

BİLGİ GÜVENLİĞİ FARKINDALIĞI



Elektronik İmza, Sadece Bir Tık Değil; Sorumluluk ve Güvendir.

E-İmzanı Kötü Niyetlilerden Koruyarak Dijital Dünyada Güvende Kal!

E-İmza Güvenliği İçin Alınabilecek Önlemler

1. Elektronik İmza Taşıyıcınızı (Akıllı Kart/USB Token) Güvende Tutunuz:

- E-İmza sertifikanızı barındıran **akıllı kartınızı veya USB token'inizi kişisel olarak gerekli özeni göstererek muhafaza ediniz.**
- İşlem yapılmadığı zamanlarda **USB token'i bilgisayardan çıkartınız.**
- **Çalınma veya kaybolma durumunda derhal Bilgi İşlem Dairemize ve Elektronik Sertifika Hizmet Sağlayıcınıza (ESHS) bildiriniz.**
- Odanızda personel kalmayacağı durumlarda son çıkan personelin **kapıyı kilitlemesine** özen gösteriniz.
- **ESHS'nizden** gelen bildirimler doğrultusunda sertifikanızın geçerlilik süresinin takibini yaparak, kullanmaya devam ederseniz **geçerlilik süresinin bitiş tarihinden en az 1 ay önce yenileme işlemlerini başlatıp** sürecin daha güvenli ve kısa sürede tamamlanmasını sağlayınız.
- E-İmzanızı uzun süre kullanmayacağınızda **"Askıya Alma"** işlemi , hiç kullanmayacağınızda ise **"Sertifika İptali"** işlemi yapmayı unutmayınız.

2. Parola Güvenliğine Dikkat Ediniz

- E-İmza PIN kodunuzu **karmaşık ve tahmin edilemeyecek şekilde belirleyiniz.** Tekrar tekrar yanlış girilen PIN kodlarının akıllı kartı bloke edeceğini unutmayınız.
- Parolalarınızı **kimseyle paylaşmayınız ve periyodik olarak değiştiriniz.**

3. Bilgisayar Güvenliğinizi Sağlayınız

- E-İmza kullandığınız bilgisayarın **güncel antivirüs yazılımına sahip olduğundan ve sistem güncellemelerinin** yapıldığından emin olunuz. **Keylogger (tuş kaydedici)** gibi zararlı yazılımlara karşı dikkatli olunuz.
- İşlem yaptığınız bilgisayarın **güvenli ağ bağlantısında (VPN, kurumsal ağ vs.)** olduğuna dikkat ediniz.
- [Nitelik elektronik sertifikanızı](#) kullanarak imzalama işlemini gerçekleştirebilmeniz için kullanmış olduğunuz kart okuyucunun, akıllı kartın ya da token'in sisteminize, sertifika

hizmet sağlayıcınızın direktiflerine uygun ve doğru olarak kurulmuş olduğundan emin olunuz. Güncel olmayan yazılım ve ayarlar, imzalama işlemlerinde hata alınmasına ve zafiyetlere neden olabilir.

Kurulum işlemleri ile ilgili detaylı bilgi ve yardıma e-imza sertifikanızı temin etmiş olduğunuz sertifika [hizmet sağlayıcınızın web sayfasından](#) veya [yardım merkezinden](#) ya da e-imza'yı kullanacağınız uygulamayı sunan [birimin destek hizmetlerinden](#) erişebilirsiniz. Bu işlemler için harici sitelerde yazanlara güvenerek virüslü olma ihtimali olan programlar yüklemeyiniz.

4. Yetkisiz İşlem Taleplerine Karşı Dikkatli Olunuz

- Size ait E-İmzanın kullanımıyla ilgili **üçüncü kişilerden gelen belge imzalama, parola isteme gibi taleplere kesinlikle itibar etmeyiniz.** E-Posta, telefon, anlık mesaj gibi yollarla gelen **şüpheli imzalama taleplerini** kabul etmeyiniz.
- Sizden **kişisel verilerinizi isteyenlere karşı dikkatli olunuz.** Kişisel verilerinizi ve e-devlet parolası gibi kritik bilgilerinizi ele geçiren saldırganların sistemlerde/süreçlerde bulacakları zafiyetlerle sizin adınıza e-imza sertifikası çıkarabileceğini unutmayınız.
E-Devlet'e girişten sonra arama kısmına aşağıdaki ibareyi yazarak adınıza üretilmiş Nitelikli Elektronik Sertifikaları sorgulama işlemini zaman zaman yapınız:
[BTK Nitelikli Elektronik Sertifika Sorgulama](#)
- **İş yükü fazlalığı, zaman darlığı veya benzeri gerekçelerle e-imzanızın başka bir kişi tarafından kullanılması kesinlikle yasaktır.** E-imzanın üçüncü kişilerle paylaşılması, şahsi hukuki ve cezai sorumluluk doğuracak, aynı zamanda kurumumuzun bilgi güvenliği süreçlerinde ciddi zafiyetlere yol açacaktır. Bu kapsamda;
 - **E-imzanızın şifresini kimseyle paylaşmayınız.**
 - **E-imzanızı kullanmaları için başkalarına teslim etmeyiniz.**
 - **İş yüküyle ilgili sorunları bağlı bulunduğunuz yöneticinizle paylaşınız; sorumluluk devri kesinlikle yapılmamalıdır.**

5. İmzalama İşlemi Sırasında Dikkat Edilmesi Gerekenler

- İmzaladığınız belgelerin **içeriklerini dikkatlice kontrol ediniz.**
- İmza işlemi sırasında karşınıza çıkan uygulama ve servislerin **güvenilir kaynaklardan olduğundan emin olunuz.**
- E-imza kullanacağınız uygulama açıldığında e-imza arayüzünden doküman üzerindeki önceki imza durumlarının geçerli olup olmadığını kontrol ediniz. Doküman üzerindeki

imzalar geçerliyse e-imza parolanızı girerek imzanızı atınız.

- Tüm imzalama işlemleri sırasında **kendi işlemlerinizin iz kaydının (logunun) tutuluyor** olduğundan emin olunuz, olası uyuşmazlıklarda sizin için hukuki güvence sağlayacaktır.
- PDF, Word gibi ofis belgelerinin görünen içerikleri dışında, gizli meta veriler, makrolar veya gömülü zararlı kodlar barındırabileceğini unutmayınız. Belgeyi açtığınızda otomatik olarak çalışabilen bu tür kodlar, cihazınıza zararlı yazılım bulaştırabilir veya veri sızdırabilir. Bu nedenle, **kaynağını bilmediğiniz veya güvenilirliğinden emin olmadığınız belgeleri açmadan önce mutlaka antivirüs/malware taramasından geçirin ve makro içeriklerine karşı dikkatli olunuz.**

6. ESHS İçin Dikkat Edilecekler

- Elektronik imza süreçlerinde, **güvenlik ve yasal geçerlilik açısından Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından [yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcıları \(ESHS\)](#)** üzerinden hizmet alınız.
- E-imzanızla ilgili **kayıp, çalıntı, iptal veya yenileme işlemlerinde hızlı hareket edebilmek için** ESHS'nize ait iletişim bilgilerini güncel ve kolayca ulaşabileceğiniz bir yerde tuttuğunuzdan emin olunuz.
- Nitelikli elektronik sertifika almak için gerekli tüm bilgi ve belgeleri eksiksiz ve doğru olarak sağlayınız. ESHS'ye vermiş olduğu bilgilerde değişiklik meydana gelmesi halinde ESHS'nizi derhal bilgilendiriniz.

7. Mobil E-İmza

- Elektronik imzaya ilişkin mevzuat mobil elektronik imzayı da kapsadığı için mobil elektronik imza da elektronik ortamda güvenli elektronik imzanın sağladığı hukuksal geçerliliği sağlamaktadır. Eğer mobil e-imza kullanıyorsanız bunun için kullandığınız mobil cihazınız için de gerekli güvenlik önlemlerini mutlaka alınız.

8. Şüpheli Durumlar

- E-İmza oluşturma aracının veya erişim verisinin kaybolması, çalınması, güvenilirliğinden kuşku duyulması durumunda Elektronik Sertifika Hizmet Sağlayıcınızı derhal bilgilendiriniz.
- Herhangi bir şüpheli durumda **Bilgi İşlem Dairesi ve ESHS ile iletişime geçiniz.**

Unutmayın!

Elektronik İmzanız size özeldir ve ıslak imzanızla eşdeğer yasal geçerliliğe sahiptir. İmzanızın yetkisiz kullanımı halinde sorumluluk size ait olacaktır.



Elektronik İmzada Güven, Dijital Hayatta Güvencedir!