SİBER GÜVENLİK FARKINDALIK AYI GÖRÜŞ VE ÖNERİLERİ

Dünya çapında her yıl Ekim ayında, "Siber Güvenlik Farkındalık Ayı" kapsamında çeşitli etkinlikler düzenlenmektedir. Ülkemizin 2020-2023 Ulusal Siber Güvenlik Stratejisi'nde siber güvenlik farkındalığının artırılmasına yönelik olarak kurum ve kuruluşlarda, kurumsal bilgi güvenliği kültürünün yerleşmesi hedeflenmektedir. Belirtilen bu hedefler kapsamında Kurumumuzda; üst yönetici, akademik/idari personel ve öğrenci düzeyinde siber güvenlik farkındalığını sağlamak amacıyla uyarı ve önerileri içeren web sayfası duyuruları ve kurumsal adreslerine gönderilen mailler aracılığıyla ara ara paylaşılmaktadır. Bu paylaşımlarla, Üniversitemiz bünyesindeki akademik/idari personellerimiz ve öğrencilerimizin güvenli çevrimiçi davranış alışkanlıkları kazanarak sağlıklı internet kullanımının sağlanması ile siber güvenlik alanında farkındalığının artırılması amaçlanmaktadır. Kurumumuzun tüm paydaşlarında siber güvenlik kültürünün yerleşmesi, yüksek düzeyde siber güvenlik farkındalığının sağlanmasına dayanmaktadır. Siber saldırılara karşı daha güvenli ve korumalı bir kurum olabilmemiz, risk ve tehditlerin olumsuz etkilerini minimumda tutabilmek, teknoloji ve bilişim cihazlarının güvenli kullanımının önemi tüm kullanıcılar tarafından benimsendiğinde mümkün olacaktır.

A- Teknoloji ve Bilişim Cihazlarının Güvenli Olarak Kullanılabilmesi için Alınması Gereken Önlemler;

- ✓ Cihazlarınızdaki işletim sistemi, güvenlik yazılımı, kullanılan temel uygulamaların en son yayınlanan güncel sürüme sahip olması, cihaz yazılımlarının otomatik güncelleme seçeneğinin açık tutulması,
- ✓ Size özel olan kurum bilgisayarları, mobil ve diğer web tabanlı cihazlarınızda mutlaka güvenlik parolası oluşturulmalı ve bu cihazlar hiçbir zaman parolasız kullanılmamalı,
- ✓ Cihazlarınıza USB bağlantı noktası veya diğer yöntemlerle harici olarak bağlanan aygıtlar, virüs taraması yapılmadan kesinlikle kullanılmamalı,
- ✓ Cihazlarınızda internette dolaşırken karşınıza gelen bir pop-up ekranında veya e-postalarınıza gelen şüpheli mail içeriklerindeki linkler, bağlantı adresleri ya da belirtilen hiçbir butona tıklanmamalı, mesaj mail içeriği derhal silinmeli, şüphe uyandıran ancak beklenen bir mail içeriğinde ise bağlantı adresi farklı bir tarayıcının adres satırına yeniden yazılarak doğrulanmalı,
- ✓ Değerli olan çalışma dosyalarınızı, fotoğraflarınızı, dijital arşiv verilerinizi belirli periyotlarda mutlaka yedeklerini almalısınız.
- ✓ Hem kendiniz hem de diğer kişiler ile ilgili değerli bilgileri internet ortamında yapacağınız paylaşımlarınızı kimlerin görebileceğini, şimdi ve gelecekte nasıl kullanabileceğini biliyor olmalısınız.
- ✓ Kablosuz yayın yaparken (Hotspot, Tethering) cihazınıza erişebilecek diğer cihaz ve kişileri sınırlandırmak ve yönetmek için cihazınızın güvenlik ve gizlilik ayarları mutlaka sizin kontrolünüzde olmalı,
- ✓ Mümkünse ortak kablosuz ağlar kullanılmamalı, zorunlu ihtiyaçlarda ise erişim sağladığınız web adreslerindeki "https" ifadesine dikkat etmelisiniz.
- ✓ Bilişim cihazlarında kullanılan giriş güvenlik anahtarlarının, hesap şifrelerinin güçlü parolalardan oluşturulması siber bilgi güvenliği açısından son derece önemlidir. Kolay çözülebilir basit oluşturulan parolalar hem bireysel cihazlarımızda hem de kullanılan kurum ağı cihazlarında güvenlik açığı oluşturacaktır. Bunun gibi durumları önlemek için aşağıda belirtilen kurallar dikkate alınmalıdır.

1- Parolalar en az bir büyük harf, bir küçük harf, bir rakam ve bir özel karakter içermeli ve en az 8 karakter uzunluğunda olmalı,
2- Şifreler oluşturulurken; 123456, abcdef gibi kolayca kırılabilecek karakterler belirlenmemeli, çocuğunuzun doğum tarihi, ad-soyad gibi kişisel bilgilerinizi de içermemeli,
3- Bütün hesapların oturum açma adımında şifreler her seferinde yeniden girilmeli, beni anımsa seçeneği mümkün olduğu sürece kullanılmamalı,
4- Parolalar en az 6 ayda bir değiştirilmeli, her bir farklı hesap için ayrı ayrı şifreler belirlenmeli,
5- Kullanıcılar hiçbir parolasını diğer kişilerle paylaşmamalı, paylaşırsa doğacak bütün hukuki sorumluluğun kendinde olduğunun bilincinde olmalı,

6- Parolaları sadece size çağrışım yapacak şekilde oluşturabilirsiniz, kolay bulunacak herhangi bir yere not edilmemeli, not edilerek saklanacak ise de mutlaka şifreli/kodlamalı şekilde saklanmalı,
7- Herkese açık olan bilgisayarlara tüm vuruşlarınızı yakalayan "keylogger" casus yazılımı bulaşmış olabilir. Bu bilgisayarlarda hesaplarınızla oturum açılmamalı, yalnızca kontrol ettiğiniz güvenilir bilgisayarlarda veya mobil cihazlarda korunan hesaplarda oturum açmalısınız.

B- Bilişim Cihazları Üzerinden Yapılan Siber Saldırılar ile ilgili Yöntem ve Açıklamalar;

1- Oltalama ve Kimlik Avı

Kimlik avı/oltalama saldırıları bilinen bir kaynaktan geliyormuş gibi görünen sahte iletişim gönderme yöntemidir. Genellikle e-posta yoluyla yapılır. Kimlik avı e-postalarının çoğu rastgele olarak çok sayıda alıcıya gönderilir. Amaç kredi kartı ve şifre bilgileri gibi hassas verileri çalmak veya cihaza kötü amaçlı yazılım yüklemektir. Kimlik avı/oltalama e-postaların içeriklerinde; herkese açık e-posta alanları, yanlış yazılmış alan adları, kötü dilbilgisi ve imla hataları, şüpheli ekler/bağlantılar ve aciliyet duygusu uyandıran durumlara çok dikkat etmek gerekir.

2- Mobil Cihazınızın Güvenliği

Bilgisayarlarınızı nasıl koruma altına alıp güvende tutuyorsanız aynı hassasiyeti mobil cihazlarınız içinde göstermelisiniz. Mobil cihazlarınızda bilgisayarlardan daha çok kişisel veriler içeren hassas bilgiler tutulmaktadır. Cihazlarınızı daima güçlü şifreler, parmak izi, ekran kilidi, desen ya da yüz tanıma ile güçlendirin. Mobil cihazlar kaybolabilir, çalınabilir ya da bir yerde unutulabilir olduğu için imkanlar ölçüsünde uzaktan silme işlemi ile değerli kişisel bilgilerinizi silip, cihazınızı fabrika ayarlarına getirebilirsiniz. Mobil cihazlarınıza mutlaka güvenilir kaynaklardan uygulama yüklenmelidir. Yüklenmek istenen uygulama iyi araştırılmalı, olumsuz yorumlara dikkat edilmeli, çok fazla veriye erişim izni isteniyorsa o uygulama ya yüklenmemeli ya da daha az veriye erişim izni isteyen uygulama bulunmalıdır. Mobil cihazlarında yazılımları güncel tutulmalı, güvenlik uygulamaları kullanılmalı, herkese açık kablosuz ağlar mümkün olduğunca kullanılmamalı, kablosuz bağlantı (Wi-Fi, Bluetooth, NFC, temassız ödeme vb.) ayarlarını her zaman pasif/kapalı konumda tutulmalı, ihtiyaç halinde aktif/açık edilerek kullanılmalıdır.

3- Sosyal Mühendislik

Sosyal mühendislik, Bilgi güvenliği kapsamında eylemleri gerçekleştirmeye veya kişisel bilgilerinizi ifşa etmeye yönelik olarak insanların psikolojik manipülasyonudur. Günümüzde en yaygın yöntemler arasında değerlendirilen sosyal mühendislik saldırıları zorlama, aldatıcı ilişkiler kurma ve geliştirme, dürüstlüğü, sorumluluğu, etik değerleri manipüle eden, güvenlik prosedürlerini veya politikalarının atlanmasını talep eden, acele etme hissiyatı yaratan yöntemler kullanılarak kişisel olan değerli verilerinizi almak için yapılan dolandırma işlemleridir. Bu tip işlemlere maruz kaldığımızda işlemi iptal edin, mesajı silin, maili silin, sayfanızı kapatın.

Bu saldırılardan kendimizi korumak için alınması gereken önlemler;

1- Kişisel/özel bilgilerinizi paylaşmayın,
2- Parolalarınızı paylaşmayın,
3- Sizinle iletişim kuran kişileri araştırın,
4- Adres/URL kontrolü yapın,
5- Güvenilir olmayan kaynaklara dikkat edin,

4- Güvenli Tarayıcı Kullanmak

İnternet üzerinden işlemlerimizi bir web tarayıcısı aracılığıyla yapmaktayız. Tarayıcılarımızın sürümlerinin güncel versiyonlarında kullanılmasına dikkat edilmelidir. Web tarayıcınız bağlantı kurmak istediğiniz sayfayı engelliyorsa o web sayfası kapatılmalı, ulaşılmak istenen bilgiye güvenli olan başka adresler üzerinden erişilmelidir. Web adresi satırlarında "https" güvenli sayfa ibaresi veya (🔒) asma kilit simgesi olmasına mutlaka dikkat edilmelidir. Tarayıcıların işlevselliğini artırmak için güvenli eklentiler/uzantılar kullanılabilir. Kullanılması zorunlu olan eklentilerinde en son sürümü kullanılmalıdır. Tarayıcı uzantılarının istediği izinlere dikkat edilmelidir. Artık ihtiyaç duyulmayan eklentiler/uzantılar tarayıcıdan kaldırılmalıdır.

5- Sosyal Paylaşım Siteleri

Sosyal medya, çevremizle irtibat kurabildiğimiz bilgi alışverişinde bulunulabilen sosyal ortamlardır. Ancak sosyal ağlar yeteri kadar güvenli ve bilinçli kullanılmadığı için siber saldırganların hedefi olmaktadır. İnternet kullanımının her adımında güvenli şifre yetkilendirme ne kadar önemli ise sosyal medya hesaplarının da parolalarının şifrelerinin diğer hesaplardan farklı, benzersiz, güçlü olması gerekir. Mümkünse iki adımlı doğrulama (two-factor authentication) tercih edilmelidir. Sosyal mühendislik saldırılarından korunma adımlarında olduğu gibi burada da aynı önlemler dikkate alınmalıdır. Paylaştığınız bilgi/belge vb. içerikleri istemediğiniz kişilerin/grupların erişimine kapalı tutmalısınız. Kişisel verilerinizin paylaşılması konusunda çok dikkatli olunması gereken sosyal medya mecralarında başka bir kişiye, kuruma ait herhangi bir veri, gizli bilgide paylaşılmamalıdır. Sosyal medya üzerinden de yüklenen uygulamalar mutlaka sizin kontrolünüzde kullanılmalı, ihtiyaç duyulmayan uygulamalar kaldırılmalı ya da sosyal medya hesabınıza erişim yetkisi devre dışı bırakılmalıdır. Aynı oltalama saldırılarında olduğu gibi sosyal medya üzerinden de kişiler kandırılmaya müsaittir. Şüpheli bir eylem ile karşı karşıya kalındığında diğer kanallardan işlem mutlaka teyit edilmeli ya da o eylem hiç dikkate alınmadan yok sayılmalıdır.

Ordu Üniversitesi Rektörlüğü