BİREYSEL
SİBER GÜVENLİK
ÖNLEMLERİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

USOM
ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

Hızla ilerleyen teknoloji, günlük yaşamımızın her alanında ayrılmaz bir parça haline gelmektedir. Henüz cep telefonu ile tanışmamızın üzerinden çok geçmemesine rağmen, artık birçok evde robot süpürgeler, internet üzerinden yönetilebilen beyaz eşyalar bulunmaktadır. Hatta evler akıllı olarak inşa edilmekte, sesli komutla işlemler yapılabilmektedir. Otonom sürüş yapabilen araçlar geliştirilmiş ve yollarda görülmektedir. Yakın tarihte havadan çekim yapabilmek için uçak veya helikopter kullanılırken artık yaygınlıkta drone'lar bulunmaktadır. Sosyal medya kullanımının çok yaygın hale gelmesi bilgi paylaşımını farklı bir boyuta taşımaktadır.

Teknolojinin daha erişilebilir hale gelmesiyle birlikte siber güvenlik tehditlerinin risk faktörü de artmaya devam etmektedir. Amaçlarına erişmek için her yöntemi deneyen siber saldırganlardan korunmak için, teknoloji kullanıcısı her birey tarafından alınması gereken tedbirler başlıca şunlardır;

01 **Güçlü parola kullanın:** Türkiye İstatistik Kurumunun 2022 yılında yayınladığı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre, ülkemizde internet kullanım oranı 16-74 yaş grubundakilerde %85 olarak kaydedilmiştir. Bu oranın artmasıyla birlikte siber güvenlik riskleri de artmaktadır. Bu nedenle, güçlü parola kullanımı kişisel verilerinizi korumanız için önemlidir. Parolanız ne kadar karmaşık ve uzun olursa, o kadar güçlü olur. Parolanızda büyük harf, küçük harf, sayı ve sembol kullanmanız önerilir. Ayrıca, parolanızı düzenli olarak değiştirmeniz güvenlik seviyesini arttırır.

02 **İki faktörlü kimlik doğrulama kullanın:** İki faktörlü kimlik doğrulama, kullanıcıların sahip oldukları kimliklerini iki farklı faktörün kombinasyonunu kullanarak onaylama yöntemidir. Bu yöntem, kullanıcının yalnızca bir faktör (genellikle bir parola veya geçiş kodu) sağladığı tek faktörlü kimlik doğrulamaya bağlı olan kimlik doğrulama yöntemlerinden daha yüksek bir güvenlik düzeyi sağlar. Türkiye'de parola kullanımı istatistikleri incelendiğinde, 2021 yılında Türkiye'de internet kullanıcılarının % 60'ının parolalarını değiştirmediği ve % 30'unun parolalarını yalnızca bir kez değiştirdiği görülmektedir. Bu nedenle, destekleyen uygulamalarda ve platformlarda iki faktörlü kimlik doğrulama kullanımı, internet kullanıcılarının hesaplarını daha güvenli hale getirmek için önerilmektedir.

03 **Güncel antivirüs ve güvenlik yazılımı kullanın:** Güncel antivirüs ve güvenlik yazılımı kullanmanın önemi, bilgisayar ve diğer cihazlarda kötü amaçlı yazılımların tespit edilmesi ve engellenmesi için hayati bir rol oynar. İstatistiklere göre, her gün binlerce yeni kötü amaçlı yazılım tespit edilmekte ve yayılmaktadır. Bu yazılımlar, kişisel bilgilerinizi çalmak, cihazlarınızı kilitlemek veya verilerinizi şifrelemek gibi zararlı faaliyetlerde bulunabilir. Güncel antivirüs ve güvenlik yazılımları, bilinen virüslerin ve diğer kötü amaçlı yazılımların tespitini sağlar ve güvenlik tehditlerine karşı koruma sağlar. Ayrıca, güncel yazılım sürümleri, yeni tehditlere karşı savunma sağlamak için düzenli olarak güncellenir ve geliştirilir. Bu nedenle, güncel antivirüs ve güvenlik yazılımı kullanmak, bilgisayarınızı ve kişisel verilerinizi korumak için önemli bir adımdır.

04 **İşletim sistemlerinizi ve uygulamalarınızı güncel tutun:** İşletim sistemlerinizi ve uygulamalarınızı güncel tutmak, güvenlik açıklarını gidermenin ve bilgisayarınızı siber saldırılara karşı korumanın en etkili yöntemlerinden birisidir. Güncellemeler, geliştiricilerin tespit ettikleri güvenlik zafiyetlerini düzeltmek ve yeni tehditlere karşı koruma sağlamak için yayınladıkları yazılım düzeltmeleridir. İstatistikler, birçok siber saldırının, güncellemeleri yapılmamış işletim sistemleri ve uygulamalar aracılığıyla gerçekleştiğini göstermektedir. Bu nedenle, güncellemeleri ihmal etmek, saldırganların bilgisayarınıza erişim sağlamasını kolaylaştırabilir. Ayrıca, eski sürümler, bilgisayarınızın performansını ve uyumluluğunu da etkileyebilir. Bu nedenle, düzenli olarak güncelleme kontrolleri yaparak işletim sistemlerinizi ve uygulamalarınızı güncel tutmanız, bilgisayarınızın güvenliğini sağlamanın önemli bir adımıdır.

05 **Düzenli yedekleme yapın:** Düzenli yedekleme yapmanın önemi büyüktür, çünkü verilerinizin kaybı durumunda önemli bilgilerinizi kurtarmanızı sağlar. Bilgisayar kırılması, donanım arızası veya başka bir nedenle veri kaybı yaşanabilir. Yedekleme, verilerinizi güvende tutmak ve kritik bilgilerinizi korumak için önemli bir adımdır. Düzenli yedekleme yaparak, önemli dosyalarınızı koruma altına alır ve veri kaybı durumunda sorun yaşamadan geri dönüş yapabilirsiniz.

06 **Güvenilir ve güncel bir tarayıcı kullanın:** Güvenilir ve güncel bir tarayıcı kullanmak, internet güvenliği açısından kritik bir faktördür. Güvenilir bir tarayıcı, güvenlik önlemleriyle donatılmış ve kötü niyetli yazılımları engelleyebilecek özelliklere sahip olmalıdır. Güncel tarayıcılar, yeni güvenlik güncellemelerini içerir ve bilinen güvenlik açıklarına karşı koruma sağlar. Ayrıca, güncel tarayıcılar, web standartlarına uyumlu olarak geliştirilen siteleri daha iyi görüntüleyebilir ve daha iyi performans sağlayabilir. Tarayıcıların güncel sürümlerinin kullanılması, çeşitli zararlı yazılımların (virüsler, truva atları, fidye yazılımları, vb.) ve kimlik avı saldırılarının engellenmesine yardımcı olur. Ek olarak, güvenilir tarayıcılar, kullanıcıları zararlı web sitelerine yönlendiren veya kişisel bilgilerini çalmaya çalışan sahte siteleri tanıyabilir. Bu nedenle, internet kullanıcıları güvenilir ve güncel bir tarayıcı kullanarak çevrimiçi güvenliklerini artırabilirler.

07 **Güvenli bir Wi-Fi ağı kullanın:** Güvenli bir Wi-Fi ağı kullanmak, internet bağlantınızın güvenliğini ve kişisel verilerinizi korumanın önemli bir adımıdır. Birçok insanın evlerinde veya halka açık alanlarda kullandığı Wi-Fi ağları, potansiyel güvenlik riskleri taşır. Güvenli bir Wi-Fi ağı kullanmak, başkalarının ağınıza izinsiz erişmesini ve veri hırsızlığını önler. Bunun için Wi-Fi ağınızı şifreleyerek ve varsayılan ayarlarını değiştirerek güvenlik önlemlerini artırabilirsiniz. Ayrıca, Wi-Fi ağınıza güçlü bir parola belirlemek de önemlidir. Ağınızı gizli tutmak, yani SSID yayınını kapatmak da güvenliği artıran bir adımdır. Halka açık Wi-Fi ağlarında gezinirken dikkatli olunmalı, hassas bilgilerinizi (banka bilgileri, parolalar) bu tür ağlar üzerinden paylaşmaktan kaçınılmalıdır. Güvenli bir Wi-Fi ağı kullanmak, siber saldırılardan ve veri sızıntılarından korunmanızı sağlar ve internet deneyiminizi güvenli hale getirir.

08 **Bilinmeyen e-posta eklerini açmayın:** E-posta, günümüzde iletişimde sıkça kullanılan bir araçtır ancak bilinçsizce açılan e-posta ekleri büyük bir siber güvenlik riski oluşturabilir. Bilinmeyen veya güvenilmeyen kaynaklardan gelen e-posta eklerinin açılması, kötü niyetli yazılımların bilgisayarlara bulaşmasına ve hassas verilerin çalınmasına yol açabilir. İstatistikler, oltalama saldırılarının ve zararlı eklerin e-posta yoluyla yayılmasının hala yaygın bir yöntem olduğunu göstermektedir. Bir e-postanın güvenilirliğini doğrulamadan, tanımadığınız veya beklenmeyen bir e-posta ekini açmaktan kaçınmalısınız. Bu önlem, kişisel bilgilerinizin ve cihazlarınızın güvende kalmasını sağlar ve siber saldırılara karşı korunmanıza yardımcı olur. Eğer şüpheli bir e-posta alırsanız, dikkatlice inceleyin, e-postanın kaynağını kontrol edin ve güvenli olduğundan emin olmadığınız sürece eklerini açmamaya özen gösterin.

09 **Sahte internet sitelerinden kaçının:** İnternet üzerindeki sahte siteler, gerçek sitelerin taklitleridir ve kullanıcıların kişisel bilgilerini ele geçirmek veya dolandırıcılık amacıyla kullanılırlar. Araştırmalar, oltalama saldırılarının siber saldırganlar tarafından kullanılan en yaygın yöntemlerden biri olduğunu göstermektedir. Sahte siteler genellikle e-posta veya sosyal medya gibi kanallar aracılığıyla kullanıcılara ulaşır ve güvendikleri sitelerin kopyalarını oluşturarak onları kandırır. Bu nedenle, kullanıcılar herhangi bir şüpheli e-posta veya bağlantıya tıklamadan önce URL'yi doğrulamalı ve bilgilerini paylaşmadan önce sitenin güvenilir olduğundan emin olmalıdır. İyi bir yöntem, sitenin SSL sertifikası olup olmadığını kontrol etmek ve URL'nin doğru yazıldığından emin olmaktır. Ayrıca, popüler e-ticaret siteleri veya bankalar gibi hassas bilgilerin paylaşıldığı sitelere erişirken dikkatli olunmalı ve güvenlik önlemleri alınmalıdır. Sahte sitelerden kaçınmak, kullanıcıların kişisel ve mali güvenliklerini korumak için önemli bir adımdır.

10 **Sosyal mühendislik saldırılarına karşı dikkatli olun:** Sosyal mühendislik saldırıları, kişileri manipüle etmek ve hassas bilgilere erişmek için psikolojik ve sosyal manipülasyon tekniklerini kullanan saldırı türleridir. Bu saldırılar, genellikle insanların güvenini kazanmaya çalışan sahte veya dolandırıcı kişiler tarafından gerçekleştirilir. Saldırganlar, telefonda, e-postada veya sosyal medya üzerinde sahte kimlikler kullanarak kendilerini başka biri olarak tanıtabilirler. Saldırıların hedefleri, kullanıcı adları, parolalar, banka bilgileri ve diğer kişisel veya mali bilgilerdir. Sosyal mühendislik saldırılarının birçok çeşidi vardır, örneğin "phishing" olarak bilinen saldırılar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini ele geçirme amacını taşır. Sosyal mühendislik saldırılarının başarı şansını azaltmanın en etkili yolu, herhangi bir istenmeyen veya şüpheli talebe karşı dikkatli ve şüpheci olmaktır. Bilinmeyen kişilerin veya kaynakların taleplerine güvenmemeli ve herhangi bir bilgi veya işlem talebi geldiğinde doğrulama yapmak için alternatif iletişim kanallarını kullanmalıyız.

11 **Sosyal medya hesaplarınızı koruyun:** Sosyal medya hesaplarınızı korumak, kişisel güvenliğinizi sağlamak ve siber saldırılardan korunmak için önemli bir adımdır. Çünkü sosyal medya platformları, kişisel bilgilerinizi ve iletişim bilgilerinizi içeren hassas verilerinizi içerir. İlk adım, güçlü bir parola kullanmaktır. Parolanız karmaşık, benzersiz ve tahmin edilemez olmalıdır. Ayrıca, iki faktörlü kimlik doğrulama özelliğini etkinleştirmek de hesap güvenliğinizi artırır. Gizlilik ayarlarınızı gözden geçirin ve sadece tanıdığınız kişilere erişim izni verin. Arkadaşlık isteklerini dikkatlice değerlendirin ve bilinmeyen kişilere erişimi sınırlayın. Sosyal medya platformlarında güvendiğiniz uygulamaları ve oyunları indirirken dikkatli olun, kötü amaçlı yazılımlar içerebilirler. Sosyal mühendislik saldırılarına karşı dikkatli olun, tanımadığınız kişilerden gelen şüpheli mesajlara veya bağlantılara tıklamayın. Bilinçli paylaşım yapın, özel veya kişisel bilgilerinizi kamuya açıklamaktan kaçının. Son olarak, sosyal medya hesaplarınızı düzenli olarak kontrol edin ve şüpheli aktiviteleri rapor edin.

12 **Sosyal medya paylaşımlarınızı sınırlayın:** Sosyal medya paylaşımlarınızı sınırlamak, kişisel gizliliğinizi korumak ve çevrimiçi güvenliğinizi artırmak için önemli bir adımdır. Çünkü sosyal medya platformlarında paylaştığınız bilgiler, sizin hakkınızda önemli ipuçları sağlayabilir ve kötü niyetli kişilerin hedefi olmanıza neden olabilir. Kişisel bilgilerinizi (adres, telefon numarası, doğum tarihi vb.) kamuya açık olarak paylaşmaktan kaçınmak, dolandırıcılık veya kimlik avı girişimlerine karşı korunmanıza yardımcı olur. Ayrıca, sosyal medyada paylaştığınız fotoğraflar veya yazılar, gelecekte iş, eğitim veya ilişkiler gibi konularda olumsuz sonuçlar doğurabilir. Bu nedenle, sosyal medya paylaşımlarınızı sınırlayarak bilgilerinizi kontrol altında tutmak ve güvende olmak önemlidir.

13 **Bilinmeyen kişilere veya kaynaklara güvenmeyin:** İnternet çağında yaşadığımız bu dönemde, bilinmeyen kişilere veya kaynaklara güvenmeme önemli bir siber güvenlik ilkesidir. İnternet üzerindeki dolandırıcılık, kimlik avı saldırıları ve kötü amaçlı yazılımlar gibi tehditler giderek artmaktadır. Birçok sahte web sitesi, sahte e-posta veya mesajlar aracılığıyla kişisel ve mali bilgilerimizi ele geçirmeye çalışmaktadır. Bu yüzden, bilmediğimiz kişilere veya kaynaklara güvenmeden önce dikkatli olunmalıdır. Herhangi bir şüpheli talep, teklif veya bağlantıya karşı şüpheci olmalı ve doğruluğunu doğrulamak için ek araştırma yapılmalıdır. Ayrıca, internet üzerindeki bilgileri paylaşırken ve çevrimiçi işlem yaparken güvenilir olduğunu bilinen kaynaklar tercih edilmelidir.

14 **Spam e-postalara dikkat edin:** Spam e-postalara dikkat etmek, güvenli bir çevrimiçi deneyim için oldukça önemlidir. Spam e-postalar, genellikle istenmeyen reklamlar, sahte teklifler veya dolandırıcılık amaçlı mesajlar içerir. Bu tür e-postaların açılması veya içindeki bağlantılara tıklanması, kötü amaçlı yazılımların bilgisayara bulaşmasına veya kişisel bilgilerin çalınmasına neden olabilir. Spam e-postalar genellikle şüpheli e-posta adreslerinden veya tanınmayan göndericilerden gelir. Bu nedenle, spam e-postaları tanımak ve açmadan önce dikkatli bir şekilde değerlendirmek önemlidir. Ek olarak, kişisel veya finansal bilgilerinizi içeren herhangi bir e-postayı paylaşmadan önce doğruluklarını teyit etmek önemlidir. Güvendiğiniz kaynaklardan gelen e-postaları dahi dikkatlice inceleyin çünkü saldırganlar, güvendiğimiz kişi veya kuruluşların kimliklerini taklit edebilir. E-posta eklerini veya bağlantılarını açmadan önce her zaman şüpheli bulduğunuz e-postaları silmek en iyisidir.

15 **Bilinmeyen bağlantılara tıklamayın:** Bilinmeyen bağlantılara tıklamamak, siber güvenlik açısından önemli bir adımdır. Bu tür bağlantılar, kötü amaçlı yazılımların ve phishing saldırılarının yayılmasında yaygın olarak kullanılır. Bilinmeyen bağlantılara tıklamak, kişisel bilgilerinizi ele geçirmek, zararlı yazılımların cihazınıza bulaşmasına neden olmak veya dolandırıcılığa maruz kalmak gibi risklerle karşı karşıya olmanıza yol açabilir. Bu nedenle, güvendiğiniz kaynaklardan gelen bağlantılar dışında, bilinmeyen veya şüpheli bağlantılara tıklamaktan kaçınmak önemlidir.

16 **Güvenli bir şekilde online alışveriş yapın:** Güvenli bir şekilde online alışveriş yapmak, kişisel ve finansal bilgilerinizi korumanın önemli bir adımıdır. İnternet üzerinden alışveriş yaparken, güvenli bir bağlantı kullanmanız gerekmektedir. SSL (Güvenli Yuva Katmanı) gibi şifreleme protokollerini kullanan güvenli siteleri tercih etmek, bilgilerinizin güvende kalmasını sağlar. Ayrıca, alışveriş yapacağınız sitenin güvenilir olduğundan emin olmalısınız. İncelemeleri ve kullanıcı yorumlarını kontrol etmek, sitenin güvenilirliği hakkında fikir edinmenizi sağlar. Kredi kartı bilgilerinizi paylaşırken, sadece güvenilir ve tanınmış ödeme sağlayıcılarını kullanmalısınız. Kart bilgilerinizi güvende tutmak için, güncel bir antivirüs yazılımı ve güvenlik duvarı kullanarak cihazınızı korumanız önemlidir. Ayrıca, düzenli olarak hesap hareketlerinizi kontrol etmek ve şüpheli aktiviteleri hızlıca rapor etmek, olası bir dolandırıcılığın erken tespitini sağlar. Özetle, online alışverişte güvenliği sağlamak için güvenilir siteleri tercih etmek, güçlü bir parola kullanmak ve kredi kartı bilgilerinizi korumak önemlidir.

17 Bilinmeyen USB belleklere veya harici cihazlara güvenmeyin: Bilinmeyen USB belleklere veya harici cihazlara güvenmemek, kişisel ve bilgisayar güvenliği açısından son derece önemlidir. Birçok siber saldırı ve kötü amaçlı yazılım, bilgisayarlara ve diğer cihazlara bulaşmak için USB bellekler veya harici cihazlar kullanmaktadır. Bilinmeyen kaynaklardan gelen USB bellekleri veya harici cihazları bilgisayara bağlamak, kötü niyetli yazılımların cihaza bulaşmasına ve hassas verilerin çalınmasına neden olabilir. Bu tür cihazlar, içlerinde zararlı yazılımlar veya virüsler taşıyabilir ve kullanıcıların haberi olmadan veri kaybına veya kimlik avı saldırılarına yol açabilir. Bu nedenle, bilinmeyen kaynaklardan gelen USB bellekleri veya harici cihazları kullanmaktan kaçınmak, güvenlik risklerini minimize etmek için önemli bir adımdır. Bunun yerine, güvendiğiniz ve güvenilir olduğunu bildiğiniz kaynaklardan aldığınız USB bellekleri veya harici cihazları tercih etmek daha güvenli bir yaklaşımdır. Ayrıca, antivirüs yazılımınızı güncel tutmak ve düzenli taramalar yapmak da bilgisayarınızın güvenliğini sağlamak için önemlidir.

18 İnternet güvenliği eğitimi alın: İnternet güvenliği eğitimi almak, internet kullanıcılarına siber tehditler hakkında bilgi verir ve güvenli internet kullanımı konusunda farkındalık yaratır. Bu eğitimler, çevrimiçi dolandırıcılık, kimlik avı saldırıları ve kötü amaçlı yazılımlar gibi tehditleri tanımak ve önlemek için gerekli becerileri sağlar. İnternet güvenliği eğitimi, kullanıcıların kişisel ve finansal bilgilerini korumayı, güvenli parolalar oluşturmayı, güvenilir kaynakları doğrulamayı ve çevrimiçi davranışlarının etkilerini anlamayı öğretir. Bu eğitimler, internet kullanıcılarının güvenliğini artırarak çevrimiçi ortamda daha bilinçli ve korunaklı hale gelmelerine yardımcı olur.

Bu kapsamda BTK Akademi tarafından etkili, ücretsiz ve sertifikalı eğitimler sağlanmaktadır. https://www.btkakademi.gov.tr adresinden haftanın her günü ve her saati eğitim alabilir, kendinizi internet güvenliği ve birçok alanda geliştirebilirsiniz.

19 **Güvenli dosya paylaşımı yapın**: Güvenli dosya paylaşımı yapmak, kişisel ve hassas bilgilerinizi korumak için önemlidir. Dosyalarınızı paylaşırken güvenli dosya paylaşım hizmetlerini tercih etmek, verilerinizin şifrelenmesini sağlar. Bu sayede, yetkisiz erişim riskini azaltır ve bilgilerinizin güvende kalmasını sağlarsınız. Ayrıca, paylaştığınız dosyalara erişim izinlerini sınırlayarak, yalnızca belirli kişilerin dosyaları görüntüleyebilmesini sağlayabilirsiniz. Böylece, dosyalarınızın güvenliğini ve gizliliğini koruyabilirsiniz.

Hızla gelişen teknolojide siber güvenliği tamamen sağlamanın bir yolu olmamakla birlikte bireysel kullanıcılar tarafından yukarıdaki önlemlerin uygulanması, saldırganlara karşı yüksek seviyede koruma sağlayacaktır.