Son zamanlarda siber saldırılar artmış durumdadır. Siber saldırı yöntemleri ve alınması gereken tedbirler aşağıda belirtilmiş olup personelimizin dikkatine sunulur.

Oltalama E-Postaları: *Genellikle içerisinde kullanıcıların ilgisini çekebilecek bilgiler bulunmaktadır. Mail başlığı "Kurumdan uzaklaştırılanların listesi", "İzinlerin iptali ile ilgili", "Kurumdaki telefon değişiklikleri" vb. şeklinde olabilmektedir. Mail içeriğinde ya bir bağlantı ya da ekli bir dosya bulunmaktadır. Bu tarz saldırılar kullanıcının tanıdığı kişiye ait bir e-posta adresinden de geliyormuş gibi gözükebilir. Söz konusu e-posta içerisinde bağlantı veya ekli dosya bulunan e-postalar beklemiyor veya konuyu farklı buluyorsanız bu tür mailleri açmayınız.*

Sosyal Medya Hesapları: *Özellikle iş kimliğinizi yönetmek ve paylaşmak için kullanılan (linkedin) sosyal medya hesaplarınızdan, yaptığınız paylaşımlardan veya internet üzerindeki web sitelerini tarayarak saldırganlar sizin hakkınızda detaylı bilgi edinebilir. Bu bilgiler sizinle iletişime geçmek veya zararlı yazılım göndermek için kullanılabilmektedir.*

Basit Parola Kullanımı: *Kurum e-postalarınızda, sosyal medya hesaplarınızda, kişisel e-posta adresleriniz de vb. 10 karakterden az parola kullanmayınız. Parolanızın içinde ez bir büyük harf, küçük harf, rakam, noktalama işareti bulunmalıdır. Parolanız ard arda sıralı karakterler içermemelidir. Saldırganlar siz farkında olmadan büyük bir liste kullanarak sizin parolanızı deneme yanılma yaparak bulmaya çalışıyor olabilirler. Bu yüzden her sistem izin farklı ve güvenilir parola kullanmanız gereklidir.*

Telefon: *Telefonla arayıp sizden bilgi isteyen (e-posta, parola, isim vb.) kişilerin doğru olduğundan emin olunuz. Özellikle şüpheniz varsa arayan kişinin kurum telefonuna internetten ulaşıp geri arayabilirsiniz.*

Flash Bellek: *Saldırganlar tarafından içerisine zararlı yazılım yükledikleri flash bellekleri bulunduğunuz ortama rastgele bırakabilirler. Başka yerde kullandığınız belleklerin içerisine zararlı yazılım bulaşmış olabilir. Kime ait olduğunu bilmediğiniz bellekleri kesinlikle bilgisayarınıza takmayınız ve güvenilmeyen bilgisayarlarda kullanılan flash bellekleri kurum bilgisayarlarında kullanmayınız.*

Mobil Güvenlik: *Bilinmeyen ağlara bağlanılması, bilinmeyen yazılım kurulması, kurulurken gereksiz izinlerin verilmesi, farklı yazılımlar (jailbreak) ile cihaza değiştirilmiş mobil işletim sistemleri kurulması büyük risk taşımaktadır. Eğer mobil cihazınızın güvenliğinden şüphe duyuyorsanız kurumsal ağlara bağlanmamanız, e-postalarınızı güvenilmeyen mobil cihazlardan takip etmemeniz, kişisel önemli işlerinizi (banka, ödeme) mobil cihazlarınızdan yapmamanız önemle tavsiye olunur.*

Antivirüs Yazılımları: *Antivirüs yazılımları yüzde yüz bir siber güvenlik sağlamaz. Kurum bilgisayarlarınızdan güvenilmeyen sitelere (dizi, film, warez, torent vb.) girilmesi büyük risk oluşturmaktadır. Bu sitelerdeki reklamlar, sitelerin içerisinde bulunabilecek zararlı kodlar sisteminize zararlı yazılım bulaştırıp, saldırganlar tarafından para elde etmek, reklam yayınlamak veya bilgi toplama amaçlı kullanılabilir. Bir zararlı yazılım bulaştıktan sonra bunun anlaşılması teknik bilgi olmadan çok zor olabilir. Eğer sisteminizde bir anomali (rastgele sayfa açılması, farklı sistemlere bağlantılar, yavaşlık) varsa lütfen zararlı yazılım bulaşma ihtimalini göz önünde bulundurun.*

Tüm personelimiz aşağıdaki hususları yerine getirmelidir.

- *Bilgisayarlarını güncel tutmaları, mutlaka antivirüs yazılımı kurmaları gerekmektedir. Üniversitemiz için lisanslı Kaspersky Antivirüs yazılımı tüm kurum bilgisayarlarında kurulu olmalıdır.*

- *Kurum bünyesinde mevcut kullanıcıların bilgisayarları ajan yazılımlar ile zombi bilgisayar haline gelebilmektedir. Zombi bilgisayarlarda internet üzerinden çeşitli komutlar ile faaliyete geçerek başka bilgisayarlara saldırı amaçlı kullanılmaktadır. Bu sebeple mesai sonrası ve hafta sonu bilgisayarların kapatılması önem arz etmektedir.*

- *Kritik görev icra eden kamu kurum ve kuruluş personelinin çalışma ortamlarında veya görevi sırasında yanında bulundurduğu akıllı cihazın görevin gizliliğini tehlikeye düşüreceği bilinciyle hareket etmesi gerekmektedir.*

- *Kurum mahremiyetini içeren görüşme ve yazışmaların anlık mesajlaşma uygulamaları (whatsapp, viber vb.) üzerinden yapılmamasına önem gösterilmelidir.*

- *Akıllı cihazlar üzerinde kurulacak uygulamalar için verilecek izinlerin incelenerek onaylanması, gereksiz izinlerin verilmesi istenen programların yüklenmemesine dikkat edilmelidir.*

- *Bilgisayar ve akıllı telefonlara kurulacak olan uygulamaların her uygulamanın resmi uygulama sağlayıcılarından indirilip yapılması gerektiği unutulmamalıdır.*