T.C. Sağlık Bakanlığı	GİRESUN İL SAĞLIK MÜDÜRLÜĞÜ SOSYAL MÜHENDİSLİK ZAAFİYETLERİ VE SOSYAL MEDYA GÜVENLİĞİ			T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü
Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01				1/1

Amaç;

Giresun İl Sağlık Müdürlüğü ve bağlı teşekküllerde çalışan Bilgisayar kullanıcılarının sosyal medyayı kullanırken uymaları gereken prosedürler konusunda bilinçlendirmektir.

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

1. Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

2. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

2.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.

2.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.

2.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

2.4. Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız.

2.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.

2.6. Oluşturulan dosyaya erişecek kişiler ve haklarını, "bilmesi gereken" prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.

2.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

2.8. Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırma makinesinde imha ediniz.

2.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.

2.10. Bilgisayarınızı yabancı bir kişiye kullandırmayınız. USB ya da harici bir disk bilgisayarınıza zararlı yazılım bulaştırabilir.

2.11. Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

3. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler şu şekilde sıralanabilir:

3.1. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyası, barkodlar, gözlem formları vs.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.

3.2. Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz.

3.3. Hasta dosyaları ilgili doktor ve hemşire dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.

3.4. SBYS programlarında kullanılan parolalar kimseyle paylaşılmaz.

4. Kişisel Sosyal Medya Güvenliği

4.1. Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalardan farklı seçilir.

4.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

4.3. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

4.4. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Celal KÖSE Bilgi Güvenliği Yetkilisi	Kamil AKTAŞ Bilgi İşlem Sorumlusu-Uzman	Mehmet ŞAHİN Personel ve Destek Hizmetleri Başkanı