkilatına, okullara ve sınıflara inildikçe ihmallerin arttığı, erişimin kolaylaştığı, güven duygusunun da bu sebeple azaldığı, öğretmenlerin kendi kişisel bilgileri için bile endişe duydukları görülmektedir.

Genel olarak aile ve eğitimcilerde olduğu kadar öğrencilerde de, paylaşılan bilgilerin ne şekilde kullanılabileceği, nerede tutulduğu, güvenlikle ilgili ne önlemlerin alınması gerektiği, siber saldırılar gibi konularda önemli bilgi ve farkındalık eksiği bulunmaktadır. Ama mevcut sistemlerin, uygulamaların, sosyal medya platformlarının geniş yetki, izin ve bilgi talep etmesi çocukların ve gençlerin vazgeçilmez buldukları bu ortamları riskleri bile bile kullanmasına engel olmamaktadır.

Çocuklar arasında dijital oyunlarda başarılı olma, “hack”leme, şifre çalma, sisteme sızma yüksek prestij ve itibar görmektedir. Bu sebeplerle birbirlerinin şifrelerini kırma, oyun hesaplarını ele geçirme, zararlı yazılım iletme, çevrimiçi oyunlar için kredi kartı bilgileri paylaşılması gibi girişimler yaygın olarak gözlenmektedir. Ayrıca şifrelerini birbirleriyle paylaşma durumları bir samimiyet göstergesi oluşturmakta, paylaşılmaması durumları arkadaşlık ilişkilerini zedelemektedir.

200 milyondan fazla IoT cihazın şifre güvenliğini test etmek gibi önemli girişimlerde bulunan Japonya gibi ülkelerin uygulamaları dikkate alındığında, ülkemizde de bu gibi önlemlerin hayata geçirilmesi durumunda, okullarda gerekli eğitim, alt yapı ve farkındalık oluşturmadan kağıt üzerinde kalma ihtimali büyüktür.