BİLİŞİM SUÇLARI

Bilişim suçu en basit tanımıyla bilişim sistemlerine karşı işlenen suçlardır. Bir bilişim sistemine hukuka aykırı girmek, bilişim sisteminden izinsiz veri kopyalamak, sistemi erişilmez kılmak veya çalışmaz hale getirmek bilişim suçlarını oluşturmaktadır. Türkiye'de bu tür suçlar ile mücadele 2007 yılındaçıkartılan **5651** sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluylaişlenen suçlarla mücadele edilmesi hakkında kanun" uyarınca yapılmaktadır.

Sık Karşılaşılan Bilişim Suçları

- **Dolandırıcılık:** Kredi kartı bilgilerini internet ortamında veya telefonla arayarak, e-posta atarak vb. çalarak haksız kazanç elde etmek, banka veya kredi kartlarının kötüye kullanılması. Banka ve kredi kartları, ATM cihazlarında, bazı iş yerlerinde ve online alış-veriş sitelerinde kopyalanabilmektedir. Kart bilgisi ele geçirilerek veya kopyalanıp kişinin hesabından alışveriş yoluyla para çekilebilmektedir. Yine bilgisayarlara bulaştırılan virüsler aracılığı ile kişilerin İnternet bankacılığı hesapları ve şifreleri ele geçirilebilmektedir ve bu hesaptaki paralar dolandırıcıların kendi hesaplarına aktarılmaktadır. İnternet bankacılığını kullanırken oldukça dikkatli olunmalıdır. Titan zincirleri de dolandırıcılık kapsamındadır.
- **Siber Saldırı:** Web sitelerini “hack”lemek, virüs, trojan ve zararlı yazılım (malware) yazıp ve yayılmasını sağlayarak;başkalarına ait kullanıcı adı, şifre, parola, fotoğraf gibi özel bilgileri ele geçirmek ve bu bilgileri kullanmak da bilişim suçları kapsamındadır. Hukuka aykırı olarak bir bilişim sistemine girme, verileri yok etme, bozma veya değiştirme, bilgisayar sistemlerini hizmet veremeyecek şekilde engellemek bilişim suçudur.

- **Saldırganlık:** Irkçılığı, küfür ve hakareti, politik olarak zarar verici, karalayıcı veya iftira edici, kışkırtıcı veya nefret suçlarını alevlendirici içerikler yaymak.
- **Müstehcenlik:** Uygunsuz içerikleri indirmek veya yayınlamak.
- **Hakaret, Şantaj:** Sanal ortamda yazışma, görüntülü veya sesli görüşme yoluyla karşıdaki kişiye hakaret etmek, şantajda bulunmak. Günümüzde sosyal medya kullanımının yoğun olmasıyla birlikte sosyal medya üzerinde yapılan paylaşımlarda ve yazılan yorumlarda hakaret edici, küçük düşürücü içeriklerin yer almamasına özen gösterilmelidir. Sosyal medya üzerinden bilişim suçları eskiye nazaran daha yoğun biçimde denetlenmektedir.**Siber Zorbalık**
- **Terörizm:** Herhangi bir terör örgütünün sanal ortamda destekçisi olunması. Devletin bilişim sistemlerine saldırı ve gizli bilgilerini açığı çıkarmak da terörizm kapsamındadır.
- **Kumar:** Devletin yasakladığı biçimde İnternet ortamında kumar oynamak veya oynatmak.
- **Telif Haklarının İhlali:** Korsan yazılım kullanmak, film-oyun-müzik CD 'si çoğaltmak.

Bilgisayar ve İnternet Güvenliği için Gerekenler

1. **GüvenlikDuvarıAçıkOlmalıdır**

Güvenlik duvarı (Firewall) internet üzerinden sizin bilginiz dışında bilgisayarınıza erişilmesini engellemek üzere kullanılan bir yazılım ya da donanımdır. Güvenlik duvarı başlangıçtainternet bağlantısı dahil tüm giriş çıkışı engeller, siz yazılımları kullandıkça size hangi yazılımlara ne kadar erişim hakkı vereceğinizi sorar.

2. **Gerekli Şifreler Doğru Şekilde Oluşturulmalıdır.**

Kişisel şifreleriniz büyük küçük harfler, özel karakterler ve sayılar kullanılarak oluşturulmalıdır.

- Şifrenizdekişiselbilgilerinizeyervermeyin.
- Şifrenizdeardışıksayılarharflerkullanmayın.
- Yanyanabulunantuşlarıkullanmayın.
- Şifrenizenaz8basamaklıolsun.
- Şifre oluştururken Büyük/Küçük Harfler, Rakamlar, Noktalama İşaretleri, Özel Karakterleri kullanın. Bilgisayar = 8iLg15@y@R

3. **Bilgisayarda anti-virüs yüklü olmalıdır.**
4. **Gerekligüncellemelerveayarlamalaryapılmalıdır.**

https://www.security.org/how-secure-is-my-password/