

5.Sınıf Sosyal Bilgiler Konu Özetleri

4.Ünite : Bilim, Teknoloji ve Toplum
Konu : Sanal Ortamda Güvenlik

İnsanlar yüzyıllar boyunca hayatlarını kolaylaştırmak için çeşitli buluşlar yapmışlar ve bunları zamanla geliştirmişlerdir. Son yıllarda hayatımıza giren en önemli buluşlardan biri bilgisayar diğeri de akıllı telefonlardır. Genel Ağ teknolojisinin de devreye girmesiyle bilgisayarlar daha işlevsel hale gelmiştir. İnsanlar artık Genel Ağ bağlantılı bilgisayarları ve akıllı telefonları kullanarak bilgi edinmekte, mal ve hizmet satın almaktadır.

Sanal ortamı iyi niyetli insanlar kullanabildiği gibi kötü niyetli insanlar da kullanmaktadır. Bu nedenle sanal ortamda kullandığımız kişisel bilgileri korumak zorunluluk haline gelmiştir.

Mesafeli Alışveriş

Genel Ağ üzerinden alışveriş yapmak mesafeli alışveriş olarak adlandırılır. Dünyada her geçen yıl mesafeli alışveriş miktarı artmaktadır. Günümüzde insanlar fiziki olarak ürünlere dokunup satın almak yerine Genel Ağ üzerinden alışveriş sitelerine girerek istedikleri ürünü sipariş etme olanağına sahiptir. Sanal ortamda alışveriş yaparken kredi kartı, havale ve EFT gibi ödeme sistemleri kullanılır. Alışveriş yaptığımız sitelere ödeme esnasında aktardığımız kişisel bilgilerin kötü niyetli kişilerin eline geçmemesi gerekir. Az bilinen alışveriş sitelerinden ziyade herkesin sıklıkla kullandığı, bilinen sitelerden mesafeli alışveriş yapmak daha güvenlidir. Bu tür siteler kendi güvenlik sistemlerini oluşturdukları için kişisel bilgilerimiz daha güvende olacaktır. Kredi kartınızı mesafeli alışverişte kullanırken sizden aşağıdaki görsellerde verilen bilgiler istenecektir. Bu bilgileri gizli tutmanız güvenliğiniz açısından önemlidir. Kredi kartlarında yazılı olan bu bilgileri başkalarının görmemesi gerekir. Kredi kartı ile yapılan mesafeli alışverişlerde kullanıcı bilgileri güvenlik amacıyla bankaların sistemleri tarafından doğrulanır.



Kimlik Hırsızlığı

Genel Ağ'ın yaygınlaşmasıyla birlikte dikkat edilmesi gereken önemli konulardan biri de siber suçlardır. Siber suçların başında kimlik hırsızlığı ve dolandırıcılık gelmektedir. Genel Ağ'ı yanlış amaçlarla kullanan kişiler; insanların kredi kartı veya kimlik bilgilerine ulaşmakta, bu bilgilerle

sanal ortamda çeşitli işlemler yapmaktadır. Kişisel bilgilerinizi ele geçiren bu kişiler, adınıza sahte kredi kartları çıkarabilir ve bu kredi kartlarıyla alışveriş yapabilirler. Böyle durumlarla karşılaşmamak için tanımadığımız kişilerden gelen e-postaları açmamalı ve sosyal medya hesaplarında kişisel bilgilerimizi ayrıntılı bir şekilde paylaşmamalıyız.

Sanal ortamda kimlik hırsızlığı ve dolandırıcılıkla karşılaşmamak için almamız gereken tedbirlerden bazıları aşağıda verilmiştir:

- Sanal ortamda kullanılan şifrelerin tümünün birbirinin aynısı olmamasına özen gösterilmelidir.
- Şifrelerin kolay tahmin edilemeyen büyük ve küçük harf, rakam, noktalama işaretleri içermesine dikkat edilmelidir. Ardışık harf ve sayılardan oluşan ifadeler (abcd, 1234 gibi), doğum tarihi (2003 gibi) ve önemli olayların gerçekleştiği yılların tarihleri (1453, 1923 gibi) şifre olarak kullanılmamalıdır.
- Kredi kartını kaybeden bir kişi, hemen bankasının müşteri hizmetlerini aramalı ve kredi kartını iptal ettirmelidir.
- Sanal ortamda telefon numarası, aile bireylerinin adı, doğum yeri gibi kişisel bilgiler paylaşılmamalıdır.
- Telefonla arayan kişilere kendilerini nasıl tanıtırlarsa tanıtınsınlar kimlik ve kredi kartı bilgileri verilmemelidir. Değerli ürünlerin sanal ortamda bedava teklif edilmesine aldanılmamalıdır. Bu kişiler size bu ürünleri göndermek vaadiyle kişisel bilgilerinizi isteyebilir. Bu ve benzeri davranışları yapan kişiler hukuki yaptırımlarla karşılaşılır.

Güvenli Genel Ağ Kullanımı

Sanal ortama bağlanacağımız teknolojik aletlerde güvenlik önlemleri bulunmaktadır. Ancak Genel Ağ bağlantılı teknolojik aletleri kullanırken ek güvenlik önlemleri alınması gerekir. Çünkü Genel Ağ'a bağlanmak tüm dünyadaki Genel Ağ bağlantılı teknolojik aletlerle iletişim halinde olmak demektir. Bu esnada virüsler, Genel Ağ bağlantılı teknolojik aletlerimiz için önemli bir tehdit oluşturur. Virüsler, Genel Ağ bağlantılı teknolojik aletlerin olağan dışı çalışmasına, programlarının bozulmasına ve veri kaybına neden olabilen yazılımlardır. Bu yazılımlar, sanal ortamı kötü amaçlı kullanan kişiler tarafından Genel Ağ bağlantılı teknolojik aletlerimize genellikle e-posta ile gönderilir. Bu durumların önüne geçebilmek amacıyla anti-virüs programları geliştirilmiştir. Lisanslı anti-virüs programları yükleyerek Genel Ağ bağlantılı teknolojik aletlerimizi daha güvenli hale getirebiliriz.

- Teknolojik aletlerimizi, ekranında özel bilgilerimiz varken açık bırakmamalıyız.
- Teknolojik aletlerimizde kullandığımız yazılımların güncel olmasına özen göstermeliyiz.
- Virüsler taşınabilir USB bellekler tarafından teknolojik aletlere bulaşabilmektedir. Bu nedenle USB bellekleri kullanmadan önce virüs taramasından geçirmeliyiz.
- Bilgisayarımızdaki önemli verileri mutlaka yedeklemeli ve bunları güvenli bir ortamda saklamalıyız.

Günümüzde birçok Genel Ağ sitesi, bağlantı adreslerinde <https://> şifreleme sistemini kullanmaktadır. Bu şifreleme sistemi sayesinde Genel Ağ adreslerinde yaptığımız işlemlerin ve kişisel bilgilerimizin başkalarının eline geçmesi önlenir. Bağlantı adreslerinde <http://> olan Genel Ağ adreslerinin bilgi aktarım sisteminde herhangi bir şifreleme söz konusu değildir. Bu nedenle işlem yaptığımız sitelerin bağlantı adresinde "<https://>" ibaresinin bulunup

bulunmadığının kontrol edilmesi gerekir. Eđer baęlantı adreslerinde yalnızca http:// yazıyorsa bu sayfalar risk içermektedir.

SOSYAL Aę KULLANIMI

Sosyal aęlar üzerinden insanlar kendileriyle ilgili çeşitli bilgileri başkalarıyla paylaşmaktadır. Sosyal aęlardaki paylaşımlarımız günlük hayatımızı ve insanlarla olan ilişkilerimizi etkilemektedir. Bu nedenle sosyal aęları kullanırken önce güvenlięimizi düşünmeliyiz. Sanal ortamı başka insanlarla tanışmak için kullanmamalı, bu yolla gelen arkadaşlık tekliflerini reddetmeliyiz. Arkadaşlık teklifinde ısrarcı olan kişileri aile büyüklerimize bildirmeliyiz. Aile büyüklerimizin yaşanabilecek olumsuz durumlara karşı bizleri koruyacağını aklımızdan çıkarmamalıyız. Sosyal medyada video ve resim paylaşımlarında dikkatli olmalıyız. Paylaştığınız videolar ve resimler sizin ve yakınlarınızın zarar görmesine neden olabilir.

Sosyal aęları güvenli kullanmak için dikkat etmemiz gerekenler

- Sosyal paylaşım sitelerinde kayıt esnasında ve sonrasında kişisel bilgilerin tümü paylaşılmamalıdır.
- Gizlilik ayarlarına dikkat edilmeli, kişisel bilgi-leri herkesin görmesi engellenmelidir.
- Paylaşılan video ve fotoęrafların kötü amaçlı kullanılabileceęi unutulmamalıdır.
- Kullanıcıların ilgisini çeken "Kazandınız" ve "Bedava" gibi mesajlara karşı dikkatli olunmalıdır.

Sosyal aęlarda paylaşmamamız gereken kişisel bilgiler

- Doğum tarihinizin gün ve ay kısmı
- Doğum yeriniz
- Anne kızlık soyadınız
- Ev, iş ve okul adresiniz
- Telefon ve T.C. kimlik numaranız