

Balıkesir Üniversitesi E-Posta Güvenliği (@balikesir.edu.tr) İki Faktörlü Kimlik Doğrulama (2FA) Kurulum ve Açıklama

Sayın Personelimiz,

Üniversitemiz kurumsal e-posta hesaplarının güvenliğini artırmak ve yetkisiz erişim risklerini en aza indirmek amacıyla **İki Faktörlü Kimlik Doğrulama (2FA)** uygulaması hizmete alınmıştır.

İki Faktörlü Kimlik Doğrulama sistemi; kullanıcı adı ve parola ile yapılan giriş işlemlerine ek olarak mobil cihaz üzerinden üretilen tek kullanımlık doğrulama kodunun girilmesini zorunlu kılmaktadır. Bu yöntem sayesinde parolanın üçüncü kişiler tarafından ele geçirilmesi durumunda dahi hesap güvenliği sağlanmaktadır.

Kurulum İşlemleri

1. Mobil cihazınıza **Google Authenticator** uygulamasını indiriniz. (App Store / Play Store)

Play Store Linki :

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=tr>

App Store Linki :

<https://apps.apple.com/us/app/google-authenticator/id388497605>

2. <https://mail.balikesir.edu.tr> adresi üzerinden kurumsal webmail hesabınıza giriş yapınız.
3. **Tercihler > Hesaplar** menüsüne giriniz.

4. "İki Faktörlü Kimlik Doğrulamayı Kurun" seçeneğini tıklayınız.

Hesaplar

Hesap Adı	Durum	E-posta Adresi	Tip
Ana Hesap	Tamam	baumweb@baunweb.com.tr	Ana

[Diğ. Hesap Ekle](#) [Kişilik Ekle](#) [Sil](#)

Ana Hesap Ayarları

E-posta adresi: baunweb@baunweb.com.tr

Hesap Adı: Ana Hesap

Gönderilen Mesajlar için Ayarlar

Kimden: E-posta mesajının "Kimden" alanında görülecek adı seçin
BAUN WEB GRUBU

Yanıtla: ☐ E-posta mesajının "Yanıtla" alanını şu şekilde ayarla
İmza: İmza alanını yönetin...

Hesap Güvenliği: Standart kimlik doğrulama kullanımı

Birincil Yöntem: ☒ Adli telefonundaki kimlik doğrulama uygulaması (engelli)

Temsilciler: Şu kullanıcıların bu hesap için temsilci yetkisi var

[Ad](#) [Tip](#)

Sonuç bulunamadı.

[Temsilci Ekle](#) [Temsilci Düzenle](#) [Kaldır](#)

Temsilci Gönderme Ayarları:

- ☒ Gönderilmiş mesajların bir kopyasını Gönderilenler kladörüne kaydet
- ☐ Gönderilmiş mesajların bir kopyasını temsilcinin Gönderilenler kladörüne kaydet
- ☐ Gönderilmiş mesajların bir kopyasını benim ve temsilcinin Gönderilenler kladörüne kaydet
- ☐ Gönderilmiş mesajların bir kopyasını kaydetme

İki faktörlü kimlik doğrulamayı ayarlayın

İki faktörlü kimlik doğrulama, yalnızca kullanıcı adınızı ve şifrenizi değil, aynı zamanda güvenli ikinci bir yöntemden gelen kodu da gerektirerek hesabınıza ek güvenlik sağlar. Bu, davetsiz misafirlerin hesabınıza erişmesini çok daha zorlaştırır.

İkinci bir yöntemi yapılandırmak için "Kurulumu Başlat"ı seçin. Yöntem yapılandırdıktan sonra, her oturum açışınızda sizden bir kod sorulmasını veya bu chaza her zaman güvenmeyi seçebilirsiniz.

[Kurulumu Başlat](#) [İptal](#)

Mail Şifrenizi giriniz.

İki faktörlü kimlik doğrulamayı ayarlayın

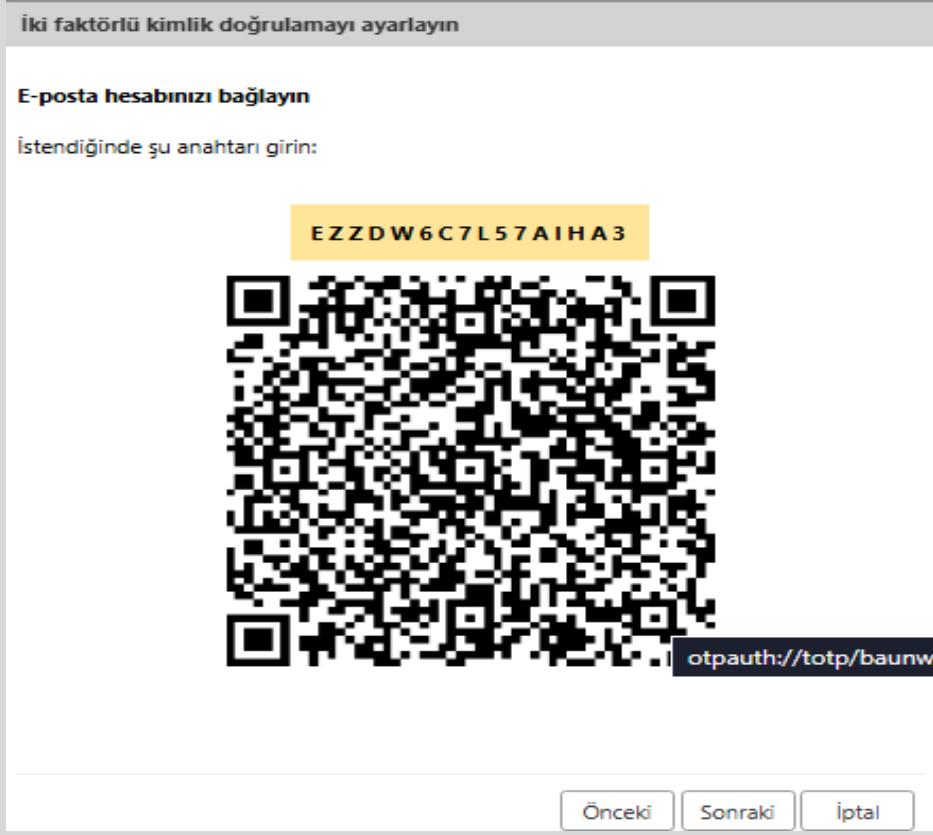
Parolayı Onayla

Devam etmek için lütfen bu hesabın şifresini onaylayın.

Parola:

[Önceki](#) [Sonraki](#) [İptal](#)

5. Ekranda oluřan QR kodu Google Authenticator uygulaması ile taratınız.



Not: TOTP altyapısını destekleyen **Microsoft Authenticator** veya **Authy** gibi alternatif uygulamalar da kullanılabilir.

6. Uygulamada görüntülenen 6 haneli kodu sisteme girerek işlemi tamamlayınız.

İki faktörlü kimlik doğrulamayı ayarlayın

Güvenli Kodu Girin

Kimlik doğrulama uygulamanız tarafından oluşturulan güvenli kodu girin.

Kod :

Önceki

Sonraki

İptal

İki faktörlü kimlik doğrulamayı ayarlayın

Başarılı!

İki faktörlü kimlik doğrulama yöntemini başarıyla yapılandırdınız. Her oturum açtığınızda sizden güvenli bir kod istenecektir. Ayrıca bu cihaza her zaman güvenmeyi de seçebilirsiniz.

Kimlik doğrulama yönteminize erişiminiz yoksa oturum açmak için kullanılabilecek bir dizi tek kullanımlık kodu yazdırın.

Son

Not: TOTP altyapısını destekleyen Microsoft Authenticator veya Authy gibi alternatif uygulamalar da kullanılabilir.

Outlook / Mobil Cihaz Kullanıcıları İçin:

2FA aktif ettikten sonra Outlook, Thunderbird veya mobil mail uygulamalarında normal şifreniz çalışmayacaktır.

Bu istemciler için:

Mobil veya 2 faktörlü kimlik doğrulamayı desteklemeyen uygulamalar için;

1. Webmail'de Tercihler > Hesaplar > Ana Hesap Ayarları bölümüne gidiniz.

2. "Uygulama Kodu Ekle" butonuna tıklayınız.

3. Oluşturulan şifreyi mail istemcinizde

kullanınız. (Outlook, Gmail uygulaması,

Samsung Mail vb.)

Hesaplar

Hesap Adı	Durum	E-posta Adresi
Ana Hesap	Tamam	arzu.tuyumaz@balikesir.edu.tr

[Diş Hesap Ekle](#) [Kişilik Ekle](#) [Sil](#)

Ana Hesap Ayarları

E-posta adresi: arzu.tuyumaz@balikesir.edu.tr

Hesap Adı: Ana Hesap

Gönderilen Mesajlar için Ayarlar

Kimden: E-posta mesajlarının "Kimden" alanında görülecek adı seçin
ARZU TUYUMAZ arzu.tuyumaz@balikesir.edu.tr

Yanıtla: ☐ E-posta mesajlarının "Yanıtla" alanını şu şekilde ayarla
Örneğin, Öğe Deme

İmza: İmzalarınızı yönetin ...

Hesap Güvenliği: İki faktörlü kimlik doğrulamayı kullanma
Birincil Yöntem: ☒ Akıllı telefonumdaki kimlik doğrulama uygulaması (etkinleştirilmiş) ☐ İki faktörlü kimlik doğrulamayı devre dışı bırakın...

Tek Kullanım Kodları: 10 kullanılmayan kod var [Görüntüle](#)

Güvenlik Ayarları: 0 güvenli ayarınız var [bu aygıtı kaldır](#) [Diğer tüm ayarları kaldır](#)

Uygulamalar: İki faktörlü kimlik doğrulamayı desteklemeyen uygulamalar için parolalar oluşturun

Ad	Oluşturuldu	En Son Kullanıldığı Tarih
Sonuç bulunamadı.		

[Uygulama Kodu Ekle](#) [Kodu İptal Et](#)

Temsilciler: Şu kullanıcıların bu hesap için temsilci yetkisi var

Ad	Tip
Sonuç bulunamadı.	

[Temsilci Ekle](#) [İzinleri Düzenle](#) [Kaldır](#)

İki Faktörlü Kimlik Doğrulama işlemi sırasında doğrulama kodu girildikten sonra, güvenli ve kişisel olarak kullanılan cihazlarda “Bu cihaza güven” seçeneğinin işaretlenmesi halinde, ilgili cihaz üzerinden yapılacak girişlerde 30 gün süreyle tekrar doğrulama kodu girilmesi gerekmeyecektir. Bu seçeneğin yalnızca kişisel ve güvenli cihazlarda kullanılması önemle tavsiye olunur.

Önemli Bilgilendirme ;

İki Faktörlü Kimlik Doğrulama işlemi sırasında doğrulama kodu girildikten sonra, güvenli ve kişisel olarak kullanılan cihazlarda “Bu cihaza güven” seçeneğinin işaretlenmesi halinde, ilgili cihaz üzerinden yapılacak girişlerde 30 gün süreyle tekrar doğrulama kodu girilmesi gerekmeyecektir.

Bu seçeneğin yalnızca kişisel ve güvenli cihazlarda kullanılması önemle tavsiye olunur. 2FA uygulaması şu anda isteğe bağlıdır; ancak 15 gün içerisinde zorunlu hale getirilecektir. Google Authenticator dışında Microsoft Authenticator veya Authy gibi TOTP destekleyen uygulamalar da kullanılabilir.

Güvenliğiniz açısından en kısa sürede aktivasyon işleminin tamamlanması önem arz etmektedir. Kurulum veya kullanım sırasında sorun yaşamanız halinde Bilgi İşlem Daire Başkanlığı ile iletişime geçebilirsiniz. (bidb.balikesir.edu.tr, destek.balikesir.edu.tr) Bu tedbirler, bireysel hatalardan kaynaklanan sorunların tüm kullanıcılarımızı ve kurumumuz mail trafiğini engellemek, sürekli ve güvenilir halde çalışır tutmak amacıyla alınmaktadır.

Bilgi güvenliği, bireysel ve kurumsal sorumluluğumuzun temel unsurlarından biridir. Göstereceğiniz hassasiyet için teşekkür ederiz.

Balıkesir Üniversitesi / Bilgi İşlem Daire Başkanlığı