

Norton Hesabım™

Kullanım Kılavuzu



Norton Hesabım Kullanıcı Kılavuzu

Bu kitapçıkta bahsi geçen yazılım bir lisans sözleşmesi çerçevesinde verilmektedir ve yalnızca söz konusu sözleşmenin koşullarına uygun olarak kullanılabilir.

Belge sürümü 22.20.1

Telif Hakkı © 2020 Symantec Corporation. Tüm hakları saklıdır.

Bu belgede anlatılan ürün; kullanım, kopyalama, dağıtım ve derlemeyi açma/tersine mühendislik uygulama sınırlaması getiren lisanslar altında dağıtılmaktadır. Bu belgenin hiçbir bölümü Symantec Corporation'ın ve varsa lisans verenlerinin önceden yazılı izni olmadan, hiçbir şekilde ve hiçbir biçimde yeniden üretilemez.

BELGELER "OLDUĞU GİBİ" SAĞLANMAKTADIR VE TÜM AÇIK VEYA ÖRTÜK KOŞULLAR, İBRAZLAR VE GARANTİLER, TİCARİ DEĞER, BELİRLİ BİR AMACA UYGUNLUK VEYA YASAYI İHLAL ETMEME KONUSUNDA UYGULANAN TÜM ÖRTÜK GARANTİLER DAHİL OLMAK ÜZERE, YASAL AÇIDAN GEÇERSİZ SAYILMAYACAK EN GENİŞ KAPSAMDA REDDEDİLİR. SYMANTEC CORPORATION, BU BELGENİN SAĞLANMASI, UYGULANMASI VEYA KULLANILMASIYLA BAĞLANTILI ARIZİ VEYA NEDEN OLUNAN ZARARLARDAN SORUMLU TUTULAMAZ. BU BELGEDE YER ALAN BİLGİLER HABER VERİLMEKSİZİN DEĞİŞTİRİLEBİLİR.

Lisanslı Yazılım ve Belgeler, FAR 12.212 bölümünde tanımlandığı gibi ticari bilgisayar yazılımı olarak kabul edilmekte olup FAR Bölüm 52.227-19 ve devamındaki "Ticari Bilgisayar Yazılımı - Kısıtlı Haklar", DFARS 227.7202 Uygun olduğu üzere ister Symantec tarafından şirket içinde isterse de servislerde teslim edilmiş olsun "Ticari Bilgisayar Yazılımı ve Ticari Bilgisayar Yazılımı Belgeleri," ve sonrasında gelen yönetmelikler. Lisanslı Yazılım ve Belgelerin ABD Hükümeti tarafından kullanımı, değiştirilmesi, üretilmesi, gösterilmesi veya ifşa edilmesi yalnızca bu Sözleşme'nin koşullarına uygun olarak gerçekleştirilebilir.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

<http://www.symantec.com>

İrlanda'da üretilmiştir.

10 9 8 7 6 5 4 3 2 1

İçindekiler

Bölüm 1	Norton LifeLock'a Hoş Geldiniz	6
	Yeni Norton 360 için sistem gereklilikleri	6
	Norton hesabınıza erişim	8
Bölüm 2	Güvenliğinizi kurma	9
	Cihaz Güvenliği'ni kurma	9
	Norton Password Manager'ı Kurma	10
	Bulut Yedekleme 'yi Kurma	15
	LifeLock Identity Theft Protection'ı kurma	15
	LifeLock** tarafından desteklenen Dark Web Denetimi	17
	Secure VPN'i Kurma	18
	Ebeveyn denetimlerini kurma	19
	Norton Safe Web'i kullanarak bankacılık işlemleri bilgilerinizi koruyun	23
Bölüm 3	Cihaz Güvenliğinizi yönetme	24
	Cihazınız risk altındayken ne yapılmalı?	24
	LiveUpdate'i Çalıştırma	25
	Norton'un tespit ettiği cihaz güvenlik tehditlerini görüntüleme ve düzeltme	25
	Karantinaya alınmış risk veya tehditlere göre hareket et	27
	Bilgisayar performansını optimize etmek ve iyileştirmek için Norton'u kullanma	29
	Bilgisayarınızda tehditleri denetlemek için Norton taramaları çalıştırma	33
	Özel Norton taramaları oluşturma	36
	Norton taramalarını zamanlama	37
	Norton SONAR korumasının tespit ettiği gerçek zamanlı tehditleri görüntüleme	38
	Dosya ve klasörleri Norton Auto-Protect, SONAR ve Download Intelligence taramalarından dışlama	39
	Düşük risk imzalı dosyaları Norton taramaları dışında bırakma	40
	Otomatik görevleri aç veya kapat	41

Özel görev çalıştırma	42
Güvenlik ve performans taramalarını zamanla	42
PC'nizi etkileyen kötü amaçlı işlemleri engellemek için Veri Koruyucu'yu yapılandırma	43
Kimlik avı girişimlerinde kullanılabilecek komut dosyalarını kaldırmak için Norton'u ayarlayın	46
SSS: Norton Komut Dosyası Kontrolü	49
Password Manager'ınızı Yönetme	51
Norton Safe Web'i açma veya kapatma	52
Norton Safe Search kullanarak web'de arama yap	53
Norton Password Manager'a Erişme	54
Norton Password Manager bulut kasası oluşturma	55
Norton Password Manager bulut kasanızı silme	57
Norton Password Manager verilerinizi dışa aktarma	57
Norton Password Manager verilerinizi içe aktarma	59
Norton Security araç çubuğunu etkinleştirme veya devre dışı bırakma	60
Uygulamalarınızı ve dosyalarınızı saldırılardan, bilgisayar korsanlarından ve sıfır gün saldırılarından koruyun.	60
Norton Güvenlik Duvarı'nı açma veya kapatma	62
Program Kuralları'nı Özelleştirme	63
Güvenlik duvarı kurallarının sırasını değiştir	63
Trafik kuralını geçici olarak kapatma	64
Bloke edilen bir programa izin ver	65
Güvenlik Duvarı Engelleme Bildirimi'ni kapat	66
İzinsiz Girişi Önlemedişlama listesi	66
Tarayıcı Koruması'nı açma	67
Norton Güvenlik Duvarı'nı, bir saldırıyı engellerken sizi uyaracak veya bildirmeye başlayacak şekilde ayarlayın	68
AutoBlock özelliğini kapat veya aç	69
AutoBlock uygulanmış bilgisayarların blokesini kaldırma	69
Aygıt Güven'ine bir cihaz ekleme	70
İndirme Bilgi Merkezi özelliğini kapat veya aç	71
Spam filtresini aç veya kapat	72
Norton'un İnternet kullanımını tanımlama	73
Ağ Kullanımı Sınırlaması'nı kapat veya aç	74
Norton'u uygulamaları izleyecek ve kötü amaçlı web sitelerinin bilgisayarınıza erişimini önleyecek şekilde ayarlayın	74
Norton Bulut Yedekleme'yi kullanmaya başlama	76
Yedekleme kümelerinize dosya ve klasör ekleme ya da dışlama	78
Norton yedekleme kümelerinden resimleri, müzik dosyalarını veya diğer önemli dosyaları geri yükleme	79

Norton yedeklemeyi açma	80
Norton ürününüzün ayarlarını özelleştirme	81
Gerçek Zamanlı Koruma ayarlarını özelleştirme	82
Taramalar ve Riskler ayarları	83
İzinsiz Giriş ve Tarayıcı Koruması ayarları	86
Norton'u korunan cihazlarınızı uzaktan yönetmenizi sağlayacak şekilde ayarlama	87
Norton cihaz güvenlik ayarlarını yetkisiz erişimden koruma	87
Norton cihaz güvenliğinde bilgi aramak için kısayol tuşu belirleme	88
 Bölüm 4	
Ek çözümler bulma	89
Cihaz Güvenliğini Kaldırın	89
Sorumluluk Reddi	90

Norton LifeLock'a Hoş Geldiniz

Bu bölümde aşağıdaki konular yer almaktadır:

- [Yeni Norton 360 için sistem gereklilikleri](#)
- [Norton hesabınıza erişim](#)

Yeni Norton 360 için sistem gereklilikleri

Yalnızca Norton Cihaz Güvenliği yetkisi

- Norton™ AntiVirus Plus, tek bir PC veya Mac'i kapsar

Cihaz Güvenliği ve Norton Secure VPN yetkileri

Windows, Mac, Android ve iOS'ta çalışan cihazları destekler

- Norton™ 360 Standard, tek bir cihazı kapsarNorton 360 Standard, tek bir cihazı kapsar
- Norton™ 360 Deluxe, 5 adede kadar cihazı kapsar
- LifeLock Select özellikli Norton™ 360, 5 adede kadar cihazı kapsar
- LifeLock Advantage özellikli Norton™ 360, 10 adede kadar cihazı kapsar
- LifeLock Ultimate Plus özellikli Norton™ 360 için cihaz kapsamı sınırsızdır (Kısıtlamalar geçerlidir*)

Cihaz Güvenliği

Not: Tüm özellikler tüm platformlarda mevcut değildir.

Not: Ebeveyn Denetimleri, Bulut Yedekleme ve SafeCam şu anda Mac OS'te desteklenmemektedir.

Windows™ İşletim Sistemleri

- ◆ ■ Microsoft Windows® 10 (tüm sürümleri)
- Microsoft Windows® 10 S modunda (32 bit veya 64 bit veya ARM32) 1803 sürümü ve üstü
- Microsoft Windows® 8/8.1 (tüm sürümleri)
Bazı koruma özellikleri, Windows 8 Başlat ekranı tarayıcılarında kullanılamaz.
- Service Pack 1 ile Microsoft indows® 7 (tüm sürümleri) veya sonrası

Not: Norton AntiVirus Plus, S modunda Windows 10'da desteklenmemektedir.

Mac® İşletim Sistemleri

- ◆ Mac OS X 10.10.x veya sonraki sürümleri, Norton ürünü sürüm 8.0 veya sonrası ile birlikte.

Not: Norton Family Ebeveyn Denetimleri ve Online Backup şu anda Mac OS'te desteklenmemektedir.

Android™ İşletim Sistemleri

- ◆ Android 4.1 veya üzeri
Google Play uygulamasının yüklü olması gerekir.
Google Play'de uygulamalar için otomatik tarama, Samsung cihazların haricinde Android 4.1 ve üzerinde desteklenmektedir. Android 4.2 veya sonraki sürümleri çalıştıran Samsung cihazları desteklenir. Daha eski Android sürümlerinde, Google Play'de uygulamaları taramak için Google Play "Paylaş" özelliğinin kullanılması gerekir.

iOS İşletim Sistemleri

- ◆ Apple iOS'un güncel ve önceki iki sürümünü çalıştıran iPhone veya iPad'ler

Norton™ Secure VPN için sistem gereksinimleri

Windows™ PC, Mac®, iOS ve Android™ cihazlar için kullanılabilir:

Norton Secure VPN PC'ler, Mac'ler, Android akıllı telefonlar ve tabletler, iPad'ler ve iPhone'larla uyumludur. Norton Secure VPN, belirli sayıda cihazda, abonelik süresi boyunca sınırsız şekilde kullanılabilir.

Windows™ İşletim Sistemleri

- ◆ ■ Microsoft Windows® 10 (Windows 10 S haricinde tüm sürümler)
 - Microsoft Windows® 8/8.1 (tüm sürümleri)
 - Service Pack 1 ile Microsoft indows® 7 (tüm sürümleri) veya sonrası
- 150MB kullanılabilir sabit disk alanı

Mac® İşletim Sistemleri

- ◆ Mac OS X 10.10.x veya sonraki sürümü.
- 150MB kullanılabilir sabit disk alanı

Android™ İşletim Sistemleri

- ◆ Android 4.4 veya sonrası
- Google Play uygulamasının yüklü olması gerekir.

iOS İşletim Sistemleri

- ◆ Apple iOS'un güncel ve önceki iki sürümünü çalıştıran iPhone veya iPad'ler

Norton hesabınıza erişim

Norton hesabınızdan Norton aboneliğinizi yönetebilir, ürün anahtarınızı bulabilir, Otomatik Yenileme seçeneklerini ayarlayabilir veya güvenlik özelliklerini yükseltebilirsiniz. Hesabınıza erişmek için cihazınızın İnternete bağlı olması gerekir.

Norton hesabınıza erişin

Not: Bir ürünü çevrimiçi mağazadan satın aldıysanız, uzun zaman önceyse bile, satın alma işleminin bir parçası olarak zaten bir Norton hesabınız vardır. Lütfen satın alma sırasında oluşturulan e-posta adresini ve parolayı kullanın. Parolanızı hatırlamıyorsanız, bkz. [Norton hesap parolanızı sıfırlama](#)

- 1 Tarayıcınızı açın ve şu adrese gidin:
<https://my.norton.com>
- 2 **Giriş Yap** 'ı seçin, ardından **Norton'a Hoş Geldiniz** sayfasında aşağıdakilerden birini yapın:
 - **Giriş yap** sekmesinde, hesap e-postanızı ve parolanızı yazın, ardından **Giriş yap** 'ı seçin.
 - **Hesap Oluştur** sekmesinde, gerekli alanları doldurun ve ardından **Hesap Oluştur** ögesini seçin. Ayrıntılı talimatlar için bkz. [Norton hesabı oluşturma](#)

Güvenliğinizi kurma

Bu bölümde aşağıdaki konular yer almaktadır:

- [Cihaz Güvenliği'ni kurma](#)
- [Norton Password Manager'ı Kurma](#)
- [Bulut Yedekleme 'yi Kurma](#)
- [LifeLock Identity Theft Protection'ı kurma](#)
- [Secure VPN'i Kurma](#)
- [Ebeveyn denetimlerini kurma](#)
- [Norton Safe Web'i kullanarak bankacılık işlemleri bilgilerinizi koruyun](#)

Cihaz Güvenliği'ni kurma

Cihazınızı korumak için Norton Device Security uygulamasını kurmanız gerekir. Cihaz Güvenliği'ni, Windows masaüstü ve dizüstü bilgisayarlarınıza, Mac bilgisayarlarınıza ve Android ve iOS'ta çalışan mobil cihazlara yükleyebilirsiniz.

Cihaz Güvenliği'nizi indirme ve yükleme

- 1 Her bir bilgisayar, dizüstü bilgisayar ve akıllı telefondan tarayıcınızı açın ve aşağıdaki URL'yi yazın:
<https://norton.com/setup>
- 2 Norton hesabınızda oturum açın.

3 Norton Kurulum penceresinde **Kabul Et ve İndir** 'e tıklayın.



4 Ekrandaki okla işaret edilen alana tıklayın ve ekrandaki talimatları uygulayın.
Hizmetiniz otomatik olarak indirilir, yüklenir ve etkinleştirilir.

Not: İndirme işleminiz tamamlanmazsa veya hizmetinizi indirdiğinizde bir hata ile karşılaşırsanız, indirmeyi yeniden başlatabilirsiniz.

Norton Password Manager'ı Kurma

Cihaz Güvenliği'ni yükledikten sonra tarayıcı uzantıları eklemeniz istenir. Özelliklerin çalışması için uzantıları Internet Explorer, FireFox ve Chrome tarayıcılarına eklemeniz gerekir.

Tarayıcıya özgü tüm özelliklere erişmek için Norton tarayıcı uzantılarını etkinleştirmelisiniz. Norton tarayıcı eklentileri şunları içerir:

Norton Safe Web

Güvenli bir arama deneyimi güvenli çevrimiçi sörf, arama ve alışveriş yapmanıza yardımcı olur. Ziyaret ettiğiniz web sitelerini analiz eder ve herhangi bir virüs, casus yazılım, zararlı program ya da başka bir tehdidin bulunup bulunmadığını tespit eder.

[Norton Safe Web hakkında daha fazla bilgi edinin](#)

Norton Safe Search

Arama sonuçları oluşturmak için Ask.com ve Yahoo! kullanan güvenli bir arama motoru. Norton Safe Search arama sonuçlarını site güvenliği ve Norton siciline göre derecelendirir.

Norton Giriş Sayfası

Norton Safe Search seçeneğini, web arama deneyiminizi geliştirmek için kullanan bir web sayfası. Oluşturulan arama sonuçlarının her biri için site güvenlik durumu ve Norton değerlendirmesi sunar.

Norton Password Manager

Oturum açma bilgileri, kişisel bilgiler ve finansal bilgiler gibi tüm gizli bilgilerinizi saklayabileceğiniz güvenli bir konum. Bu bilgileri web sitelerine giriş yapmak, çevrimiçi formları otomatik olarak doldurmak ve çevrimiçi ödemeler için kullanabilirsiniz.

Internet Explorer

Internet Explorer'a Norton tarayıcı uzantısı ekleyin

- 1 Cihaz Güvenliği'ni ilk defa yükledikten sonra **Tarayıcı Koruması** sayfası yeni bir Internet Explorer oturumu açıldıktan sonra yeni bir pencerede otomatik olarak açılır.
- 2 **Tarayıcı Koruması** sayfasında **Norton Security Araç Çubuğunun Etkinleştir** seçeneğine tıklayın.
- 3 Açılan uzantı sayfasında **Uzantı Ekle** ögesine tıklayın.
- 4 Norton Security araç çubuğunu etkinleştirdikten sonra tarayıcınız için Norton Safe Search, Norton Giriş Sayfası ve Norton Password Manager uzantılarını etkinleştirebilirsiniz.

Ekleme için Tıklayın seçeneğini kullanabilirsiniz ve bu özellikleri etkinleştirmek için ekrandaki talimatları takip edebilirsiniz.

- 5 Bu uzantılardan herhangi birini yüklemeyerseniz **Internet Explorer Koruma Uyarısı** bildirimleri Internet Explorer bir hafta sonra başlatıldığında görünür.

Şimdi Yükle 'ye tıklayın ve uzantıları eklemek için ekrandaki talimatları izleyin.

Not: Norton uzantısını daha sonra etkinleştirmek istiyorsanız **Daha Sonra Hatırlat** seçeneğine tıklayın. Bildirim uyarısının görünmesini istemiyorsanız **Tekrar sorma** 'ya tıklayın.

Google Chrome

Google Chrome'a Norton tarayıcı uzantıları ekleme

Not: Google Chrome'un tarayıcı uzantılarını yüklemek için en son Norton 360 sürümüne sahip olmalısınız. En son sürüme sahip değilseniz, Norton ürününde LiveUpdate'i çalıştırın. Google Chrome tarayıcıları için aşağıdaki uzantıları sunarız:

- Norton Safe Web
 - Norton Password Manager
 - Norton Safe Search
 - Norton Giriş Sayfası
- Aşağıdaki talimatları izleyerek Chrome tarayıcı uzantılarını yükleyebilirsiniz.
- 1 Cihaz Güvenliği'ni ilk defa yükledikten sonra **Tarayıcı Koruması** sayfası yeni bir Google Chrome oturumu açıldıktan sonra yeni bir pencerede otomatik olarak açılır.
Ayrıca, **İnternet Güvenliği** sütununda **Şimdi Kur** seçeneğine tıklayarak **Tarayıcı Koruması** sayfasını başlatabilirsiniz.
 - 2 **Tarayıcı Koruması** sayfasında **Norton Safe Web** 'in **Ekleme için Tıkla** seçeneğine tıklayın.
 - 3 Açılan uzantı sayfasında **Uzantı Ekle** ögesine tıklayın.
 - 4 Norton Safe Web'i etkinleştirdikten sonra Norton Safe Search, Norton Giriş Sayfası ve Norton Password Manager uzantılarını tarayıcınız için etkinleştirebilirsiniz. **Ekleme için Tıklayın** seçeneğini kullanabilirsiniz ve bu uzantıları etkinleştirmek için ekrandaki talimatları takip edebilirsiniz.
- Google Chrome'daki tüm Norton uzantılarını etkinleştirmek için **Tüm Norton Uzantılarını Ücretsiz Ekleyin** ögesine tıklayın ve ekrandaki talimatları izleyin.
- Norton Safe Web uzantısı yüklü değilse bir hafta sonra Google Chrome başlatıldığında **Chrome Koruması Kaldırıldı** uyarı bildirimi görüntülenir.

- Bu uzantılardan herhangi birini yüklemediyseniz **Google Chrome Koruma Uyarısı** bildirimleri Google Chrome bir hafta sonra başlatıldığında görünür.

5 **Şimdi Yükle** 'ye tıklayın ve uzantıları eklemek için ekrandaki talimatları izleyin.

Not: Norton uzantısını daha sonra etkinleştirmek istiyorsanız **Daha Sonra Hatırlat** seçeneğine tıklayın. Bildirim uyarısının görünmesini istemiyorsanız **Tekrar sorma** 'ya tıklayın.

Mozilla Firefox

Norton tarayıcı özelliklerini Mozilla Firefox'a ekleme

Not: Mozilla Firefox'un web tabanlı, bağımsız tarayıcı uzantılarını yüklemek için en son Norton 360 sürümüne sahip olmalısınız. En son sürüme sahip değilseniz, Norton ürününde LiveUpdate'i çalıştırın. Firefox tarayıcıları için aşağıdaki uzantıları sunarız:

- Norton Safe Web
- Norton Safe Search
- Norton Giriş Sayfası
- Norton Password Manager

Aşağıdaki talimatları izleyerek tarayıcı uzantılarını yükleyebilir veya yükseltebilirsiniz.

- 1 Cihaz Güvenliği'ü ilk kez yükledikten sonra **Tarayıcı Koruması** sayfası Mozilla Firefox oturumu başlatıldığında yeni pencerede/sekmede otomatik olarak açılır.

Norton Cihaz Güvenliği'ni yükselttiyseniz uzantı sayfasını görüntülemek için **Tarayıcı Koruması** uyarısındaki pencerede **Tamam** 'a tıklayın.

Not: Ayrıca, **İnternet Güvenliği** sütununda **Şimdi Kur** seçeneğine tıklayarak **Tarayıcı Koruması** sayfasını başlatabilirsiniz.

- 2 **Tarayıcı Koruması** sayfasında **Norton Safe Web** 'in **Etkinleştir** seçeneğine tıklayın.
- 3 Açılan uzantı sayfasında **İzin Ver** ögesine tıklayın.

Norton Safe Web'i etkinleştirdikten sonra Norton Safe Search, Norton Giriş Sayfası ve Norton Password Manager özelliklerini tarayıcınız için etkinleştirebilirsiniz. **Etkinleştir** seçeneğini kullanabilirsiniz ve bu özellikleri etkinleştirmek için ekrandaki talimatları takip edebilirsiniz.

Firefox'taki tüm Norton uzantılarını etkinleştirmek için **Tüm Norton Uzantılarını Ücretsiz Ekleyin** ögesine tıklayın ve ekrandaki talimatları izleyin.

Bu uzantıyı yüklemeyiyseniz **Firefox Koruma Uyarısı** bildirimleri Firefox bir hafta sonra başlatıldığında görünür. Norton uzantısını daha sonra etkinleştirmek istiyorsanız **Daha Sonra Hatırlat** seçeneğine tıklayın. Bildirim uyarısının görünmesini istemiyorsanız **Tekrar sorma** 'ya tıklayın. **Daha Sonra Hatırlat** 'ı seçerseniz Firefox bir hafta sonra Koruma Uyarısı bildirimi görüntüler. Bildirimdeki **Şimdi Yükle** seçeneğine tıklayabilir ve uzantıları eklemek için ekrandaki talimatları izleyebilirsiniz.

Microsoft Edge

Microsoft Edge'e Norton tarayıcı uzantısını ekleme

Not: Norton Password Manager bağımsız bir uzantıdır ve Microsoft Edge tarayıcısına bir Norton ürününün yüklenmesini gerektirmez. Uzantı yalnızca Windows 10 Creators Update veya sonraki sürümlerin yüklü olduğu bilgisayarlarla uyumludur.

- 1 Microsoft Edge tarayıcısını başlatın.
- 2 Sağ üst köşedeki **Daha Fazla** düğmesine tıklayın ve **Uzantılar** 'ı seçin.
- 3 **Uzantı** penceresinde **Uzantıları mağazadan al** 'a tıklayın.
- 4 **Mağaza** penceresindeki Arama kutusuna **Norton** yazın ve sonuçlardan **Norton Password Manager** 'a tıklayın.
- 5 **Yükle** 'ye tıklayın.

Uzantı yüklendikten sonra **Başlat** 'a tıklayın.

- 6 **Yeni bir uzantınız var** açılır penceresinde **Aç** 'a tıklayın.
- 7 Norton Password Manager simgesini adres çubuğunda görüntülemek için önce tarayıcının sağ üst köşesindeki **Daha Fazla** düğmesine ardından **Uzantılar** 'a tıklayın.
- 8 **Uzantı** penceresinde **Norton Password Manager** 'ı seçin.
- 9 **Norton Password Manager** penceresinde **Düğmeyi adres çubuğunun yanında göster** altındaki kaydırıcıyı **Açık** konuma getirin.

Bulut Yedekleme 'yi Kurma

Bulut Yedekleme, fidye yazılımı, kötü amaçlı yazılım nedeniyle ya da PC'nizde önemli donanım sorunları yaşıyorsanız, veri kaybını önleyici bir önlemdir. Aboneliğiniz size belirli miktarda Norton Cloud Yedekleme alanı sağlar. Ücretsiz bulut depolama alanı hacmi, satın aldığınız aboneliğe bağlıdır.

Not: Norton Cloud Backup özelliği yalnızca Windows'ta kullanılabilir.

İlk yedeklemenizi çalıştırmadan önce Bulut Yedekleme'yi etkinleştirmeniz gerekir.

Not: Bulut Yedekleme özelliğini kullanmak için **Güvenlik Duvarı Ayarları** penceresindeki **Ağ Kullanımı Sınırlaması** seçeneğini **Sınır Yok** olarak ayarlamanız gerekir.

Bulut Yedeklemeyi etkinleştirme

- 1 Norton'u başlatın.
- 2 **Norton Hesabım** penceresinde, **Bulut Yedekleme** 'nin yanında **Kurulum** 'a tıklayın.
- 3 Görüntülenen pencerede **Nereye** sekmesinde, **Ücretsiz Etkinleştir** 'e tıklayın.
- 4 İstendiğinde Norton hesabı kimlik bilgilerinizi sağlayın ve **Giriş Yap** 'a tıklayın
- 5 **Ayarları Kaydet** 'e ve sonra **Kapat** 'a tıklayın.

LifeLock Identity Theft Protection'ı kurma

Şimdi tek bir şirket altında güçlerini birleştiren LifeLock ve Norton, kimliğinizi korumaya yardımcı oluyor.

Aşağıdaki kişisel bilgileri izlemesi için LifeLock'a ekleyebilirsiniz†:

- Sürücü belgesi
- Sosyal güvenlik numarası, doğum tarihi, anne kızlık soyadı

- 5 Sigorta numarası
- 5 adres
- 5 telefon numarası
- 10 banka hesabı
- 10 kredi kartı*

İzlenmesi için telefon numaraları, e-posta adresi veya hesaplar gibi ek bilgiler ekleyebilirsiniz.

LifeLock Kimlik Uyarı Sistemi, kimliğiniz başkası tarafından kullanıldığında sizi uyarır†. Bunlar sizin adınıza cep telefonu hesabı veya araç kredisi almaya çalışan kişiler olabilir.

Not: LifeLock Identity Theft Protection işletmeleri kapsamaz. Teknolojimiz ve hizmetimiz, sosyal güvenlik numaraları ve işletmelerin sahip olmadığı diğer kişisel tanımlanabilir bilgileri olan bireylerin korunmasına yardımcı olmak için tasarlanmıştır.

*Visa, MasterCard, American Express ve Discover gibi başlıca kredi kartları eklenebilir. Ne yazık ki şu anda, perakende mağaza kartları veya hediye kartları gibi diğer kart türleri desteklenmemektedir.

Kimse tüm kimlik hırsızlıklarını veya siber suçları önleyemez.

†LifeLock, tüm işletmelerdeki tüm işlemleri izlemez.

LifeLock Identity Theft Protection'ı kurma

- 1 Norton'u başlatın.
- 2 **Norton Hesabım** penceresinde, **Kimlik Hırsızlığı Koruması** 'nın yanında **Kurulum** 'a tıklayın.
- 3 **LifeLock Üye Girişi** sayfasında **Norton ile Oturum Aç** 'a tıklayın.
- 4 Hesabı kimlik bilgilerinizi girin ve ardından giriş yap'a tıklayın.
- 5 Ekrandaki talimatları izleyin.

Android'de Norton 360 için LifeLock uygulamasını yükleme

- 1 **Play Store** uygulamasını Android cihazınızda başlatın ve **LifeLock Identity Theft Protection** 'ı arayın.
- 2 Uygulama sayfasını Play Store'da bulduktan sonra, **Yükle** 'ye ve ardından **Kabul et** 'e dokununuz.
- 3 Yüklendikten sonra uygulamayı açın ve hesap bilgilerinizle giriş yapın.

Norton 360 için LifeLock uygulamasını iOS'ta yükleme

- 1 **App Store** uygulamasını iOS cihazınızda başlatın ve **LifeLock Identity Theft Protection** 'ı arayın.
- 2 Uygulama sayfasını App Store'da bulduktan sonra, **Al** 'a ve ardından **Yükle** 'ye dokununuz.
- 3 Yüklendikten sonra uygulamayı açın ve hesap bilgilerinizle giriş yapın.

LifeLock** tarafından desteklenen Dark Web Denetimi

Karanlık Web İzleme nedir?

Bulunması zor karanlık web siteleri ve forumlarda kişisel bilgilerinizin** kullanımını izliyoruz. Bilgilerinizi dark web'de tespit ettiğimizde sizi bilgilendiririz.

Bu neden önemli?

Kimlik hırsızları, kişisel bilgilerinizi bulunması zor karanlık web sitelerinde ve forumlarda satabilir.

Ne yapmalısınız?

Bildirimde size ait herhangi bir bilgi bulursanız, aşağıdaki adımlara başvurun.

- **Banka/Kredi Kartı İhlali** : Kart kapalıysa herhangi bir işlem yapılmasına gerek yoktur. Hesap kullanılıyorsa kredi/banka kartı şirketinizle iletişime geçin ve yeni bir kart talep edin. Hesap hareketlerinizi yakından takip edin.
- **E-posta İhlali** : Mevcut e-posta parolanızı değiştirin. Aynı parolaya sahip başka bir hesabınız varsa bunların parolalarını da değiştirin. Devam eden sorunlarınız varsa yeni bir e-posta hesabı açmak iyi bir seçim olabilir. Parolalarınızı her 30 günde bir değiştirmenin hesaplarınızın güvende kalmasına yardımcı olacağını unutmayın.
- **Sosyal Güvenlik Numarası İhlali** : Kimliğinizi korumanıza yardımcı olmak için üç kredi kayıt bürosundan biriyle dolandırıcılık uyarıları ayarlamanızı öneririz.
- **İsim/Adres/Telefon Numarası İhlali** : Neyse ki, Sosyal Güvenlik numaranız gibi daha fazla zarar oluşturabilecek bilgileriniz bu durumda paylaşılmamıştır. Ancak kişisel bilgilerinizin bir kısmı ihlal edildiğinden, herhangi bir tutarsızlığa yönelik olarak kredi raporunuzu yakından takip etmenizi öneririz.

Kişisel bilgileriniz için dark web'i izlemeye devam edeceğiz**. Bilgilerinizi tespit edersek yeni bir e-posta daha göndereceğiz.

Not: Kimse kimlik hırsızlıklarının tamamını önleyemez.

**Norton 360'daki Dark Web Denetimi, yalnızca e-posta adresinizi izlemek için varsayılanları planlar. İzleme amacıyla daha fazla bilgi ekleyebilirsiniz lütfen incelemek için portalda oturum açın.

Secure VPN'i Kurma

Herkese Açık Wi-Fi her yerde: havalimanlarında, kafelerde, alışveriş merkezlerinde ve otellerde. Ücretsiz "kablosuz erişim noktaları" o kadar yaygın ve kullanışlı ki, insanlar iki kere düşünmeden bu ağlara bağlanabiliyor. Ancak herkese açık Wi-Fi kullanırken e-postaları okumak, banka hesabınızı kontrol etmek veya oturum açma gerektiren herhangi bir faaliyet gerçekleştirmek riskli bir iştir. Herkese açık Wi-Fi kullanıyorsanız çevrimiçi etkinlikleriniz izlenebilir. Siber suçlular, kullanıcı adlarınız, parolalarınız, konumunuz, sohbetleriniz, e-postalarınız veya hesap numaralarınız gibi kişisel bilgileri çalabilir.

Secure VPN, ortak bir kablosuz bağlantı kullandığınızda bağlantınızın güvenliğini sağlamaya yardımcı olur. Gizli verilerinizi şifreleyen bir sanal özel ağ (VPN) oluşturur.

Secure VPN, herkese açık Wi-Fi kullanırken gönderdiğiniz ve aldığınız verileri aşağıdaki şekillerde korumanıza yardımcı olur:

- Herkese açık Wi-Fi kablosuz bağlantı noktalarında sizi korumak için banka sınıfı şifreleme ekler.
- Çevrimiçi gizliliğinizi korumak için web'de anonim şekilde gezinmenizi sağlar.
- Sık kullandığınız uygulamalara ve içeriğe gittiğiniz her yerde evinizdeymiş gibi erişim sağlayın.
- Çevrimiçi etkinliğinizi izlemeyen veya kaydetmeyen ve günlüğü olmayan sanal özel ağ ile verilerinizi şifreler.
- Tüketici çevrimiçi güvenliğinde lider Norton LifeLock' ile birinci sınıf müşteri desteği sunar.

Not: Secure VPN özelliği tüm aboneliklerde mevcut değildir.

Secure VPN'i kurmak için aşağıdaki talimatları izleyin.

Güvenli VPN'i Kurma

- 1 Norton'u başlatın.
- 2 **My Norton** penceresinde, **Secure VPN** 'in yanında **Kur** 'a tıklayın.
- 3 Görüntülenen web sayfasında **Oturum Aç** 'a tıklayın.
- 4 Hesabı kimlik bilgilerinizi girin ve ardından giriş yap'a tıklayın.
- 5 Ününü indirmeniz istenirse **İndir** 'e tıklayın.
- 6 Ekrandaki talimatları izleyin.

Diğer masaüstü kullanıcılarla tartışmaya [Norton Topluluğu](#)'ndan katılın.

Ebeveyn denetimlerini kurma

Artık çocuklarınıza güvenli bir İnternet sağlamak için Ebeveyn Denetimlerini kurabilirsiniz. Kurulum oldukça kolaydır ve üç adımdan oluşur.

Ebeveyn Denetimleri, ailenizin çevrimiçi etkinliklerini İnternet tehlikelerinden ve uygunsuz içerikten korumak için gerekenleri sağlar. Aynı zamanda çocuklarınızın gizli bilgileri çevrimiçi ortamlarda iletmesini engelleme size yardımcı olur.

Norton hesabınızda oturum açın

- 1 Norton'u başlatın.
- 2 **Norton Hesabım** penceresinde, **Ebeveyn Denetimleri** 'nin yanında **Kurulum** 'a tıklayın.
- 3 Giriş yapmanız isterse, hesap bilgilerini girin ve giriş yapın.
- 4 Görüntülenen sayfada **Family** sekmesine tıklayın.
- 5 Ailenizi kurmak için **Hizmet Koşulları** 'nı okuyun ve **Kabul ve Devam Et** 'e tıklayın.
- 6 Ekrandaki talimatları izleyin.

Hesabınıza çocuk ekleme

Siz çocuk ekledikçe, Ebeveyn Denetimi, çocuğun yaşına göre önceden tanımlanmış ev kuralları uygular. Ev kurallarını, her çocuğun olgunluk seviyesine göre dilediğiniz zaman özelleştirebilirsiniz.

Not: Hesabınıza 15 adede kadar çocuk ekleyebilirsiniz. Norton Family hesabınıza dilediğiniz zaman çocuk ekleyebilir ya da kaldırabilirsiniz.

- 1 **Çocuğun Adı** kutusuna çocuğun adını girin.

Not: Ad; &, # veya \$ gibi özel karakterler içeremez.

- 2 Çocuğunuzun doğum yılını seçin.

Ev kuralları, çocuğunuzun yaşına göre uygulanır.

- 3 Çocuğunuz için bir profil resmi ayarlamak üzere **Bir Avatar Seç** veya **Bir Fotoğraf Yükle** 'yi seçin.

Not: İlk çocuğun kurulumunu tamamlandıktan sonra hesabınıza [daha fazla çocuk ekleyebilirsiniz](#).

- 4 **İleri** 'ye tıklayın.

Norton Family uygulamasını çocuğunuzun cihazına yükleme

Çocuğunuzun kullandığı her cihaza Norton Family yükleyin. Çocuğunuzun cihazında değilseniz e-posta ile bir indirme bağlantısı göndermek için **Hayır** seçeneğine tıklayın. Norton Family ürününü yüklemek istediğiniz cihazda bu e-postayı açın.

Norton Family uygulamasını Windows'a yüklemek için

- 1 **Çocuğunuz bu aygıtı kullanıyor mu?** altında, **Evet** 'i ve ardından **İleri** 'ye tıklayın.
- 2 İndirilen yükleme dosyasına tıklayın veya çalıştırın.
- 3 Norton İndirme Yöneticisi, Norton Family ürününü cihaza otomatik olarak yükler.
- 4 Kullanıcı Lisans Sözleşmesi'ni okuyun ve ardından **Kabul Et ve Yükle** seçeneğini tıklayın. Yükleme tamamlandığında cihaz hesabınıza otomatik olarak eklenir.
- 5 **Devam** 'ı tıklayın.
- 6 Cihazları ata penceresinde cihazı atamak istediğiniz çocuğun yanındaki **Düzenle** 'yi tıklayın.
- 7 **Farklı oturum aç** 'ı tıklayın ve çocuğun bu cihazda oturum açarken kullandığı hesabı seçin. Çocuğunuz birden fazla kullanıcı hesabına sahipse çocuğu kullanıcı hesaplarının tümünde işaretleyin.
- 8 **Kaydet > Tamam** öğelerine tıklayın.

Norton Family uygulamasını Android'e yüklemek için

- 1 **Norton Family'yi YÜKLE** penceresinde, önce **Evet** 'e ve ardından **Devam** 'a dokunun.
- 2 **Norton Family uygulamasını indir** 'e dokunun.
- 3 İstenirse bu eylemi **Play Store** ile tamamlayın.
- 4 **Yükle** seçeneğine tıklayın ve ekrandaki talimatları izleyin.
- 5 Norton Family ebeveyn denetimi uygulamasını açın.
- 6 **Norton Lisans Sözleşmesi** 'ni okuyun ve ardından **Kabul Et ve Devam Et > Başla** seçeneklerine dokunun.
- 7 **Giriş Yap** 'a tıklayın ve hesap kimlik bilgilerinizi girin.

- 8 Çocuk moduna geçmek için **Çocuk** seçeneğine ve ardından **Devam** düğmesine dokunun.
Çocuk modu, çocuk eklemenize ve ev kurallarını bu cihaza atamanıza olanak tanır.
- 9 Çocuk eklemek için **Çocuk ekle** seçeneğine dokunun ve **PROFİL** penceresinde çocuğunuza ilişkin bilgileri girin.
Avatar simgesine dokunarak çocuğunuzun profili için bir avatar seçin. Galerinden bir resim seçebilir veya çocuğunuzun profili için anlık bir resim çekebilirsiniz.
- 10 **Devam** 'a ve ardından **Kaydet** 'e dokunun.
Norton Family, varsayılan ev kurallarını çocuğunuzun doğum tarihine göre seçmiştir. Çocuğunuz için atanan kuralları incelemek için **Ev Kuralları** 'na dokunabilirsiniz.
- 11 Bu cihazı atamak istediğiniz çocuğu seçin ve cihazı tanımlamanıza yardımcı olacak bir ad vererek **Bitti** 'ye dokunun.
- 12 İstenirse, **Uygulama Kullanımı** ve **Erişilebilirlik** seçeneklerini açın.
- 13 Görüntülenen uyarıda, Norton Family ürününü cihaz yöneticisi olarak ayarlamak için **Etkinleştir** seçeneğine tıklayın.

Norton Family uygulamasını iOS'e yüklemek için

- 1 **Norton Family'yi YÜKLE** penceresinde, önce **Evet** 'e ve ardından **Devam** 'a dokunun.
- 2 **Norton Family uygulamasını indir** 'e dokunun.
- 3 **Norton Family** uygulamasına dokunun ve yükleyin.
- 4 **Aç** seçeneğine dokunun.
- 5 Norton Family ürününün size bildirim göndermesine izin vermek için **Tamam** seçeneğine dokunun.
- 6 **Norton Lisans Sözleşmesi** 'ni ve **Gizlilik Politikası** 'nı okuyun ve ardından **Kabul et ve Devam et** 'e dokunun.
- 7 Hesap kimlik bilgileriniz ile giriş yapın.
- 8 **Çocuk Ekle** ekranında çocuğunuza ilişkin bilgileri girin ve **Ekle'ye** dokunun.
Başka bir çocuk eklemek için **Yeni çocuk ekle** seçeneğine dokunun ve **Çocuk Ekle** penceresinde çocuğunuza ilişkin bilgileri girerek **Ekle'ye** dokunun.
Avatar simgesine dokunarak çocuğunuzun profili için bir avatar seçin. Galerinizden bir resim seçebilir veya çocuğunuzun profili için anlık bir resim çekebilirsiniz.
- 9 Bu aygıtı atamak istediğiniz çocuğu seçin ve bu aygıtı tanımlamanıza yardımcı olacak bir ad verin.
- 10 **Ata** 'ya dokunun.

11 Profil yüklemek için **Yükle** 'ye dokununuz ve ekrandaki talimatları izleyiniz.

Hemen kilitle ve diğer özelliklerin çalışması için Profil kurulumu gereklidir.

12 Sınırlamaları belirlemek için ekrandaki talimatları izleyiniz.

Norton Family uygulamasını bir ebeveyn cihazına yükleme

Kurulumu tamamladıktan sonra, aşağıdaki mobil uygulamayı indirip cihazınıza yüklemeniz gerekir:

- Android cihaz: **Norton Family ebeveyn denetimi** uygulamasını yükleyiniz
- iOS cihazı: **Ebeveynler için Norton Family** uygulamasını yükleyiniz

Android'de Norton Family ebeveyn denetimi uygulamasını indirme ve yükleme

- 1 Play Store uygulamasını açınız ve **Norton Family ebeveyn denetimi**ni arayınız.
- 2 **Norton Family ebeveyn denetimi uygulamasını** seçiniz ve ardından **Yükle** 'ye dokununuz.
- 3 Yüklendikten sonra uygulamayı açınız.
- 4 **Norton Lisans Sözleşmesi** ve diğer politikaları okuyunuz ve ardından **Devam** seçeneğini tıklayınız.
- 5 Hesap kimlik bilgileriniz ile giriş yapınız.
- 6 **Ebeveyn cihazına** dokununuz. Cihazı çocuğunuzla paylaşıyorsanız, cihazı çocuğunuza vermeden önce **Çocuk moduna** geçiniz.

iOS'ta Ebeveynler için Norton Family uygulamasını indirme ve yükleme

- 1 App Store uygulamasını açınız ve **Ebeveynler için Norton Family uygulamasını** arayınız.
- 2 **Ebeveynler için Norton Family** uygulamasını seçiniz ve **Yükle** 'ye dokununuz.
- 3 Yüklendikten sonra uygulamayı açınız.

- 4 **Norton Lisans Sözleşmesi** ve diğer politikaları okuyun ve ardından **Devam** seçeneğini tıklayın.
- 5 Hesap kimlik bilgileriniz ile giriş yapın.

Ailenizle konuşma

Çevrimiçi aile güvenliğinin anahtarı iletişimdir. Bu nedenle, çocuğunuzla İnternet'in sorumlu kullanımının önemini açıklayan bir konuşma başlatabilirsiniz.

Norton Safe Web'i kullanarak bankacılık işlemleri bilgilerinizi koruyun

Norton Safe Web'deki Bankacılık İşlemleri Koruması bankacılık web sitelerinde işlem yaparken daha fazla güvenlik sağlar. Google Chrome, Mozilla Firefox veya Microsoft Edge tarayıcıyı kullanarak bir bankacılık işlemleri web sitesine erişim sağladığınızda, Norton Safe Web uzantısını yüklemenizi ya da etkinleştirmenizi için bir bildirim alırsınız. Bildirimde **Yükle** veya **Etkinleştir** öğesine tıklayın ve Norton Safe Web uzantısını yüklemek ya da etkinleştirmek için ekrandaki talimatları uygulayın.

Bildirimde **Tekrar Gösterme** seçeneğine tıklayarak veya **Ayarlar** penceresine giderek Bankacılık İşlemleri Koruması Bildirimi uyarısını kapatabilirsiniz.

Bankacılık İşlemleri Koruması Bildirimlerini açma veya kapatma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesinin altında, **Bankacılık İşlemleri Koruması Bildirimleri** satırında, **Açık / Kapalı** kaydırıcısını **Kapalı** ya da **Açık** konumuna getirin.
- 5 **Ayarlar** penceresinde **Uygula** 'ya ve ardından **Kapat** 'a tıklayın.

Cihaz Güvenliğinizi yönetme

Bu bölümde aşağıdaki konular yer almaktadır:

- Cihazınız risk altındayken ne yapılmalı?
- Bilgisayar performansını optimize etmek ve iyileştirmek için Norton'u kullanma
- Bilgisayarınızda tehditleri denetlemek için Norton taramaları çalıştırma
- Password Manager'inizi Yönetme
- Uygulamalarınızı ve dosyalarınızı saldırılardan, bilgisayar korsanlarından ve sıfır gün saldırılarından koruyun.
- Norton'u uygulamaları izleyecek ve kötü amaçlı web sitelerinin bilgisayarınıza erişimini önleyecek şekilde ayarlayın
- Norton Bulut Yedekleme'yi kullanmaya başlama
- Norton ürününüzün ayarlarını özelleştirme

Cihazınız risk altındayken ne yapılmalı?

Norton ürününün ana penceresindeki Güvenlik, İnternet Güvenliği, Yedekleme ve Performans döşemelerinin renkleri her bir kategorinin durumunu şu şekilde belirtir:

- **Yeşil** : Korunuyorsunuz.
- **Turuncu** : Bilgisayarınız ile ilgili uyarılar var.
- **Kırmızı** : Bilgisayarınız risk altında.

Not: Yedekleme kategorisi yalnızca Deluxe, Premium ve Norton 360 abonelikleriyle kullanılabilir.

Norton, korumanızı veya sistem performansınızı azaltan çoğu sorunu otomatik olarak giderir ve ana pencerede durumu Korumalı olarak gösterir. Norton, dikkatinizi gerektiren sorunları **Risk Altında** veya **Dikkat** şeklinde gösterir.

Dikkat veya Risk Altında durum göstergelerine yanıt ver

- 1 Norton'u başlatın.

Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Risk Altında** veya **Dikkat** belirten kategorinin kırmızı veya turuncu döşemesini tıklayın.

- 3 **Şimdi Düzelt** seçeneğini tıklayın ve ekrandaki talimatları izleyin.

Sorunlarınız devam ediyorsa tanı aracını çalıştırmak için **Yardım > Destek AI** seçeneğini tıklayın.

Ayrıca, bilgisayarınızın ciddi bir şekilde virüslü olduğunu düşünüyorsanız [Norton Yardım Araçları](#) seçeneğini kullanmayı deneyebilirsiniz.

LiveUpdate'i Çalıştırma

Symantec, aşağıdaki durumlarda LiveUpdate'i belirli aralıklarla çalıştırmanızı tavsiye eder:

- Eğer **Otomatik LiveUpdate** seçeneğini kapattıysanız
- Eğer bilgisayarınız uzun zaman internete bağlı değilse

Not: LiveUpdate'i çalıştırmak için, geçerli bir abonelik ve internet bağlantısına sahip olmanız gerekir.

LiveUpdate'i manuel çalıştırma

- 1 Norton'u başlatın.

Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'a tıklayın.

- 2 Norton ürünü ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **LiveUpdate** ögesine tıklayın.
- 3 **Norton LiveUpdate** penceresinde LiveUpdate başarıyla tamamlandığında **Tamam** ögesine tıklayın.

Norton'un tespit ettiği cihaz güvenlik tehditlerini görüntüleme ve düzeltme

Norton bir tehdit tespit ettiğinde, tehdidi nasıl ortadan kaldırmak istediğinizle ilgili sizden cevap gerekemediği sürece bunu otomatik olarak kaldırır. Sizden bir cevap gerekiyorsa Norton, tehdi

nasıl yanıt verileceğiyle ilgili öneriler içeren bir Tehdit Algılandı veya Güvenlik Riski uyarısı görüntüler.

Bir tarama boyunca otomatik olarak giderilen riskleri görüntüle

Bir tarama boyunca otomatik olarak giderilen riskleri görüntüle

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklatın ve ardından **Geçmiş** ögesini tıklatın.
- 3 **Güvenlik Geçmişi** penceresinde, **Göster** açılır listesinde **Çözülen Güvenlik Riskleri** ögesini seçin.
- 4 Listedenden bir risk seçin, ardından **Ayrıntılar** panelinde yapılan işlemi görüntüleyin.

Bir tarama sırasında tespit edilen çözülmemiş riskleri düzeltme

Bazı durumlarda Norton otomatik olarak bir riski gideremez ancak riski gidermek için size yapmanız için bir işlem önerir.

Bir tarama sırasında tespit edilen çözülmemiş riskleri düzeltme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklatın ve ardından **Geçmiş** ögesini tıklatın.
- 3 **Güvenlik Geçmişi** penceresinde, **Göster** açılır listesinde **Çözülmemiş Güvenlik Riskleri** ögesini seçin.
- 4 Çözülmemiş riskler görüntüleniyorsa listeden bir riski seçin.
- 5 **Ayrıntılar** panelinde **Önerilen Eylem** 'i uygulayın.

Çözülmeyen bir riski gideremezseniz Norton Power Eraser'ı çalıştır

Sisteminizin virüslü olduğunu düşünüyorsanız Norton Power Eraser'ı çalıştırın. Norton Power Eraser kaldırılması zor olan güvenlik risklerini gideren, güçlü bir zararlı program kaldırma aracıdır. Daha fazla bilgi için, Bkz: "[Bilgisayarınızda tehditleri denetlemek için Norton taramaları çalıştırma](#)" sayfa 33. bölümüne bakınız

Not: Norton Power Eraser, agresif bir kötü amaçlı yazılım kaldırma aracıdır. Bazen Norton Power Eraser kötü amaçlı yazılımlar ile birlikte gerekli dosyaları da silebilir, bu yüzden silme işleminden önce tarama sonuçlarını gözden geçirmelisiniz.

Yanlışlıkla güvenlik riski olarak tanımlanan bir dosyayı geri yükle

Norton varsayılan olarak güvenlik risklerini bilgisayarınızdan kaldırır ve karantinaya alır. Bir dosyanın yanlışlıkla kaldırıldığını düşünüyorsanız, dosyayı Karantina'dan orijinal konumuna geri yükleyebilir ve gelecek taramalardan dışlayabilirsiniz.

Bir dosyayı Karantina'dan geri yükleyin

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde önce **Güvenlik** 'i ardından **Geçmiş** 'i tıklatın.
- 3 **Güvenlik Geçmişi** penceresinde, **Göster** açılır menüsünün altında **Karantina** 'yı seçin.
- 4 Geri yüklemek istediğiniz dosyayı seçin.
- 5 **Ayrıntılar** bölümünde **Seçenekler** 'i tıklatın.
- 6 **Tehdit Algılandı** penceresinde, **Bu dosyayı kaldır ve dışla** 'yı tıklatın.
- 7 **Karantina Geri Yükleme** penceresinde **Evet** 'i tıklatın.
- 8 **Klasöre Gözet** iletişim kutusunda, dosyayı geri yüklemek istediğiniz klasörü veya sürücüyü seçin ve ardından **Tamam** 'ı tıklatın.

Not: Bir programı Norton taramalarından sadece programın güvenli olduğundan eminseniz dışarıda tutun. Örneğin, başka bir programın çalışması, güvenlik riski olarak algılanan bir programın çalışmasına bağlıysa, bu programı bilgisayarınızda tutmaya karar verebilirsiniz.

Karantinaya alınmış risk veya tehditlere göre hareket et

Karantinaya alınan öğeler bilgisayarınızın diğer öğelerinden tecrit edilir; böylece bu öğeler bilgisayarınıza yayılamaz veya yeniden bulaşamaz. Virüslü olduğunu düşündüğünüz halde, Norton tarafından risk olarak tanımlanmayan bir öğeyle karşılaşırsanız; bu öğeleri manuel olarak Karantinaya alabilirsiniz.. Ayrıca, düşük bir risk olduğunu düşünüyorsanız bir öğeyi karantinadan geri yükleyebilirsiniz. Norton, geri yüklediğiniz öğeyi onaramaz. Bununla birlikte, Norton, sonraki taramalar sırasında geri yüklenen öğeleri dezenfekte edebilir.

Bir öğeyi karantinadan çıkarma

- 1 Norton'u başlatın.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **Geçmiş** ögesine tıklayın.
- 3 **Güvenlik Geçmişi** penceresinde, açılır listeyi **Göster** ögesinde **Karantina** kategorisini seçin.
- 4 Yönetmek istediğiniz bir nesne seçin.
- 5 **Ayrıntılar** bölümünde **Seçenekler** 'i tıklayın.
Öge için eylem seçmeden önce öge hakkında daha fazla ayrıntı görüntülemek için **Daha Fazla Bilgi** bağlantısını kullanabilirsiniz. Bağlantı, riskle ilgili daha fazla bilgi içeren **Dosya Sicili** penceresini açar.
- 6 **Tehdit Bulundu** penceresinden aşağıdakilerden birini seçin:
 - **Geri yükle** : Dosyaları bilgisayarınızdaki orijinal konumuna geri yükleyin. Bu seçenek yalnızca manüel olarak karantinaya alınmış öğeler için kullanılabilir.
 - **Geri yükle ve Dosyayı dışarıda tut** Seçilen öğeyi onarmadan orijinal konumuna döndürür ve gelecekteki taramalarda tespit edilmenin dışında tutar Bu seçenek, virüs içeren ve içermeyen tehditleri saptamak için kullanılmaktadır.
 - **Geçmişten kaldır** : Seçilen öğeyi **Güvenlik Geçmişi** günlüğünden kaldırır
- 7 **Karantina Geri Yükleme** penceresinde **Evet** 'e tıklayın.
- 8 **Klasöre Gözet** iletişim kutusunda, dosyayı geri yüklemek istediğiniz klasörü veya sürücüyü seçin ve ardından **Tamam** 'a tıklayın.

Symantec'in değerlendirmesi için bir öge gönderin

Güvenlik açısından bir risk olduğunu düşündüğünüz dosyaları göndererek Norton ürününüzün etkinliğine katkıda bulunabilirsiniz. Symantec Security Response dosyayı analiz eder ve eğer riskliyse, gelecekteki koruma tanımlarına ekler.

Not: Kişisel bilgiler gönderimlere eklenmez.

- 1 Norton'u başlatın.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **Geçmiş** ögesine tıklayın.

- 3 **Güvenlik Geçmişi** penceresinde, açılır listeyi **Göster** ögesinde **Karantina** kategorisini seçin.
- 4 Yönetmek istediğiniz bir nesne seçin.
- 5 **Ayrıntılar** bölümünde **Seçenekler** 'i tıklayın.
Öge için eylem seçmeden önce öge hakkında daha fazla ayrıntı görüntülemek için **Daha Fazla Bilgi** bağlantısını kullanabilirsiniz. Bağlantı, riskle ilgili daha fazla bilgi içeren **Dosya Sicili** penceresini açar.
- 6 **Tehdit Algılandı** penceresinde, **Symantec'e Gönder** 'e tıklayın.
- 7 Görüntülenen ekranda **Tamam** 'a tıklayın.

Bir ögeyi manuel olarak karantinaya ekleme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **Geçmiş** ögesine tıklayın.
- 3 **Güvenlik Geçmişi** penceresinde, açılır listeyi **Göster** ögesinde **Karantina** kategorisini seçin.
- 4 **Karantinaya ekle** 'ye tıklayın.
- 5 **Manuel Karantina** penceresinde, karantinaya almak istediğiniz dosyayı ekleyin ve referansınız için bir açıklama girin.

Not: Çalışan işlemlerle ilişkili bir dosyayı karantinaya alırsanız, işlemler sonlandırılır. Bu nedenle, karantinaya bir dosya eklemekten önce tüm açık dosyaları ve çalışan işlemleri kapatın.

Bilgisayar performansını optimize etmek ve iyileştirmek için Norton'u kullanma

Bilgisayarınızın yavaşlamasının ve basit işlemlerin çok zaman almasının ne kadar rahatsızlık verici olduğunu biliyoruz. Bazı kullanıcılar Norton'u yükledikten sonra bilgisayarlarının performansının zayıfladığını düşünmektedir. Ancak aslında Norton, performanstan taviz vermeden dünya sınıfında bir koruma sağlayacak şekilde geliştirilmiştir.

Norton, günlük işleri daha hızlı gerçekleştirmenizi sağlayan performans yönetimi ve optimizasyon araçlarıyla bilgisayarınızın hızını da artırabilir.

Bilgisayarımın açılış süresini hızlandırma

Çoğu uygulama, bilgisayarınızı başlattığınız zaman başlatılacak şekilde yapılandırılmıştır. Bunlar hiçbir zaman kullanmadığınız, nadiren kullandığınız veya sahip olduğunuzun bir hiçbir zaman farkında olmadığını programları kapsar. Bilgisayarınızı başlattığınızda ne kadar fazla program başlatılırsa bilgisayarınızın açılması o kadar uzun sürer. **Norton Startup Manager** bilgisayarınızı daha hızlı başlatmanıza yardımcı olmak için başlangıç programlarını devre dışı bırakmanızı veya geciktirmenizi sağlar.

Başlangıç öğelerini devre dışı bırakma veya geciktirme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Performans** öğesini çift tıklayın ve ardından **Başlangıç Yöneticisi** öğesini tıklayın.
- 3 **Başlangıç Yöneticisi** penceresinde aşağıdakileri gerçekleştirebilirsiniz:
 - **Açık/Kapalı** sütununda, bilgisayarınızı başlattığınızda kullanmadığınız programların yüklenmesini önlemek için programların işaretini kaldırın.
 - **Gecikmeli Başlat** sütununda açılıştan sonra yüklenmesini istediğiniz programları seçin.
- 4 **Uygula** öğesini ve ardından **Kapat** öğesini tıklayın.

Programların ve dosyaların yüklenme süresini iyileştirme

Diski Optimize Et aracı, zamanla bilgisayarınızda dağılan dosya parçacıklarını yeniden düzenler. Daha verimli çalışmanızı sağlayacak şekilde bilgisayar performansını iyileştirir.

Diski Optimize Et'i Çalıştırın

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Performans** öğesini çift tıklayın ve ardından **Diski Optimize Et** öğesini tıklayın.
- 3 İşlem tamamlandığında **Kapat** 'ı tıklayın.

Bilgisayarımı yavaşlatan geçici dosyaları ve klasörleri kaldırma

Dosyalara göz attığınız veya dosyaları indirdiğiniz her seferde bilgisayarınız geçici dosyaları kaydeder. Bu dosyaları tutmanız gerekmez de zamanla birikebilir ve sizi yavaşlatabilir. Dosya Temizleme aracı, dağınıklığı gidererek bilgisayarınızın daha hızlı çalışmasını sağlar.

Geçici dosyaları ve klasörleri kaldırma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde, **Performans** ögesini çift tıklayın, ardından **Dosya Temizleme** ögesini tıklayın.
- 3 İşlem tamamlandığında **Kapat** 'ı tıklayın.

Bilgisayarınızı optimize etme

Bilgisayarınızın sabit disklerini optimize etmek, performansı ve güvenilirliği artırabilir. Norton, sabit disklerinizde parçalanma olup olmadığını otomatik olarak kontrol eder ve parçalanma yüzde 10'dan fazlaysa bu diskleri optimize eder. Optimizasyon gerekip gerekmediğini görmek için istediğiniz zaman en son raporları inceleyebilirsiniz.

Diske yüzde 15'ten fazla boş alan varsa Disk Optimizasyonu'nu çalıştırabilirsiniz. Disk optimizasyon işlemi sırasında, katı hal sürücüler (SSD), yalnızca Windows 8 veya üzeri işletim sistemlerinde birleştirilir.

Sabit disklerinizi optimize etme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Performans** ögesini çift tıklayın ve ardından **Diski Optimize Et** ögesini tıklayın.
- 3 Etkinlik tamamlandığında **Kapat** ögesini tıklayın.

Önyükleme biriminizi optimize etme

Önyükleme biriminizin optimizasyonu sonucunda, dosya parçaları birbirine yakın veya bitişik kümelere yerleştirilerek kullanılabilir boş disk alanı en üst düzeye çıkarılır. Sabit diskinizin sürücü kısmı bir yerdeki dosya verilerinin tümüne erişim sağlarsa, dosya bellekte daha hızlı okunur.

Önyükleme biriminizi optimize etme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Performans** ögesini çift tıklatın ve ardından **Grafikler** ögesini tıklatın.
- 3 **Grafikler** penceresinde, güvenlik durumu grafiğinin üst kısmında, **Optimize et** 'i tıklatın.

Oyun oynama veya film izleme performansını iyileştirme

Güvenlik yazılımınız çalışırken bir oyun oynadığınızda veya film izlediğinizde ekranınız en heyecanlı anda dokunuyor mu? **Tam Ekran Tespiti** aracını, müdahale edilmesi gereken bir programı çalıştırdığınızı anlayacak şekilde ayarlayabilirsiniz. Norton, korunmanızı sağlayan arka plan görevlerini yürütmeye devam etmeden önce uygulamayı kapatmanızı bekler.

Tam Ekran Tespiti aracının açık olduğundan emin olun

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Yönetim Ayarları** 'nı tıklatın.
- 4 **Etkileşimsiz Modu Ayarları** 'nın altında, **Tam Ekran Tespit** satırında, anahtarı **Açık** konumuna getirin.
- 5 **Uygula** ögesine ve ardından **Kapat** ögesini tıklatın.

Sık kullanılan uygulamalar etkinken kesintiyi önleme

Norton'un sık kullandığınız programları yavaşlattığını düşünüyorsanız **Sessiz Mod** ayarları, bu uygulamaları kullanırken Norton'un çalışmasını önler. Norton, korunmanızı sağlayan arka plan görevlerini yürütmeye devam etmeden önce bu programları kapatmanızı bekler.

Sık kullanılan programları Sessiz Mod 'da çalıştırma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Yönetim Ayarları** 'nı tıklatın.
- 4 **Etkileşimsiz Mod Ayarları** altında, **Kullanıcı Tarafından Belirlenmiş Programlar** satırında, **Yapılandır** 'ı tıklatın.
- 5 **Sessiz Mod Programları** penceresinde, **Ekle** 'yi tıklatın.

- 6 **Program Ekle** iletişim kutusunda programınıza gidin.
- 7 Dosyayı seçin **Aç** 'ı tıklayın ve ardından **Tamam** ögesini tıklayın.

Kaynakları tüketen ve bilgisayar yavaşlatan programları görüntüleme

Norton, bilgisayarınızı izler ve bir program veya işlem çok fazla kaynak kullanıyor görünüyorsa sizi uyarır. Kullanmıyorsanız bu programları kapatarak bilgisayarınızın performansını iyileştirebilirsiniz.

Kaynakları yoğun olarak kullanan işlemleri belirleme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **Performans** ögesini çift tıklayın ve ardından **Grafikler** ögesini tıklayın.
- 3 **Grafikler** penceresindeki sol panelde **Kullanım** ögesini tıklayın.
- 4 Aşağıdakilerden birini yapın:
 - CPU grafiğini görüntülemek için **CPU** sekmesini tıklayın.
 - Bellek grafiğini görüntülemek için **Bellek** sekmesini tıklayın.
- 5 Kaynak tüketimi yüksek olan işlemlerin listesini görmek için grafikteki herhangi bir noktayı tıklayın.
İşlem hakkında daha fazla bilgi edinmek için **Dosya Sicili** penceresinde işlemin adını tıklayın.

Bilgisayarınızda tehditleri denetlemek için Norton taramaları çalıştırma

Norton virüs tanımlarını otomatik olarak günceller ve bilgisayarınızda çeşitli tehditleri düzenli aralıklarla tarar. Çevrimdışı olduysanız veya bilgisayarınızda virüs olduğundan şüpheleniyorsanız aşağıdakileri manuel olarak çalıştırabilirsiniz:

- **Hızlı Tarama** ile bilgisayarınızın tehditlere karşı en fazla riske açık alanlarını analiz edebilirsiniz.
- **Tam Sistem Taraması** ile Hızlı Tarama sırasında denetlenenlere göre daha az risk altında olan uygulama, dosya ve çalışan işlemler dahil tüm sisteminizi analiz edebilirsiniz.
- **Özel Tarama** ile risk altında olduğundan şüphelendiğiniz dosya, klasör veya sürücülerini analiz edebilirsiniz.

Not: Norton'u yükledikten sonra ilk tarama, tüm sisteminizi analiz etmek için bir saat veya daha uzun sürebilir.

Hızlı Tarama, Tam Sistem Taraması veya Özel Tarama Çalıştırma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Taramalar** ögesini tıklayın.
- 3 **Taramalar** penceresinde, **Taramalar ve Görevler** 'in yanında aşağıdakilerden birini seçin:
 - **Hızlı Tarama > Git**
 - **Tam Sistem Taraması > Git**
 - **Özel Tarama > Git** 'i seçin ardından **Sürücü Tara**, **Klasör Tara** veya **Dosya Tara** 'nın karşısındaki **Çalıştır** düğmesini tıklayarak taramak istediğiniz bileşenlere gidin.
- 4 **Sonuçların Özeti** penceresinde **Son** 'u tıklayın.
Dikkat etmeniz gereken herhangi bir öge varsa **Algılanan Tehditler** penceresinde riskleri inceleyin.

Tam Sistem Taraması

Tam Sistem Taraması virüsleri ve diğer güvenlik tehditlerini kaldırmak için sisteminizde derinlemesine tarama yapar. Kullanıcının erişebildiği tüm önyüklemeye kayıtlarını, dosyaları ve çalışan işlemleri denetler. Bu tarama tüm bilgisayarınızı tarar ve daha uzun sürer.

Not: Yönetici ayrıcalıklarıyla Tam Sistem Taraması çalıştırdığınızda, yönetici ayrıcalıkları olmadan çalıştırılmasına kıyasla daha fazla dosyayı tarar.

Tam Sistem Taramasını Çalıştırın

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Taramalar** ögesini tıklayın.

- 3 **Taramalar** penceresinde **Taramalar ve Görevler** altında **Tam Sistem Taraması** 'nı tıklayın.
- 4 **Git** 'i tıklayın.

Özel Tarama

Bazen belirli bir dosyayı, taşınabilir sürücüler ve bilgisayarınızdaki sürücülerden birini ya da bilgisayarınızdaki klasör ve dosyaları taramak isteyebilirsiniz. Örneğin, çıkarılabilir bir medyayla çalışıyor ve virüsten şüpheleniyorsanız, sadece o diski tarayabilirsiniz. Ayrıca, e-posta iletişimde sıkıştırılmış bir dosya aldıysanız ve virüsten şüpheleniyorsanız, sadece o öğeyi tarayabilirsiniz.

Öğeleri tek tek tara

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** öğesini çift tıklayın ve ardından **Taramalar** öğesini tıklayın.
- 3 **Taramalar** penceresinde **Bilgisayar Taramaları** altında **Özel Tarama** 'yı tıklayın.
- 4 **Git** 'i tıklayın.
- 5 **Taramalar** penceresinde, aşağıdakilerden birini yapın:
 - Belirli sürücüler taramak için **Sürücü Tarama** 'nın yanındaki **Çalıştır** 'ı tıklayarak taramak istediğiniz sürücüler seçin ve ardından **Tara** 'yı tıklayın.
 - Belirli klasörleri taramak için **Klasör Tara** 'nın yanındaki **Çalıştır** 'ı tıklayın, taramak istediğiniz dosyaları seçin ve ardından **Tara** 'yı tıklayın.
 - Belirli dosyaları taramak için **Dosya Tara** yanındaki **Çalıştır** 'ı tıklayın, taramak istediğiniz dosyaları seçin ve ardından **Ekle** 'yi tıklayın. Ayrıca **Ctrl** tuşuna basabilir ve birden fazla dosyayı taramayı seçebilirsiniz.
- 6 **Sonuçların Özeti** penceresinde **Son** 'u tıklayın.

Herhangi bir öğeye dikkat etmeniz gerekiyorsa gözden geçirin ve önerilen işlemi uygulayın.

Norton Power Eraser taraması

Norton Power Eraser giderilmesi zor güvenlik risklerini ortadan kaldırmaya yardım edebilecek güçlü bir zararlı program kaldırma aracıdır. Norton Power Eraser normal tarama tekniklerinden daha agresif teknikler kullanır; bazen Norton Power Eraser'ın meşru bir programı kaldırmak üzere işaretleme riski vardır. Norton Power Eraser kullanırken herhangi bir dosyayı kaldırmadan önce tarama sonuçlarını dikkatle inceleyin.

Norton Power Eraser kullanarak tarama

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Taramalar** ögesini tıklayın.
- 3 **Taramalar** penceresinde **Norton Power Eraser** altında **Norton Power Eraser** 'ı tıklayın.
- 4 **Git** 'i tıklayın.
- 5 **Norton Power Eraser** penceresinde **Tamam** 'ı tıklayın.
- 6 **Norton Power Eraser** penceresinde **Gelişmiş Taramalar** 'ı tıklayın.
- 7 **Sistem Taraması** 'nı tıklayın.
- 8 Tespit edilen güvenlik risklerini onarmak için tarama sonuçlarını görüntüleyin ve ekrandaki talimatları yerine getirin.

Özel Norton taramaları oluşturma

Varsayılan Norton otomatik tarama ayarları çoğu kullanıcı için yeterli olmasına karşın bazı kullanıcılar belirledikleri zamanlarda belirli sürücüler, klasörleri veya dosyaları tarama seçeneklerini özelleştirmek isteyebilir.

Özel tarama oluşturma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Taramalar** ögesini tıklayın.
- 3 **Taramalar** penceresinde **Taramalar ve Görevler** bölümünde **Özel Tarama** 'yı tıklayıp **Git** 'i tıklayın.
- 4 **Taramalar** penceresinde, **Tarama Oluştur** 'u tıklayın.
- 5 **Yeni Tarama** penceresinde, **Tarama Adı** 'nın karşısında özel tarama için bir ad yazın ve aşağıdaki ayarları ekleyin:
 - **Öğeleri Tara** sekmesinden **Sürücüler Ekle**, **Klasörleri Ekle** ya da **Dosyaları Ekle** seçeneklerini tıklayarak taramaya dahil etmek istediğiniz bileşenlere gidin.
 - **Tarama Zamanlama** sekmesinde, Taramayı ne zaman çalıştırmak istiyorsunuz? bölümünde bir aralık seçin ve ardından zamanlama seçeneklerini seçin.
Tarama çalıştır bölümünde seçeneklerden seçim yapın. Çoğu kullanıcı için tüm kutuları işaretli bırakmak en iyisidir. Böylece taramalar sadece bilgisayarınızı kullanmadığınız

ve pil gücü kullanmadığınız zamanlarda çalışır ve bilgisayarınızın tarama sırasında uyku moduna geçmesini önler.

- **Tarama Seçenekleri** sekmesinde, tarama sırasında sıkıştırılmış dosyalar ve düşük riskli tehditler için davranışları özelleştirmek amacıyla anahtarları kaydırın.

6 **Kaydet** 'i tıklatın.

Norton özel taramasını düzenleme veya silme

Taramayı yeniden adlandırmak, dosya eklemek veya kaldırmak ya da zamanlamayı değiştirmek için oluşturduğunuz özel taramayı düzenleyebilirsiniz. Artık tarama gerçekleştirmeniz gerekmiyorsa silebilirsiniz.

Özel taramayı düzenleme veya silme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklatın ve ardından **Taramalar** ögesini tıklatın.
- 3 **Taramalar** penceresinde **Taramalar ve Görevler** bölümünde **Özel Tarama** 'yı tıklatıp **Git** 'i tıklatın.
- 4 **Taramalar** penceresinde, **Taramayı Düzenle** sütununda değiştirmek istediğiniz özel taramanın yanında aşağıdakilerden birini yapın:
 - Düzenle simgesini tıklatın ve ardından **Taramayı Düzenle** penceresinde, anahtarlarla tarama seçeneklerini açın veya kapatın. Çoğu kullanıcı için varsayılan ayarlar iyi çalışır. Özel ayarları kaldırmak için **Varsayılanları Kullan** 'ı tıklatın.
 - Çöp kutusu simgesini tıklatın ve özel taramayı silmek istediğinizi onaylamak için **Evet** 'i tıklatın.
- 5 **Kaydet** 'i tıklatın.

Norton taramalarını zamanlama

Norton bilgisayardan uzak olduğunuzu zamanı tespit eder ve otomatik olarak tarama çalıştırarak sistemde tehditlerin düzenli olarak izlenmesini sağlar. Hızlı Tarama, Tam Sistem Taraması veya Özel Tarama'yı seçtiğiniz zamanlarda gerçekleştirecek şekilde zamanlayabilirsiniz.

Norton Hızlı Tarama, Tam Sistem Taraması veya Özel Taramayı Zamanlama

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklatın ve ardından **Taramalar** ögesini tıklatın.

- 3 **Taramalar** penceresinde **Bilgisayar Taramaları** altında **Özel Tarama** 'yı tıklayın.
- 4 **Git** 'i tıklayın.
- 5 **Taramalar** penceresinde, **Taramayı Düzenle** sütununda Hızlı Tarama, Tam Sistem Taraması veya daha önce oluşturduğunuz Özel Tarama yanındaki düzenle simgesini tıklayın.
- 6 **Taramayı Düzenle** penceresinde **Tarama Programlama** sekmesinde:
 - **Taramayı ne zaman çalıştırmak istiyorsunuz?** bölümünde bir aralık seçin ve ardından zamanlama seçeneklerini seçin.
 - **Tarama çalıştır** bölümünde seçeneklerden seçim yapın. Çoğu kullanıcı için tüm kutuları işaretli bırakmak en iyisidir. Böylece taramalar sadece bilgisayarınızı kullanmadığınız ve pil gücü kullanmadığınız zamanlarda çalışır ve bilgisayarınızın tarama sırasında uyku moduna geçmesini önler.
- 7 **İleri** 'yi tıklayın.
- 8 **Tarama Seçenekleri** sekmesinde **Kaydet** 'i tıklayın.

Norton SONAR korumasının tespit ettiği gerçek zamanlı tehditleri görüntüleme

Symantec Online Network for Advanced Response (SONAR), tehditlere karşı gerçek zamanlı koruma sağlar ve bilinmeyen güvenlik risklerini proaktif olarak tespit eder. SONAR, yeni çıkan tehditleri uygulamaların çalışma biçimine göre teşhis eder, bu yöntem imzaya dayalı klasik tehdit tespitinden daha hızlıdır. Henüz virüs tanımları LiveUpdate ile alınmamışken bile, sizi kötü amaçlı kodlara karşı korumaya yardımcı olur.

SONAR Koruması işlevini her zaman açık tutmalısınız.

Not: Otomatik Koruma kapatıldığında, SONAR Koruması da devre dışı bırakılır ve bilgisayarınız gelişen tehditlere karşı korunmaz.

SONAR Koruması'nın açık olduğundan emin olun

- 1 Norton'u başlatın.
 - Aygıt Güvenliği** 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'ü tıklayın.

- 4 **Otomatik Koruma** sekmesinde, **Gerçek Zamanlı Koruma** altında, **SONAR Koruması** anahtarını **Kapalı** veya **Açık** konumuna getirin.

Kısa bir süre bile anahtarı kapalı konuma getirirseniz gerçek zamanlı koruma özellikleri devre dışı kalır ve bilgisayarınız riske açık hale gelir.

- 5 **Uygula** seçeneğini tıklatın.
- 6 Anahtarı kapalı konuma getirdiyse SONAR'ın ne kadar süreyle devre dışı kalacağını seçin ve **Tamam** 'ı tıklatın.
- 7 **Ayarlar** penceresinde, **Kapat** seçeneğini tıklatın.

SONAR tarafından tespit edilen riskleri görüntüle

- 1 Norton'u başlatın.
- Aygıt Güvenliği** 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklatın ve ardından **Geçmiş** ögesini tıklatın.
- 3 **Güvenlik Geçmişi** penceresinde, açılanlar listesinde **SONAR Etkinliği** 'ni seçin.
- 4 Gösterilen çözülmemiş riskler varsa listeden bir risk seçin.
- 5 **Ayrıntılar** panelinde **Önerilen Eylem** 'i uygulayın.

Ayrıca bu kategoride, bilgisayarınızın yapılandırmasını veya ayarlarını değiştiren etkinlikler de listelenir. Bu kategoriye ait **Daha Fazla Ayrıntı** seçeneği, bu etkinliğin etkilediği kaynaklar hakkında bilgi verir.

Dosya ve klasörleri Norton Auto-Protect, SONAR ve Download Intelligence taramalarından dışlama

Norton'u belirli programları Oto Koruma taramalarından ve SONAR taramalarından hariç tutacak şekilde yapılandırabilirsiniz. Virüsleri ve diğer yüksek riskli güvenlik tehditlerini taramanın dışında tutmak için, **Tarama Dışlamaları** penceresini ve **Gerçek Zamanlı Koruma Dışlamaları** penceresini kullanabilirsiniz. Dışarıda bırakma listesine bir dosya ya da klasör eklediğinizde, Norton güvenlik riskleri taraması yaptığında, bu dosya ya da klasörü görmezden gelir.

Bir dosyayı Download Intelligence'in dışında bırakmak için, bir klasör seçmeli ve dosyayı seçilen klasöre indirmeniz gereklidir. Örneğin, güvenilir olmayan yürütülebilir dosyayı bu klasöre indirdiğinizde, Norton dosyayı indirmenize olanak sağlar ve bu dosyayı bilgisayardan kaldırmaz. İndirme Bilgi Merkezi hariç bırakmaları için yeni özel bir klasör oluşturmanız gereklidir.

Not: Norton taramalarından bir dosyayı hariç tuttuğunuzda bilgisayarınızın koruma düzeyi azalır ve bunu yalnızca özel bir ihtiyacınız olduğunda kullanmalısınız. Yalnızca, virüslü olmadığından emin olduğunuz öğeleri tarama dışında tutmalısınız.

Yüksek riskli güvenlik tehditlerini tarama dışında tut

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'e tıklayın.
- 4 **Antivirüs** ayarları penceresinde, **Taramalar ve Riskler** sekmesine tıklayın.
- 5 **Dışlamalar / Düşük Riskler** penceresinde, aşağıdakilerden birini yapın:
 - **Taramaların Dışında Tutulacak Öğeler** satırında **Yapılandır** 'a tıklayın.
 - **Auto-Protect, Komut Dosyası, SONAR ve İndirme Bilgi Merkezi Tespitinin Dışında Bırakılacak öğelerde** satırında, **Yapılandır** 'a tıklayın.
- 6 Çıkan pencereden **Klasör Ekle** 'ye veya **Dosya Ekle** 'ye tıklayın.
Dışlamaları yerel sürücülere, klasörlere, dosya gruplarına, tekli dosyalara veya ağ sürücülerine atayabilirsiniz. Bununla birlikte Norton ağ üzerindeki dosyalar için dışlamaları desteklemez. Dışlama listesine bir ağ sürücüsü ekliyorsanız, sürücünün bilgisayarınıza bağlı olduğundan emin olun.
- 7 **Öğe Ekle** iletişim kutusunda göz at simgesine tıklayın.
- 8 Çıkan iletişim kutusunda, taramadan dışlamak istediğiniz öğeyi seçin.
Klasör eklerken alt klasörlerin eklenip eklenmeyeceğini belirleyebilirsiniz.
- 9 **Tamam** 'a tıklayın.
- 10 **Öğe Ekle** iletişim kutusunda, **Tamam** 'a tıklayın.
- 11 Açılan pencerede, **Uygula** 'ya tıklayın ve ardından **Tamam** 'a tıklayın.

Düşük risk imzalı dosyaları Norton taramaları dışında bırakma

Norton İmza Dışlamaları, Norton taramalarının dışında tutulacak bilinen belirli güvenlik risklerini seçmenize olanak sağlar. Ücretsiz bir oyun gibi meşru bir uygulamanın çalışması için reklam yazılımı gibi başka bir program gerekiyorsa sizin açınızdan risk oluştursa bile reklam yazılımını tutmaya karar verebilirsiniz. Ayrıca gelecekteki taramalarda program hakkında bildirim almamayı da seçebilirsiniz.

Not: Dışlamalar koruma düzeyinizi düşürür ve yalnızca özel bir ihtiyacınız olduğunda ve bilinen tehditleri Norton taramaları dışında tutmanın olası riskini tam olarak kavradığınızda kullanılmalıdır.

İmza Dışlamaları'na düşük riskli bir imza ekleme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'e tıklayın.
- 4 **Antivirüs** ayarları penceresinde, **Taramalar ve Riskler** sekmesini tıklatın.
- 5 **Tüm Tespitlerin Dışında Tutulacak İmzalar** satırındaki **Dışlamalar / Düşük Riskler** altında **Yapılandır** 'ı tıklatın.
- 6 **İmza Dışlamaları** penceresinde, **Ekle** 'yi tıklatın.
- 7 **Güvenlik Riskleri** penceresinde dışlamak istediğiniz güvenlik riskini tıklatın ve ardından **Ekle** 'yi tıklatın.
- 8 **İmza Dışlamaları** penceresinde **Uygula** 'yı ve sonra **Tamam** 'ı tıklatın.

Otomatik görevleri aç veya kapat

Norton otomatik görevleri, bilgisayarınızı korumak için sesizce çalışacak şekilde yürütür. Bu otomatik görevler virüsleri taramayı, İnternet bağlantınızı izlemeyi, koruma güncellemelerini indirmeyi ve diğer önemli görevleri içerir. Bu etkinlikler bilgisayarınız açıkken arka planda çalışır.

Eğer bir öğeyle ilgili yapılması gereken bir işlem varsa, Norton mevcut durumu ya da gereken işlemi içeren bir mesaj gösterir. Eğer hiçbir mesaj görmüyorsanız, bilgisayarınız korunuyor demektir.

Norton'u istediğiniz zaman açıp PC'nizin durumunu hemen görebilir veya koruma ayrıntılarını görüntüleyebilirsiniz.

Bir arka plan etkinliği sürerken, Norton sizi görev çubuğunun en sağında bulunan bildirim alanında bir iletiyle uyarır. En son etkinliklerin sonuçlarını, Norton ana penceresini sonraki açışınızda görebilirsiniz.

Otomatik görevleri aç veya kapat

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **Görev Zamanlama** 'ya tıklayın.
- 4 **Görev Zamanlama** penceresinde, **Otomatik Görevler** sekmesinde, aşağıdakileri yapın:
 - Otomatik olarak çalışmasını istediğiniz özelliği işaretleyin.
Özelliklerin tümünü bir seferde işaretlemek için **Görevler** onay kutusunu işaretleyin.

- Otomatik olarak çalışmasını istemediğiniz özelliğin işaretini kaldırın. Özelliklerin tümünün işaretini bir seferde kaldırmak için **Görevler** onay kutusundaki işareti kaldırın.

5 **Uygula** 'ya ve sonra **Kapat** 'a tıklayın.

Özel görev çalıştırma

Norton sisteminizi otomatik olarak denetler ve sisteminizi güvende tutan en iyi ayarları seçer. Bununla birlikte, bazı özel görevleri çalıştırabilirsiniz: **Özel Görevler** penceresindeki seçenekleri kullanarak, çalıştırmak istediğiniz özel görevleri seçebilirsiniz.

Bir seferlik taramalarda kendi görev kombinasyonunuzu seçebilirsiniz. LiveUpdate'i çalıştırabilir, verilerinizi yedekleyebilir, tarama geçmişini temizleyebilir, diskte biriken gereksiz dosyaları temizleyerek boş disk alanı oluşturabilir ve disklerinizi optimize edebilirsiniz.

Özel görev çalıştırma

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Taramalar** ögesini tıklayın.
- 3 **Taramalar** penceresinde **Taramalar ve Görevler** bölümünde **Özel Görev** 'i tıklayıp ardından **Git** 'i tıklayın.
- 4 **Özel Görevler** penceresinde, çalıştırmak istediğiniz görevleri işaretleyin.
Tüm görevleri seçmek için, **Görevler** seçeneğini işaretleyin.
- 5 **Git** 'i tıklayın.

Güvenlik ve performans taramalarını zamanla

Norton programının sisteminizdeki güvenlik ve performans sorunlarını otomatik olarak incelemesi için Görev Zamanlama ayarlarını kullanın. Norton programının bu incelemeleri ne zaman ve hangi sıklıkta yapması gerektiğini belirtebilirsiniz.

Güvenlik ve performans taramalarını zamanlamak için şu seçenekleri kullanabilirsiniz:

Otomatik (Önerilen)

PC'niz boşta olduğunda PC'nizdeki güvenlik ve performans sorunları incelenir.

Bu ayar maksimum koruma sağlar.

Haftalık	PC'nizdeki güvenlik ve performans sorunları haftada bir veya birkaç kez incelenir. Taramanın gerçekleştirileceği günleri ve saatleri seçebilirsiniz.
Aylık	PC'nizdeki güvenlik ve performans sorunları ayda bir kez incelenir. Taramanın ayın hangi gününde ve günün hangi saatinde gerçekleştirileceğini seçebilirsiniz.
Manuel Zamanlama	PC'nizde zamanlanmış bir güvenlik veya performans taraması gerçekleştirilmez. Bu seçeneği tercih ederseniz, korumayı sürdürmek için, PC'nizde güvenlik ve performans taramalarını belirli aralıklarla düzenli olarak gerçekleştirmeniz gerekir.

Önemli işlemlerinizi bilgisayarınız boştayken yapılacak şekilde zamanlarsanız bilgisayarınızın performansı en üst düzeye çıkar. Taramalarınızı haftalık veya aylık olarak gerçekleştirecek şekilde zamanlar ve **Yalnızca boştayken çalıştır** seçeneğini işaretlerseniz, Norton bilgisayarınızı boştayken tatar. Symantec, bilgisayarınızdan daha iyi performans alabilmeniz için, **Yalnızca boştayken çalıştır** 'ı işaretlemenizi önerir.

Güvenlik ve performans taramalarını zamanla

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **Görev Zamanlama** 'yı tıklatın.
- 4 **Zamanlama** bölümündeki **Zamanlama** sekmesinden bir seçenek belirleyin.
Haftalık veya **Aylık** seçeneğine tıkladığınızda, otomatik görevlerin çalıştırılacağı gün ve saati seçmeniz gerekir. Otomatik görevlerin yalnızca PC boştayken çalıştırılması gerektiğini belirtme seçeneğine de sahipsiniz.
- 5 **Uygula** 'ya ve sonra **Kapat** 'ı tıklatın.

PC'nizi etkileyen kötü amaçlı işlemleri engellemek için Veri Koruyucu'yu yapılandırma

Veri Koruyucu, PC'nizi dengesizleştirmek, verilerinizi bozmak ve/veya çalmak, kötü amaçlı varlıkları sistemlere yaymak isteyen kötü amaçlı işlemlerden korur. Bir işlemi güvenli, kötü niyetli veya bilinmeyen olarak tanımlamak için Norton itibar teknolojisini kullanır. Tanımlamaya dayanarak, kötü amaçlı işlemlerin PC'nizde herhangi bir işlem gerçekleştirmesini engeller.

Dosyaları o kadar agresif korur ki çalışma sırasında kötü amaçlı bir dosyaya enjekte edilirse güvenli işlemler bile engellenir. Varsayılan olarak Veri Koruyucu açıktır ve önceden ayarlanmış klasörleri ve uzantıları korur. Durumunuza bağlı olarak, daha fazla klasör ve/veya uzantı ekleyebilir ve ayrıca tarama ve koruma işlemlerini de hariç tutabilirsiniz.

Uyarı: Bu özelliğin kapatılması bilgisayar korumanızı azaltır. Bu nedenle bu özelliği daima açık tutmanızı öneririz. Ancak kapatmak isterseniz, geçici olarak kapatın ve yeniden açıldığından emin olun.

Veri Koruyucu'yu açma veya kapatma

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde, **Ayarlar > Antivirüs** 'ü tıklayın.
- 3 **Antivirüs** ayarları penceresinde **Veri Koruyucu** sekmesini tıklayın.
- 4 **Veri Koruyucu** satırında, **Açık/Kapalı** anahtarını **Açık** veya **Kapalı** konuma getirin.
- 5 **Bildirimler Göster** satırında aşağıdakilerden birini yapın:
 - Veri Koruyucu'nun bir tehdit engellediği her seferde size bildirimde bulunması için düğmeyi **Açık** konuma getirin.
 - Bildirimleri engellemek için anahtarı **Kapalı** konuma getirin. **Güvenlik Geçmişi** penceresinden engellenen tehditlerin ayrıntılarını görebilirsiniz.
Güvenlik Geçmişi penceresine erişmek için Norton ana penceresinde önce **Güvenlik**, ardından **Geçmiş > Veri Koruyucu** öğelerini çift tıklayın.
- 6 **Uygula** seçeneğini tıklayın.
- 7 İstenirse, Veri Koruyucu özelliğinin kapalı kalmasını istediğiniz süreyi seçin ve ardından **Tamam** 'ı tıklayın.

Veri Koruyucu koruması için bir klasör ekleme veya düzenleme

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde, **Ayarlar > Antivirüs** 'ü tıklayın.
- 3 **Antivirüs** ayarları penceresinde **Veri Koruyucu** sekmesini tıklayın.
- 4 **Veri Koruyucu** satırında, **Açık/Kapalı** anahtarını **Açık** konuma getirin.
- 5 Bir klasör eklemek veya düzenlemek için aşağıdakileri yapın:
 - **Korunan Klasörler** 'in yanında, **Yapılandır** 'ı tıklayın.
 - **Korunan Klasörler** penceresinde aşağıdakileri yapın:

- Yeni bir öge eklemek için **Ekle** 'yi tıklatın.
- Mevcut bir ögeyi değiştirmek için ögeyi seçin ve ardından değiştirmek için **Düzenle** 'yi tıklatın.

Not: Önceden ayarlanmış bir klasörü düzenleyemezsiniz.

- Gezinmek ve klasör seçmek için **Öge Ekle** veya **Öge Düzenle** penceresinde



simgesini tıklatın.

- Alt klasörleri dahil etmek için onay kutusunu tıklatın.
- **Tamam** 'ı tıklatın.

6 Uygula 'yı ve ardından **Tamam** 'ı tıklatın.

Veri Koruyucu koruması için uzantı ekleme

1 Norton'u başlatın.

Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklatın.

2 Norton ürünü ana penceresinde, **Ayarlar** > **Antivirüs** 'ü tıklatın.

3 **Antivirüs** ayarları penceresinde **Veri Koruyucu** sekmesini tıklatın.

4 **Veri Koruyucu** satırında, **Açık/Kapalı** anahtarını **Açık** konuma getirin.

5 Bir uzantı eklemek için aşağıdakileri yapın:

- **Korunan Dosya Türleri** 'nin yanında **Yapılandır** 'ı tıklatın.
- **Korunan Dosya Türleri** penceresinde **Ekle** 'yi tıklatın.
- **Öge Ekle** penceresinde, korumak istediğiniz uzantıyı yazın. Örneğin, yürütülebilir dosyaları korumak istiyorsanız, kutuya .exe yazın. Bilgisayarın herhangi bir yerindeki .exe uzantılı tüm dosyalar korunur.
- **Tamam** 'ı tıklatın.

6 Uygula 'yı ve ardından **Tamam** 'ı tıklatın.

Veri Koruyucu'dan bir klasör veya uzantıyı kaldırma

1 Norton'u başlatın.

Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklatın.

2 Norton ürünü ana penceresinde, **Ayarlar** > **Antivirüs** 'ü tıklatın.

- 3 **Antivirüs** ayarları penceresinde **Veri Koruyucu** sekmesini tıklayın.
- 4 **Veri Koruyucu** satırında, **Açık/Kapalı** anahtarını **Açık** konuma getirin.
- 5 **Korunan Klasörler** veya **Korunan Dosya Türleri** 'nin yanında, **Yapılandır** 'ı tıklayın.
- 6 **Korunan Klasörler** veya **Korunan Dosya Türleri** penceresinde, kaldırmak istediğiniz öğeyi seçin.

Not: Ön ayarlı bir klasörü veya uzantıyı kaldıramazsınız.

- 7 **Kaldır** 'ı tıklayın.
- 8 **Uygula** 'yı ve ardından **Tamam** 'ı tıklayın.

Veri Koruyucu dışlamaya bir işlem ekleme veya kaldırma

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde, **Ayarlar** > **Antivirüs** 'ü tıklayın.
- 3 **Antivirüs** ayarları penceresinde **Veri Koruyucu** sekmesini tıklayın.
- 4 **Veri Koruyucu** satırında, **Açık/Kapalı** anahtarını **Açık** konuma getirin.
- 5 **İşlem Dışlama** satırında, **Yapılandır** 'ı tıklayın ve aşağıdakileri yapın:
 - Veri Koruyucu'dan dışlanacak bir işlem eklemek için **Ekle** 'yi tıklayın ve ardından işlemi seçin.
 - Bir işlemin Veri Koruyucu'dan dışlanmaması için işlemi tıklayın ve ardından **Kaldır** 'ı tıklayın.
- 6 **Uygula** 'yı ve ardından **Tamam** 'ı tıklayın.

Kimlik avı girişimlerinde kullanılabilecek komut dosyalarını kaldırmak için Norton'u ayarlayın

Komut Dosyası Kontrolü, kimlik avı e-postalarında ek olarak aldığınız veya indirdiğiniz zararlı programlardan korunmanıza yardımcı olur. Varsayılan olarak şüpheli komut dosyalarını kaldırır ve dosyaları temizler.**. Ancak, orijinal dosyaları komut dosyasıyla geri yükleyebilir ve Norton'un gömülü komut dosyaları içeren belgeleri nasıl yöneteceğini yapılandırabilirsiniz.

Not: **Chrome, Edge ve Internet Explorer tarayıcıları için bu özellik Windows 10 RS2 ve sonraki sürümlerinde desteklenir.

Komut dosyaları belgeleri dinamik ve etkileşimli hale getirmek için kullanılır. Her ne kadar komut dosyalarının temel amacı belge deneyimini geliştirmek olsa da, siber suçlular, bilgisayarınızda kötü amaçlı yazılımları gizlemek için kullanabilir. Komut dosyaları genellikle bir belgenin işlevi için önemli değildir ve birçok yazılım programı bunları varsayılan olarak devre dışı bırakır.

Kötü amaçlı içerik içermediklerinden eminseniz, Norton'u belirli dosyaları Komut Dosyası Kontrolü dışında tutması için ayarlayabilirsiniz. Daha fazla bilgi için, Bkz: "[Dosya ve klasörleri Norton Auto-Protect, SONAR ve Download Intelligence taramalarından dışlama](#)" sayfa 39. Temizlenen dosyaları değiştirerek orijinal dosyaları geri yükleyebilirsiniz. Yalnızca, kötü amaçlı içerik içermediklerinden emin olduğunuz dosyaları dışarıda bırakmalısınız.

Komut Dosyası Denetimi, dosyaların davranışına göre olası tehditleri tanımlar. Norton, gömülü kod içeren bir belgeyi açtığınızda olası tehlikeli bir etkinlik tespit ederse, uygulamanın komut dosyasını çalıştırmasını engeller. Belgeleri katıştırılmış komut dosyası ile açtığınızda Norton'un komut dosyalarını nasıl yöneteceğini yapılandırabilirsiniz.

Özgün dosyayı geri yükleyin

- 1 Norton'u Başlat.
Cihaz Güvenliği satırında **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **Geçmiş** ögesine tıklayın.
- 3 **Güvenlik Geçmişi** penceresinde, **Açılır listeyi Göster**'den **Komut Dosyası Kontrolünü** seçin.
- 4 **Komut Dosyası görünümünden**, geri yüklemek istediğiniz içeriği seçin.
- 5 Sağ bölmede, **Ayrıntılar** altında, **Geri Yükle** ögesine tıklayın.
- 6 **Komut Dosyası Geri Yükleme** penceresinde, **Evet** 'e tıklayın.
- 7 Görüntülenen istemde **Evet** 'i seçin.
- 8 **Güvenlik Geçmişi** penceresinde, **Kapat** 'a tıklayın.

Komut Dosyası Kontrolü açın veya kapatın

- 1 Norton'u Başlat.
Cihaz Güvenliği satırında **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'ü tıklayın.
- 4 Antivirüs **ayarları penceresinde**, **Komut Dosyası** sekmesine tıklayın.
- 5 **Belgeleri indirirken komut dosyalarını kaldırın** satırında, **Açık/Kapalı** anahtarını **Açık** veya **Kapalı** konuma getirin.

Kapatırsanız şunları yapın:

- **Güvenlik Talebi** penceresinde, **Süreyi seçin** açılır listesinden kapatmak istediğiniz süreyi seçin.

- 6 **Belgeleri açarken komut dosyalarını engelleme** satırında, **Açık/Kapalı** anahtarını **Açık** veya **Kapalı** konuma getirin.

Kapatırsanız şunları yapın:

- **Güvenlik Talebi** penceresinde, **Süreyi seçin** açılır listesinden kapatmak istediğiniz süreyi seçin.

- 7 **Ayarlar** penceresinde **Uygula** 'ya ve ardından **Kapat** 'a tıklayın.

Tüm Komut Dosyası Kontrol öğelerini kalıcı olarak silin

- 1 Norton'u Başlat.
Cihaz Güvenliği satırında **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Güvenlik Geçmişi** penceresinde, **Açılır listeyi** göster seçeneğinden **Komut Dosyasını** seçin.
- 4 **Komut Dosyası Kontrolü** penceresinde, görünümünde, **Girdileri Temizle** 'ye tıklayın.
- 5 **Girdileri Temizle** penceresinde **Evet** 'e tıklayın.
- 6 Onay iletişim kutusunda **Evet** 'e tıklayın.
- 7 **Güvenlik Geçmişi** penceresinde, **Kapat** 'a tıklayın.

Norton'un gömülü komut dosyası içeren belgeleri nasıl yöneteceğini yapılandırma

- 1 Norton'u Başlat.
Cihaz Güvenliği satırında **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'ü tıklatın.
- 4 Antivirüs **ayarları** penceresinde, **Komut Dosyası** sekmesine tıklayın.
- 5 **Belgeleri açarken komut dosyalarını engelle** altında, **Microsoft Office** satırında, **Yapılandır** 'a tıklayın.
- 6 **Microsoft Office Tercihleri** penceresinde, **Eylemler** 'in altında, Norton'un her uygulama için gerçekleştirmesini istediğiniz eylemi seçin.

Seçenekleriniz şunlardır:

- **Engelle**

- **İzin Ver**
- **Bana Sor**

Her uygulama için farklı bir işlem seçebilirsiniz.

- 7 Açılan onay penceresinden **Tamam** 'a tıklayın.
- 8 **Microsoft Office Tercihleri** penceresinde **Uygula** 'yı ve sonra **Tamam** 'a tıklayın.
- 9 **Adobe Belge** satırında, Norton'un Adobe belgeleri için gerçekleştirmesini istediğiniz işlemi seçin.
- 10 **Ayarlar** penceresinde **Uygula** 'ya ve ardından **Kapat** 'a tıklayın.

SSS: Norton Komut Dosyası Kontrolü

Komut dosyaları nedir ve Norton neden bunları kaldırır?

Komut dosyaları belgeleri dinamik ve etkileşimli hale getirmek için kullanılır. Ayrıca bazı görevleri otomatikleştirerek işlevsellik ekleyebilirler.

Komut dosyaları şunları içerebilir:

- ActiveX denetimleri
- Eklentiler
- Veri bağlantıları
- Makrolar
- Bağlantılı nesne bağlama ve gömülü OLE dosyaları
- Renk teması dosyaları

Her ne kadar komut dosyalarının temel amacı belge deneyimini geliştirmek olsa da, siber suçlular, bilgisayarınızda kötü amaçlı yazılımları gizlemek için kimlik avı girişimlerinde kullanabilir. Komut dosyaları genellikle bir belgenin işlevi için önemli değildir ve birçok yazılım programı bunları varsayılan olarak devre dışı bırakır.

Komut dosyalarını kaldırmak sorunlara neden olabilir mi?

Değişir. Bir belge etkileşim sağlamak veya ek içerik indirmek için komut dosyalarına dayanıyorsa, bu durumda komut dosyası kaldırılırsa bu işlev çalışmaz.

Komut Dosyası Kontrolü'nü kapatsam bile hala korunur muyum?

Norton, komut dosyalarında gömülü olanlar da dahil olmak üzere kötü amaçlı yazılımların bir belgede ne zaman çalıştırılmaya çalışılacağını algılar, böylece korunursunuz. Komut Dosyası

Kontrolü, komut dosyalarını kaldırarak ve belgeleri temizleyerek ekstra bir güvenlik katmanı sağlar.

Orijinal dosyayı nasıl geri alabilirim?

- 1 Norton'u Başlat.
Cihaz Güvenliği satırında **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Güvenlik** ögesine çift tıklayın ve ardından **Geçmiş** ögesine tıklayın.
- 3 **Güvenlik Geçmişi** penceresinde, **Açılır listeyi** göster seçeneğinden **Komut Dosyası Kontrolünü** seçin.
- 4 **Komut Dosyası görünümünden**, geri yüklemek istediğiniz aktif içeriği seçin.
- 5 Sağ bölmede, **Ayrıntılar** altında, **Geri Yükle** ögesine tıklayın.
- 6 **Komut Dosyası Geri Yükleme** penceresinde, **Evet** 'e tıklayın.
- 7 Görüntülenen istemde **Evet** 'i seçin.
- 8 **Güvenlik Geçmişi** penceresinde, **Kapat** 'a tıklayın.

Norton, olası bir tehdit tespit ederse hangi uygulamaları engeller?

Norton, potansiyel olarak tehlikeli bir etkinlik tespit ederse aşağıdaki uygulamaların açılmasını engeller:

- Microsoft Excel
- Microsoft Powerpoint
- Microsoft Word

Norton, bu uygulamalara ek olarak Adobe belgelerinden, ortak geliştirici hizmet programlarından, Windows Yönetim Araçları (WMI) araçlarından, komut satırı arabirimlerinden ve komut dosyası arabirimlerinden komut dosyalarını algılar ve engeller.

Belgeleri indirirken komut dosyalarını engelleme ve belgeleri açma: farkı nedir?

Katıştırılmış komut dosyası içeren bir belge indirdiğinizde, Script Kontrolü şüpheli komut dosyalarını algılamak için **Auto-Protect** özelliğini kullanır. **Auto-Protect**, indirdiğiniz bir dosyanın güvenliğini belirlemek için Norton programının virüs tanımı güncellemeleri sırasında aldığı tehdit imzalarını ve diğer güvenlik güncellemelerini kullanır.

Gömülü kod içeren bir belgeyi açtığınızda, Komut Dosyası Denetimi, tehlikeli olabilecek herhangi bir etkinliği tespit etmek için **SONAR Koruması** kullanır. Dosya davranışına dayanarak olası tehditleri tanımlar ve uygulamanın komut dosyasını çalıştırmasını engeller.

Not: Chrome, Edge ve Internet Explorer tarayıcıları için, **Belgeleri indirirken komut dosyalarını kaldır** seçeneği yalnızca Windows 10 RS2 ve sonraki sürümlerinde kullanılabilir.

Norton, hem Komut Dosyası Denetimi seçeneklerinin her zaman açık kalmasını önerir.

Password Manager'inizi Yönetme

Password Manager, parolalarınızı yönetmenize yardım eder ve çevrimiçi işlem yaparken ek güvenlik sağlar. Adresler, doğum tarihi, ve kredi kartı bilgisi gibi kişisel bilgilerinizi yönetmek için Password Manager'daki çeşitli özellikleri kullanabilirsiniz.

Password Manager'ı Google Chrome'daki Eklentiler sayfasından veya Mozilla Firefox'taki Eklentiler sayfasından kapatabilir veya açabilirsiniz.

Password Manager'ı Google Chrome'daki Eklentiler sayfasından kapatma veya açma

- 1 Google Chrome'u başlatın.
- 2 Sağ üst köşedeki **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** seçeneğinde **Diğer araçlar** 'a gidin ve **Uzantılar** 'a tıklayın.
- 4 **Uzantılar** sayfasında **Norton Password Manager** etkinse **Etkin** kutusunun işaretini kaldırın.
Uzantılar sayfasında Norton Password Manager devre dışıysa **Etkin** kutusunu işaretleyin
- 5 Google Chrome'u Yeniden Başlatın

Mozilla Firefox'ta Password Manager'ı Eklentiler sayfasından kapatın veya açın

- 1 Mozilla Firefox'u başlatın.
- 2 **Firefox** menüsünde **Eklentiler** 'e tıklayın.
- 3 **Uzantılar** sekmesinde **Norton Password Manager** 'a tıklayın.
- 4 **Norton Password Manager** gri renkteyse **Etkinleştir** 'e tıklayın.
· Norton Password Manager gri renkte değilse **Devre dışı bırak** 'a tıklayın
- 5 Mozilla Firefox'u yeniden başlatın.

Safari'de Password Manager'ı uzantılar sayfasından kapatın veya açın

- 1 Safari'yi başlatın.
- 2 Safari menüsünde **Safari** 'ye ve ardından **Tercihler** 'e tıklayın.
- 3 **Uzantılar** 'a tıklayın.
- 4 Sol bölmede, Norton Password Manager etkinse **Etkin** kutusunun işaretini kaldırın.
Uzantılar sayfasında Norton Password Manager devre dışıysa **Etkin** kutusunu işaretleyin

Norton Safe Web'i açma veya kapatma

Norton Safe Web Internet Explorer, Firefox veya Chrome kullanarak çevrimiçi gezindiğinizde, arama veya alışveriş yaptığınızda sizi korur. Ziyaret ettiğiniz web sitelerinin güvenlik düzeyini analiz eder ve web sitelerinin tehdit içerip içermediğini gösterir. Arama sonuçlarının yanında site derecelendirmesi simgeleri sunar, böylelikle web sitelerini daha ziyaret etmeden kötü amaçlı olup olmadıklarını anlarsınız.

Google Chrome'da Norton Safe Web'i uzantılar sayfasından kapatma veya açma

- 1 Google Chrome'u başlatın.
- 2 Sağ üst köşedeki **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** seçeneğinde **Diğer Araçlar** 'a gidin ve **Uzantılar** 'a tıklayın.
- 4 **Uzantılar** sayfasında Norton Safe Web etkinse **Etkin** kutusunun işaretini kaldırın.
Norton Safe Web devre dışıysa, **Etkin** kutusunu işaretleyin
- 5 Google Chrome'u yeniden başlatın.

Mozilla Firefox'ta Norton Safe Web'i Eklentiler sayfasından kapatma veya açma

- 1 Mozilla Firefox'u başlatın.
- 2 Firefox menüsünde **Eklentiler** 'e tıklayın.
- 3 **Uzantılar** sekmesinde, **Etkinleştir** 'e tıklayın.
Norton Safe Web gri değilse **Devre dışı bırak** 'a tıklayın
- 4 Mozilla Firefox'u yeniden başlatın.

Safari'de Norton Safe Web'i uzantılar sayfasından kapatma veya açma

- 1 Safari'yi başlatın.
- 2 **Safari** menü çubuğunda, **Safari** 'yi ve ardından **Tercihler** 'i tıklayın.
- 3 **Uzantılar** 'a tıklayın.
- 4 Sol bölmede, Norton Safe Search etkinse, **Etkin** kutusunun işaretini kaldırın.
Uzantılar sayfasında Norton Safe Search devre dışıysa **Etkin** kutusunu işaretleyin.

Microsoft Edge'de Norton Safe Web'i Uzantılar sayfasından kapatma veya açma

- 1 Microsoft Edge'i başlatın.
- 2 Sağ üst köşedeki **Daha fazla** 'e tıklayın



ve **Uzantılar** 'ı seçin.

- 3 **Uzantı** penceresinde **Uzantıları mağazadan al** 'a tıklayın.
- 4 **Mağaza** penceresinde, Arama kutusuna Norton yazın.
- 5 Sonuçlarda, **Norton Safe Web** ögesine ve **Kur** ögesine tıklayın.
- 6 Uzantı yüklendikten sonra **Başlat** 'a tıklayın.
- 7 **Yeni bir uzantınız var** açılır penceresinde **Aç** 'a tıklayın.
Açılır pencereyi kaçırsanız, Microsoft Edge'in sağ üst köşesinde **Diğer** düğmesini tıklayın.



, ve **Uzantılar** 'ı seçin.

- 8 **Norton Safe Web** altında **Norton Safe Web** penceresinde, kaydırıcıyı **Açık** konumuna hareket ettirin.

Norton Safe Web uzantısını kapatmak için, kaydırıcıyı **Kapalı** konuma getirin.

Norton Safe Search kullanarak web'de arama yap

Norton Safe Search, web'de arama deneyiminizi geliştirir. İnternette Norton Safe Search kullanarak arama yaptığınızda, arama sonuçları oluşturmak için Ask.com ve Yahoo! arama motorlarını kullanır. Norton Safe Search, oluşturulan arama sonuçlarının her biri için site güvenlik durumu ve Norton değerlendirmesini sağlar.

Norton Safe Search klavyeden giriş yaparken akıllı arama özelliği sunmakta ve arayacağınız ifadenin ilk birkaç harfini girdiğinizde arama önerileri sunmaktadır.

Not: Norton Safe Search özelliği Avustralya, Belçika, Brezilya, Kanada, Danimarka, Finlandiya, Fransa, Almanya, İtalya, Japonya, Hollanda, Norveç, İspanya, İsveç, İsviçre, Amerika ve İngiltere dahil sadece belli bölgelerde mevcuttur. Privacy Safeguard özelliği, ABD, Birleşik Krallık ve Kanada'da kullanılabilir.

Password Manager özelliklerini kapatmış olsanız bile, Norton Safe Search'ü kullanabilirsiniz.

Not: Norton Safe Search yalnızca Internet Explorer, Firefox veya Chrome tarayıcılarında desteklenir.

Norton Safe Search kullanarak web'de arama yap

- 1 Tarayıcınızı açın.
- 2 Norton Security araç çubuğunda **Norton Safe Search** kutusuna aramak istediğiniz ifadeyi klavyeden girin.
- 3 Aşağıdakilerden birini yapın:
 - **Safe Search** 'e tıklayın.
 - Açılır pencerede, arama dizinizle eşleşen bir arama önerisini seçin.

Araç çubuğundaki Norton Safe Search Kutusunu etkinleştir

Not: Bu özellik yalnızca Internet Explorer için kullanılabilir.

Norton'u yüklediğinizde, Internet Explorer'a Norton Security araç çubuğu eklenir. Internet Explorer'ı açtığınızda araç çubuğunuzdaki **Norton Safe Search** kutusunu etkinleştirmeniz istenir.

Norton Safe Search kutusunu manuel olarak devre dışı bıraktıysanız ve yeniden etkinleştirmek istiyorsanız şunu yapın:

- 1 Tarayıcınızı açın.
- 2 Norton Security araç çubuğunda ayarlar (...) simgesine tıklayın.
- 3 Görünen menüde **Norton Safe Search** seçeneğinin yanındaki anahtarı **Açık** konuma getirin.

Norton Safe Search kutusunu devre dışı bırakmak için aşağıdakileri yapın:

- 1 Tarayıcınızı açın.
- 2 Norton Security araç çubuğunda ayarlar (...) simgesine tıklayın.
- 3 Görünen menüde **Norton Safe Search** seçeneğinin yanındaki anahtarı **Kapalı** konuma getirin.

Norton Password Manager'a Erişme

Password Manager'a aşağıdaki bölgelerden erişebilirsiniz:

- Windows'ta ürün ana penceresindeki **İnternet Güvenliği** bölümünden
- Norton Password Manager uzantısından
- Android ve iOS'ta Norton Password Manager uygulamasından

Sırasıyla **Oturum Açma Bilgilerini Yönet** penceresine ve **Kartları Yönet** penceresine erişmek için **Web Koruması** bölümündeki **Oturum Açma Bilgileri** ve **Kartlar** seçeneklerini kullanabilirsiniz.

Ürünün kullanım süresi geçtikten sonra bile tüm Password Manager bilgilerine erişebilirsiniz. Ürünün süresi dolduktan sonra görüntüleyebileceğiniz veya erişebileceğiniz özellikler şunlardır:

Oturumlar	Saklanan çevrimiçi banka hesabı, e-posta kullanıcı adı ve parolası gibi oturum bilgilerini görüntüleyebilirsiniz.
Adresler	Ad, doğum tarihi, posta adresi, e-posta adresi ve telefon numaraları gibi, saklanan kişisel bilgilerinizi görüntüleyebilirsiniz.
Cüzdan	Kredi kartı bilgisi, banka hesabı bilgisi ve kredi ödeme ayrıntıları gibi, saklanan finansal bilgilerinizi görüntüleyebilirsiniz.
Notlar	Girdiğiniz metni ileride başvurmak için görüntüleyebilirsiniz.

Not: Password Manager özelliklerine erişmek için Password Manager'a giriş yapmış olmanız gerekir. Password Manager özellikleri Internet Explorer, Firefox, Safari ve Chrome tarayıcılarında desteklenir.

Android veya iOS'ta Norton Password Manager uygulamasını indirme ve yükleme

- 1 Şunlardan birini yapın:
 - Android'te, **Play Store** 'a gidin. Play Store'u ilk kez açıyorsanız Hizmet Koşulları ekranı açılır. Devam etmek için **Kabul** 'e dokunun.
 - iOS'ta, ana ekranınızda **App Store** simgesine dokunun.
- 2 Norton Password Manager uygulamasını arayın ve seçin.
- 3 Şunlardan birini yapın:
 - Android'te, uygulama ayrıntıları ekranında **Yükle** 'ye dokunun ve **Kabul et ve indir** 'e dokunun.
 - iOS'ta, **Ücretsiz** 'e dokunun ve sonra **UYGULAMAYI YÜKLE** 'ye dokunun. **Apple ID Parolası** ekranında, Apple hesabı parolanızı girin.

Norton Password Manager bulut kasası oluşturma

Password Manager bir bulut kasası oluşturmanızı ve Password Manager verilerinizi kaydetmenizi sağlar. Bir Norton hesabı için bir bulut kasası oluşturabilirsiniz. Bulut kasası hareket halinde olduğunuzda Password Manager verilerinizi kullanma kolaylığı sağlar.

Password Manager bulut kasasına İnternet'e bağlı herhangi bir bilgisayardan erişebilirsiniz.

Tarayıcıdan bulut kasası oluşturma

- 1 Tarayıcınızı açın.
- 2 Tarayıcının sağ üst köşesindeki **Norton Password Manager** 'a tıklayın.
- 3 Norton Password Manager giriş ekranında **Giriş Yap** 'a tıklayın.
- 4 Görüntülenen **Norton'a Hoş Geldiniz** penceresinde, **Hesap Oluştur** 'a tıklayın.
- 5 **Hesap Oluşturma** sekmesinde, bilgileri doldurun ve **Hesap Oluştur** 'a tıklayın.
- 6 **Kasa tespit edilmedi** penceresinde, **Kasa Oluştur** 'a tıklayın.
- 7 **Kasanızı oluşturun** penceresinde, parolanızı yazın ve **İleri** 'ye tıklayın.
Parolanın kabul edilmesi için belirtilen bütün kriterleri karşılaması gerekir.
- 8 Parolanızı yeniden yazın ve **İleri** 'ye tıklayın.
- 9 Size parolanızı hatırlatacak bir ipucu yazın ve **Kasayı Oluştur** 'a tıklayın.
- 10 **Kurulum tamamlandı** penceresinde, **Kasaya git** seçeneğine tıklayın.

Norton'dan bulut kasası oluşturma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **İnternet Güvenliği** 'ni çift tıklayın ve ardından **Password Manager** 'a tıklayın.
- 3 **Başlayın** penceresinde hesap bilgilerinizle giriş yapın.
- 4 **Yeni kasa oluşturma: kasa parolası** penceresindeki, **Kasa Parolası** kutusunda, parolanızı girin ve ardından **İleri** 'ye tıklayın.
- 5 **Yeni kasa oluşturma: parolayı onayla** penceresinde, onaylamak için parolanızı tekrar girin ve ardından **İleri** 'ye tıklayın.
- 6 **Yeni Kasa oluşturma: parola ipucu** kutusuna, parola için bir ipucu girin ve **İleri** 'ye tıklayın.
Password Manager verilerinizin yedeğine zaten sahipseniz, **İçe aktar** 'a tıklayın ve yeni hesapla birleştirilecek yedeklenmiş dosyayı seçin.
- 7 **Son** 'a tıklayın.

Android veya iOS'ta bulut kasası oluşturma

- 1 **Norton Password Manager** uygulamasında oturum açın.
- 2 **Oturum Aç** penceresinde, Norton hesabınızın e-posta adresini ve parolasını yazın.
- 3 **Oturum aç** 'a dokununuz ve ekrandaki talimatları uygulayın.

Norton Password Manager bulut kasanızı silme

Bulut kasanız şifrelidir ve yalnızca Norton hesabınızı ve kasa parolalarınızı kullanarak erişmek mümkündür. Bulut kasanızı silmek istiyorsanız, bunu manüel olarak yapmalısınız. Norton ürününü cihazınızdan kaldırırsanız bile kasanızı diğer cihazlardan kullanmaya devam edebilirsiniz.

Uyarı: Bir kasayı sildiğinizde, kasada kaydettiğiniz tüm Password Manager verileri kalıcı olarak kaldırılır. Kasa verilerinizi daha sonra kullanabileceğinizi düşünüyorsanız, kasanızı silmeyin.

Bulut kasanızı silin

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **İnternet Güvenliği** 'ni çift tıklayın ve ardından **Password Manager** 'a tıklayın.
- 3 **Kasa Kapalı** penceresinde, parolanızı üç kez yanlış girin.
- 4 **Kasanızı silmeniz mi gerekli?** seçeneğinin yanındaki **Buraya tıklayın** bağlantısına tıklayın.
- 5 **Kasayı Sil** penceresinde, **Evet, kasamı sil** 'e tıklayın.
- 6 Uyarı iletişim kutusunda **Evet** 'e tıklayın.
- 7 Doğrulamak için Norton hesabınızın parolasını yazın ve ardından **Giriş Yap** 'a tıklayın.
- 8 Onay penceresinde **Tamam** 'a tıklayın.

Norton ürünümü kaldırdıktan sonra bulut kasası hesabıma nasıl erişirim?

- 1 Norton hesabı kimlik bilgilerinizle Norton Password Manager web sitesine [giriş yapın](#).
- 2 **Kasanızı açın** penceresinde kasa parolanızı yazın ve **Kasayı Aç** seçeneğine tıklayın.

Norton Password Manager verilerinizi dışa aktarma

Password Manager verilerinizi güvenlik, veri kurtarma sebebiyle ya da Password Manager verilerinizi yeni bir bilgisayara aktarmak için dışa aktarabilirsiniz. Kasa parolanız sıfırlanamaz. Bu nedenle Symantec, Kasa verilerinizi periyodik olarak yedeklemenizi önerir. Otomatik yedekleme özelliğini etkinleştirdiğinizde Kasanızın yedekleri otomatik olarak oluşturulur ve cihazınızda yerel olarak saklanır.

Ürününüzün kullanım süresi dolduğunda Password Manager verilerini alabilirsiniz.

Not: Norton Password Manager, Norton Password Manager (.NPM) dosyalarının dışarı aktarılmasına izin vermez.

Norton Password Manager verilerinizi tarayıcıdan dışa aktarma

- 1 Tarayıcınızı açın.
- 2 Tarayıcının sağ üst köşesindeki **Norton Password Manager** 'ı tıklayın.
- 3 Görünen açılır pencerede **Kasayı aç** 'ı tıklayın.
- 4 **Kasanızın kilidini açma** penceresinde, kasa parolanızı girin ve **Kasayı aç** 'ı tıklayın.
- 5 Norton Password Manager tarayıcı eklentisi simgesini ve **Kasa** 'yı tıklayın.
- 6 Norton Password Manager penceresinde



simgesini ve **Kasayı dışa aktar** 'ı tıklayın.

- 7 **Korumalı kasa Eylemi** penceresinde, Norton Password Manager verilerini dışa aktarmak için kasa parolanızı girin.

Norton Password Manager verilerinizi Norton'dan dışa aktarma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **İnternet Güvenliği** 'ni çift tıklayın ve ardından **Password Manager** 'ı tıklayın.
- 3 **Norton Password Manager** penceresinde, pencerenin altında mevcut **Ayarlar** simgesini tıklayın.
- 4 **İçe Aktar/Dışa Aktar** sekmesini tıklayın.
- 5 **Dışa Aktar** bölümünde, dosya biçimini seçin.

Aşağıdakilerden birini seçebilirsiniz:

- **Password Manager Yedekleme Biçimi - DAT Dosyası**
Daha fazla güvenlik için bir parola ile verilerinizi yedeklemek istiyorsanız, parolayı girin ve onaylayın.

- **Düz Metin – CSV dosyası (Sadece Oturumlar ve Notlar)**

Kasa yedeklerinize, **My Documents\Norton Password Manager Backups\<Norton account name>** dizininden erişebilirsiniz.

- 6 **Dışa Aktar** 'ı tıklayın.
- 7 **Password Manager için Parolayı Doğrula** penceresinde, Password Manager verilerinizi dışarı aktarmak için kasa parolanızı girin.
- 8 Onay iletişim kutusunda **Tamam** 'ı tıklayın.

Norton Password Manager verilerinizi içe aktarma

Password Manager verilerinizi daha önceden yedeklediğiniz dosyadan içeri aktarabilirsiniz. Kasa otomatik yedekleme, yalnızca otomatik yedekleme özelliği etkin olduğunda gerçekleşir. Otomatik yedekleme klasörünün varsayılan konumu C: \Documents\Norton Password Manager'dır.

İçe aktarılan verileri mevcut veriler ile Birleştir ve Mevcut verileri içe aktarılan verilerle değiştir seçenekleri Norton Password Manager verilerini yedekleme dosyasından içe aktardığınızda görünür. İçeri aktarılan verileri, şu anda giriş yaptığınız kasa ile birleştirebilir ya da kasanızda sakladığınız mevcut verilerinizi içe aktarılan verileriniz ile değiştirebilirsiniz

Not: İçe aktarırken, .CSV dosyaları boyutunun 15 MB'tan fazla olmaması gerekir. Norton Password Manager, Norton Password Manager (.NPM) dosyalarının içe aktarılmasına izin vermez.

Norton Password Manager verilerinizi Norton'dan içe aktarma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **İnternet Güvenliği** 'ni çift tıklayın ve ardından **Password Manager** 'ı tıklayın.
- 3 **Norton Password Manager** penceresinde, pencerenin altında mevcut **Ayarlar** simgesini tıklayın.
- 4 **İçe Aktar/Dışa Aktar** sekmesini tıklayın.
- 5 **İçe Aktar** satırından, **İçe Aktar** 'ı tıklayın.
- 6 **Kasayı İçe Aktar** penceresinde, aşağıdaki seçeneklerden birini belirleyin:
 - **İçe aktarılan verileri mevcut verilerle birleştirin**
 - **İçe aktarılan verileri mevcut verilerle birleştirin**
- 7 **İçe Aktar** 'ı tıklayın.
- 8 Göndermek istediğiniz dosyanın konumuna göz atın.
Kasa yedeklerinize, **My Documents\Norton Password Manager Backups\<Norton account name>** dizininden erişebilirsiniz.
- 9 Dosyayı seçip **Aç** 'ı tıklayın.
- 10 Mevcut kasada ve içe aktarılan kasada sakladığınız oturum açma bilgileri için farklı parolalarınız varsa, Norton bir onaylama iletisi görüntüler. Aşağıdakilerden birini seçin:
 - Bulut kasasında saklanan parolayı tutmak için **Mevcut Parolayı Koru** 'yu tıklayın.

- Bulut kasasında saklanan parolayı içe aktarma kasasında saklanan parolanın üzerine yazmak için **İçe Aktarılan Parolayı Korumayı** tıklatın.

11 Onay iletişim kutusunda **Tamam** 'ı tıklatın.

Norton Security araç çubuğunu etkinleştirme veya devre dışı bırakma

Norton Security araç çubuğu etkinleştirildiğinde Norton Password Manager, Norton Safe Web açılır penceresini ve ziyaret ettiğiniz web siteleri için güvenlik sıralamasını görüntüler. Araç devre dışı bırakıldığında, Norton Password Manager, Norton Safe Web açılır penceresini görüntüleyemez ancak sizi şüpheli ve dolandırıcı web sitelerine karşı bilgilendirmeye devam eder.

Norton Security araç çubuğunu etkinleştirme veya devre dışı bırakma

- ◆ Tercih ettiğiniz tarayıcıyı açın:
 - Internet Explorer'da menü çubuğunu sağ tıklatın, **Norton Security Araç Çubuğu** 'nu etkinleştirmek veya devre dışı bırakmak için işaretleyin ya da işareti kaldırın ve daha sonra ekrandaki talimatları takip edin.
 - Safari'de **Görünüm > Araç Çubuğunu Özelleştir** 'i tıklatın ve ardından etkinleştirmek veya devre dışı bırakmak için Norton Security Araç Çubuğu uzantısını sürükleyin ve bırakın.

Uygulamalarınızı ve dosyalarınızı saldırılardan, bilgisayar korsanlarından ve sıfır gün saldırılarından koruyun.

Sıfır gün açıklarından yararlanma girişimi, bilgisayar korsanlarının bilgisayarınızda kötü amaçlı eylemler gerçekleştirebilmek için bir programdaki güvenlik açıklarından yararlanmak için kullandıkları bir tekniktir. Bilgisayarınızı yavaşlatmanın ya da programların çalışmalarını engellemenin yanı sıra, bu istismarlar kişisel verilerinizi ve gizli bilgilerinizi bilgisayar korsanlarına açabilir.

Norton ürününüzdeki Açıklardan Yararlanma Girişimini Engelleme özelliği, açıklardan yararlanma girişimi saldırılarına meyilli uygulamaları ve dosyaları korur. Varsayılan olarak, Norton Açıklardan Yararlanma Girişimini Engelleme etkinleştirilmiştir ve savunmasız programları kapatarak bu programlara yönelik saldırıları engeller. Norton, bir programı kapattığında ve saldırı hakkındaki bilgilere bağlantılar sağladığında Saldırı Engelleme bildirimi gönderir.

Açıklardan Yararlanma Girişimini Engelleme'yi açın veya kapatın

Not: Açıklardan Yararlanma Girişimini Engelleme kapalı olduğunda, bilgisayarınız sıfır gün ve diğer istismlara karşı savunmasızdır.

1 Norton'u başlatın.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

2 Norton ana penceresinde **Ayarlar** 'a tıklayın.

3 Ayarlar penceresinde, **Açıklardan Yararlanma Girişimini Engelleme** 'yi tıklayın.

4 Açıklardan Yararlanma Girişimini Engelleme satırında, **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.

5 Ayarlar penceresinde **Uygula** ve ardından **Kapat** 'ı tıklayın.

Açıklardan Yararlanma Girişimini Engelleme Teknikleri

Norton, bilgisayarınızı en son sıfır gün saldırılarına karşı korumak için proaktif açıklardan yararlanma girişimini engelleme teknikleri kullanır. Teknikleri **Ayarlar** penceresinden açabilir veya kapatabilirsiniz. Varsayılan olarak, tüm teknikler açıktır.

Not: Norton, en geniş kapsamlı istismlara karşı korumak için tüm bireysel Açıklardan Yararlanma Girişimini Engelleme tekniklerini açık tutmanızı önerir.

Açıklardan Yararlanma Girişimini Engelleme Teknikleri şunları içerir:

■ Java İşlem Koruması

Uzaktan korsanların, java işlemleri yoluyla zararlı kod kullanmasını önler ve yalnızca güvenilir java işlemlerinin çalışmasına izin verir.

■ Yapılandırılmış İstisna İşleyicisi Üzerine Yazma Koruması

Bir istisna eylemcisinin işaretçisini saldırgan tarafından denetlenen bir adresle üzerine yazarak bir uygulamayı tehlikeye atan, yapılandırılmış dışlama yönetme açıklardan yararlanma girişimlerine karşı koruma sağlar.

■ Yığın Özet Algılama

Geri Dönüş Yönelimli Programlama (ROP) tarafından hazırlanmış saldırı kodunu yürütmek için yığın göstericisini saldırganın denetimli belleğiyle değiştiren açıklardan yararlanma girişimlerini engeller.

■ Veri Yürütme Engelleme Yaptırımı

Saldırganların, bilgisayarınızın yığın veya yığın belleğinden kötü amaçlı kod çalıştırmasını engeller.

■ Bellek Düzeni Rastgeleleştirme Yaptırımı

Uygulamalarınızı ve dosyalarınızı saldırılardan, bilgisayar korsanlarından ve sıfır gün saldırılarından koruyun.

Dinamik olarak yüklenmiş uygulama DLL'lerini veya modüllerini, saldırganlardan korumak için her zaman rastgele konumlarda yüklenmesini zorunlu kılar.

- **Öbek Sprey Koruması**
Açıkça hedeflenen bellek konumlarını, saldırganların ya da saldırganların yığın sprej saldırı teknikleriyle kabuk kodlarını tahsis ettikleri yerleri korur.
- **Bellek Düzeni Rastgeleleştirme Geliştirme**
Uygulamanın kritik bellek konumlarını tahsis ederken işletim sisteminin ASLR (Adres Alanı Düzeni Randomizasyon) davranışını geliştirir. Bu, hafıza konumlarını saldırganlardan daha az tahmin edilebilir kılar.
- **Boş Sayfa Koruması**
Boş işaretçi açıklık güvenlik açıkları üzerindeki saldırıları önlemeye yardımcı olacak boş bellek konumunu önceden ayırır.
- **Uzak DLL Enjeksiyon Algılama**
Uzak bilgisayar korsanlarının, genel IP adresleri veya etki alanları gibi harici ağlar üzerinden kötü amaçlı yürütülebilir kod eklemelerini engeller.
- **Yığın Yürütme Engeli, Şüpheli API Çağırma Algılaması ve Öbek Yüğü Algılama**
teknikleri, bilgisayarınızı Adres Alanı Düzeni Randomizasyon ve Veri Yürütme Engellemesi azaltma tekniklerini atlayan Geriye Yönelik Programlama (ROP) saldırılarına karşı korur.

Norton Güvenlik Duvarı'nı açma veya kapatma

Akıllı Güvenlik Duvarı, İnternetteki diğer bilgisayarlarla sizin bilgisayarınız arasındaki iletişimi izler. Ayrıca bilgisayarınızı sık karşılaşılan güvenlik sorunlarına karşı korur. Akıllı Güvenlik Duvarı kapalı olduğunda, bilgisayarınız İnternet kaynaklı tehditlere ve güvenlik risklerine karşı korunmaz.

Akıllı Güvenlik Duvarı'nı kapatmanız gerekirse yalnızca belirli bir süreyle kapatmalısınız. Akıllı Güvenlik Duvarı süreden sonra otomatik olarak yeniden açılır.

Norton Güvenlik Duvarı'nı açma veya kapatma

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Genel Ayarlar** sekmesinde, **Akıllı Güvenlik Duvarı** satırında, **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.
- 5 **Uygula** seçeneğine tıklayın.
- 6 İstenirse, Güvenlik duvarı özelliğinin kapalı kalmasını istediğiniz süreyi seçin ve ardından **Tamam** 'a tıklayın.

Norton Güvenlik Duvarı'nı, Windows bildirim alanından devre dışı bırakma veya etkinleştirme

- 1 Görev çubuğundaki bildirim alanında Norton simgesini çift tıklayın ve ardından **Akıllı Güvenlik Duvarını Devre Dışı Bırak** veya **Akıllı Güvenlik Duvarını Etkinleştir** öğesini tıklayın.
- 2 İstenirse, Güvenlik duvarı özelliğinin kapalı kalmasını istediğiniz süreyi seçin ve ardından **Tamam** 'a tıklayın.

Program Kuralları'nı Özelleştirme

Norton programını belirli bir süre kullandıktan sonra bazı programların erişim ayarlarını değiştirmeniz gerekebilir.

Program Kuralları 'nı Özelleştirme

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Program Kontrolü** sekmesinde **Program** sütununda, değiştirmek istediğiniz programı seçin.
- 5 Değiştirmek istediğiniz programın yanındaki aşağı açılır listede, bu programa vermek istediğiniz erişim düzeyini seçin. Seçenekleriniz şunlardır:

İzin Ver	Bu program tarafından yapılan tüm erişim denemelerine izin verir.
Engelle	Bu program tarafından yapılan tüm erişim denemeleri reddedilir.
Özel	Bu programın İnternete nasıl erişeceğini denetleyen kuralları oluşturur.

- 6 **Uygula** 'ya tıklayın.

Güvenlik duvarı kurallarının sırasını değiştir

Her güvenlik duvarı kuralı listesi yukarıdan aşağıya doğru işlenir. Güvenlik duvarı kurallarının sıralarını değiştirerek nasıl işleneceğini ayarlayabilirsiniz.

Not: İleri düzey kullanıcı değilseniz varsayılan Trafik kurallarının sırasını değiştirmeyin. Varsayılan Trafik kurallarının sırasını değiştirmek, güvenlik duvarı işlevselliğini etkileyebilir ve bilgisayarınızın güvenliğini azaltabilir.

Trafik kurallarının sırasını değiştir

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Trafik Kuralları** sekmesinde, taşımak istediğiniz kuralı seçin.
- 5 Aşağıdakilerden birini yapın:
 - Bu kuralı üstündeki kuralın önüne taşımak için, **Yukarı Taşı** 'ya tıklayın.
 - Bu kuralı altındaki kuralın arkasına taşımak için, **Aşağı Taşı** 'ya tıklayın.
- 6 Kuralları taşımayı tamamladıktan sonra **Uygula** 'ya tıklayın.

Program kurallarının sırasını değiştirme

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Program Kontrolü** sekmesinde, taşımak istediğiniz kuralı içeren programı seçin.
- 5 **Değiştir** seçeneğine tıklayın.
- 6 **Kurallar** penceresinde, taşımak istediğiniz kuralı seçin.
- 7 Aşağıdakilerden birini yapın:
 - Bu kuralı üstündeki kuralın önüne taşımak için, **Yukarı Taşı** 'ya tıklayın.
 - Bu kuralı altındaki kuralın arkasına taşımak için, **Aşağı Taşı** 'ya tıklayın.
- 8 Kuralları taşımayı tamamladıktan sonra **Tamam** 'a tıklayın.
- 9 **Güvenlik Duvarı** ayarları penceresinde, **Uygula** 'ya tıklayın.

Trafik kuralını geçici olarak kapatma

Bir bilgisayara veya programa özel erişim izni vermek istiyorsanız, bir Trafik kuralını geçici olarak kapatabilirsiniz. Bu değişikliği gerektiren programla veya bilgisayarla çalışmanız bittiğinde, kuralı tekrar açmayı unutmayın.

Not: Listede görünen varsayılan güvenlik duvarı kurallarının bazılarını kapatamazsınız.

Görüntüle seçeneğini kullanarak yalnızca bu kuralların ayarlarını görüntüleyebilirsiniz.

Trafik kuralını geçici olarak kapatma

- 1 Norton'u Başlat.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.

- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'nı tıklayın.

- 4 **Trafik Kuralları** sekmesinde, kapatmak istediğiniz kuralın yanındaki kutunun işaretini kaldırın.

- 5 **Uygula** 'yı tıklayın.

Bloke edilen bir programa izin ver

Bazen Akıllı Güvenlik Duvarı bazı programların internete erişmesini bloke eder. Bu programlar arasında; gerçek zamanlı aktarılan belirli medya programları, ağ oyunları veya işvereniniz tarafından sağlanan özel iş uygulamaları bulunabilir. Programın internet etkinliğinin güvenliğinize yönelik bir tehdit oluşturmadığını biliyorsanız, bloke edilen programın internete erişmesine izin verebilirsiniz.

Bloke edilen bir programa izin ver

- 1 Norton'u Başlat.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.

- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.

- 4 **Program Kontrolü** sekmesinde, İnternet'e erişmesine izin vermek istediğiniz programı seçin.

- 5 Program girişine ait **Erişim** açılır listesinde, **İzin Ver** 'e tıklayın.

- 6 **Uygula** seçeneğine tıklayın.

Norton güvenlik duvarı, web'e bağlanabilen programlar ilk kez çalıştırıldığında internet erişimi ayarlarını varsayılan olarak yapılandırır. Bir program ilk defa İnternete erişmeye çalıştığında, Otomatik Program Denetimi bu program için kurallar oluşturur. Programlarınızın İnternet erişimi ayarlarını kendiniz belirlemek isterseniz, Otomatik Program Denetimi'ni kapatın. Bir program ilk kez İnternete erişmeye çalıştığında, erişim ayarlarının yapılandırılmasını isteyen bir uyarı alırsınız.

Otomatik Program Kontrolü'nü kapat

- 1 Norton'u Başlat.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.

- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Güvenlik Duvarı** ayarları penceresinde **Gelişmiş Program Kontrolü** seçeneğine tıklayın.
- 5 **Otomatik Program Denetimi** satırında, **Açık/Kapalı** anahtarını **Kapalı** konuma getirin.

Güvenlik Duvarı Engelleme Bildirimi'ni kapat

Otomatik Program Kontrolü açıkken, Smart Firewall özelliği kötü niyetli uygulamaları ve ağınızdan diğer makineler ile iletişime geçme konusunda kötü sicile sahip uygulamaları engeller.

Norton, Akıllı Güvenlik Duvarı bir uygulamanın ağınıza bağlanmasını engellediğinde sizi uyarır. Eğer bildirim görmek istemiyorsanız bunu **Gelişmiş Program Kontrolü** 'ni kullanarak kapatabilirsiniz.

Güvenlik Duvarı Engelleme Bildirimi 'ni kapat

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Gelişmiş Program Kontrolü** sekmesinde **Güvenlik Duvarı Engelleme Bildirimini Göster** anahtarını **Kapalı** konuma getirin.

İzinsiz Girişi Önlemedişlama listesi

Ağınızda bulunan bir aygıtın güvenli olduğundan eminseniz aygıtın güven düzeyini Tam Güvenli şeklinde değiştirebilirsiniz. Bir cihazın güven düzeyini Ağ Ayarlarının altındaki Cihaz Güvenilirliği kısmından yapılandırabilirsiniz. Bu tam güvenli aygıtları İzinsiz Girişi Önleme taramasının dışında tutabilirsiniz. Tam Güvenli aygıtları İzinsiz Girişi Önleme taramasından dışladığınızda tarama süresi kısalmış ve bilgisayarınızın ağ hızı artar. Tam Güvenli olarak ayarlanan bir aygıtı dışladığınızda Norton ürününüz bu aygıttan alınan hiçbir bilgiyi taramaz. İzinsiz Girişi Önleme taramasının dışında tutulan Tam Güvenli aygıtlar İzinsiz Girişi Önleme dışlama listesine eklenir.

İzinsiz Girişi Önleme taramasından hariç tuttuğunuz aygıtlara virüs bulaştığını tespit ederseniz, kaydedilen dışlama listesini temizleyebilirsiniz. Dışlama listesini temizlerseniz Norton ürününüz dışlama listesinden tüm IPS tarafından dışlanmış aygıtları kaldırır.

Kaydedilen dışlama listesini aşağıdaki şartlar altında temizleyebilirsiniz:

- İzinsiz Girişi Önleme taramasından dışladığınız cihazlardan birisine virüs bulaştı.
- İzinsiz Girişi Önleme taramasından dışladığınız cihazlardan birisi bilgisayarınıza virüs bulaştırmaya çalışıyor.
- Ev ağınıza virüs bulaştı.

İzinsiz Girişi Önleme dışlama listesindeki cihazların tamamını nasıl kaldırabilirim?

İzinsiz Girişi Önleme dışlama listesinden tüm aygıtları kaldır

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 Ayarlar penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklatın.
- 5 İzinsiz Girişi Önleme altında, Dışlama Listesi satırında **Temizle** seçeneğini tıklatın.
- 6 Onay iletişim kutusunda **Evet** 'e tıklayın.
- 7 Ayarlar penceresinde, **Kapat** 'ı tıklatın.

Tarayıcı Koruması'nı açma

Kötü amaçlı web siteleri, zararlı program indirmek için tarayıcının güvenlik açıklarını tespit eder ve bunlardan yararlanır. Tarayıcı Koruması'nı açtığınızda Norton zararlı programları, onlar saldırmadan önce engeller. Gizli bilgilerinizi korumanıza yardımcı olur ve saldıranların bilgisayarınıza erişmesini engeller.

Tarayıcı Koruması varsayılan olarak açıktır. Kötü amaçlı web sitelerine karşı korumayı sağlamak için Tarayıcı Koruması'nı açık tutun.

Not: Tarayıcı Koruması özelliği Google Chrome, Microsoft Internet Explorer, Mozilla Firefox ve Microsoft Edge tarayıcıları için kullanılabilir.

Tarayıcı Koruması'nı nasıl açarım?

Tarayıcınızı kötü amaçlı web sitelerine karşı korumak için, Tarayıcı Koruması özelliği varsayılan olarak açıktır. Ancak herhangi bir nedenden ötürü özelliği kapatmanız durumunda yeniden açabilirsiniz.

Tarayıcı Koruması'nı aç

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 Ayarlar penceresinde **Güvenlik Duvarı** veya **Ağ** 'a tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklatın.
- 5 Tarayıcı Koruması satırında, **Açık/Kapalı** anahtarını **Açık** konuma getirin.

- 6 **Uygula** seçeneğini tıklatın.
- 7 **Ayarlar** penceresinde, **Kapat** 'a tıklayın.

Norton Güvenlik Duvarı'nı, bir saldırıyı engellerken sizi uyaracak veya bildirmeye başlayacak şekilde ayarlayın

Norton İzinsiz Girişleri Önleme şüphelenilen saldırıları engellediğinde bildirim alıp almayacağınızı seçebilirsiniz.

Bildirimleri almamayı seçtiyseniz, Norton'un güvenlik geçmişinizde engellediği saldırıları görüntülemeye devam edebilirsiniz.

İzinsiz Girişi Önleme bildirimlerini kapat veya aç

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'ı tıklatın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesine tıklayın.
- 5 **İzinsiz Girişi Önleme** ögesinin altında, **Bildirimler** satırında **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.
- 6 **Ayarlar** penceresinde **Uygula** 'yı ve ardından **Kapat** 'a tıklayın.

Tek bir İzinsiz Girişi Önleme bildirimini kapat veya aç

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'ı tıklatın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesine tıklayın.
- 5 **İzinsiz Girişi Önleme** altında, **İzinsiz Giriş İmzaları** satırında **Yapılandır** 'a tıklayın.
- 6 **İzinsiz Giriş İmzaları** penceresinde, ögesini imzaya denk gelen **Bildir** ögesini işaretleyin veya işaretini kaldırın.
- 7 **Tamam** 'ı tıklatın.
- 8 **İzinsiz Giriş İmzaları** penceresince önce **Uygula** 'yı ve sonra **Tamam** 'ı tıklatın.
- 9 **Ayarlar** penceresinde, **Kapat** 'a tıklayın.

AutoBlock özelliğini kapat veya aç

Norton AutoBlock, ağdaki cihaz ile bu cihazdan yararlanmaya çalışan başka herhangi bir bilgisayar arasındaki tüm trafiği durdurur. Bu, zararlı olmayabilecek trafiği içerdiğinden, AutoBlock yalnızca bir tehdit algıladıktan sonra sınırlı bir süre için bağlantıyı durdurur. Norton ürününüzün saldıran bilgisayarlardan gelen bağlantıları bloke edeceği süreyi belirtebilirsiniz. Varsayılan olarak Norton ürününüz, bilgisayarınız ve saldıran bilgisayar arasındaki tüm trafiği 30 dakika için bloke eder.

AutoBlock, erişmeniz gereken bir bilgisayarı veya bilgisayarları bloke ediyorsa, AutoBlock özelliğini kapatabilirsiniz.

AutoBlock özelliğini kapat veya aç

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'ı tıklatın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklatın.
- 5 **Intrusion AutoBlock** altında, **Intrusion AutoBlock** satırında **Yapılandır** 'ı tıklatın.
- 6 **Intrusion AutoBlock** penceresinde, **AutoBlock** altında, aşağıdakilerden birini yapın:
 - Intrusion AutoBlock'u kapatmak için **Kapalı** seçeneğini tıklatın.
 - Intrusion AutoBlock'u engellemek için **Açık (Önerilir)** öğesini tıklatın ve ardından **Saldıran bilgisayarı oto engelle** aşağı açılan listesinden AutoBlock'u ne kadar süre açık tutacağınızı seçin.
- 7 **Intrusion AutoBlock** penceresinde, **Tamam** 'ı tıklatın.
- 8 **Ayarlar** penceresinde, **Kapat** 'ı tıklatın.

AutoBlock uygulanmış bilgisayarların blokesini kaldırma

Norton Güvenlik Duvarı, güvenli olduğunu bildiğiniz bir bilgisayar ağ trafiğini durdurursa, bilgisayarı Norton Güvenlik Duvarı ayarlarındaki AutoBlock listesinden kaldırarak bağlantıları geri yükleyebilirsiniz.

AutoBlock uygulanmış bir bilgisayarın engellemesini kaldırma

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'ı tıklatın.

- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklatın.
- 5 **Intrusion AutoBlock** altında, **Intrusion AutoBlock** satırında **Yapılandır** 'a tıklayın.
- 6 **İzinsiz Giriş Otomatik Engelleme** penceresinden, **Şu anda İzinsiz Giriş Otomatik Engelleme tarafından engellenen bilgisayarlar** 'ı seçin ve bilgisayarınızın IP adresini tıklayın.
- 7 **Eylem** sütunu altında, açılır listeden **Blokeyi Kaldır** 'ı seçin.
- 8 **Intrusion AutoBlock** penceresinde, **Tamam** 'a tıklayın.
- 9 **Ayarlar** penceresinde, **Kapat** 'ı tıklatın.

Aygıt Güven'ine bir cihaz ekleme

Bir cihazı Güvenli Aygıt'a manuel olarak ekleyebilirsiniz. Aşağıdakileri belirterek bir aygıtı ekleyebilirsiniz:

- Cihazın adı veya açıklaması
- Cihazın IP adresi veya fiziksel adresi

Not: Ağınızda bulunmayan bir cihaza güvenirsiniz, bilgisayarınızı potansiyel güvenlik riskine maruz bırakabilirsiniz.

Aygıt Güven'ine bir cihaz ekleme

- 1 Norton'u Başlat.
- 2 **Aygıt Güvenliği** 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 3 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 4 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 5 **Genel Ayarlar** sekmesi **Aygıt Güveni** menüsünün altındadır; buradan **Yapılandır** seçeneğine tıklayın.
- 6 **Aygıt Güveni** penceresinden **Ekle** seçeneğine tıklayın.
- 7 **Cihazı Ekle** penceresinde, **Ad** kutusuna, ağınıza eklemek istediğiniz cihazın adını yazın. Maksimum cihaz adı en fazla 15 karakteri aşmamalıdır.

- 7 **IP veya Fiziksel Adres** kutusuna, Ağ Güvenlik Haritası'na eklemek istediğiniz cihazın IP adresini veya fiziksel adresini yazın.

IP Adresi veya Fiziksel Adres kutusunda aşağıdaki biçimleri kullanabilirsiniz:

IPv4 adresi	172.16.0.0
IPv6 adresi	fe80::12ac:fe44:192a:14cc
Fiziksel adres	11-22-c3-5a-fe-a4
Çözümlenebilir ana bilgisayar	ftp.myfiles.com

Cihaz ağda fiziksel olarak bulunana kadar, verdiğiniz adres doğrulanmaz.

- 8 **Güven Düzeyi** alt menüsünden bir seçenek seçin Seçenekleriniz şunlardır:

Tam Güvenli

Cihazı Tam Güvenli listesine ekler.

Tam Güvenli cihazlar yalnızca bilinen saldırılar ve virüs bulaşmaları için izlenir. Bu uyarı ancak, cihazın tamamen güvenli olduğundan eminseniz seçmelisiniz.

Kısıtlı

Cihazı, Kısıtlı listesine ekler.

Kısıtlı cihazlar bilgisayarınıza erişemez.

- 9 Eğer bir cihazı Saldırı Önleme taraması listesinden çıkartmak istiyorsanız, **IPS Taramasından Çıkart** seçeneğini gözden geçirin.
- 10 **Cihaz Ekle** 'ye tıklayın.

İndirme Bilgi Merkezi özelliğini kapat veya aç

İndirme Sicili, desteklenen bir tarayıcı kullanarak indirdikten sonra çalıştırabileceğiniz veya yürütebileceğiniz güvenli olmayan bir dosyaya karşı bilgisayarınızı korur. **İndirme Bilgi Merkezi** seçeneği varsayılan olarak açıktır. Bu durumda İndirme Sicili, indirdiğiniz yürütülebilir dosyaların güvenilirlik düzeyleri hakkında size bildirimde bulunur. İndirme Sicili'nin verdiği güvenilirlik bilgileri, indirilen dosyayı yüklemenin güvenli olup olmadığını gösterir.

Bazen İndirme Sicili'ni kapatmak isteyebilirsiniz. Örneğin, güvenli olmayan bir dosyayı indirmek istiyorsunuz. Bu durumda, Norton ürününüzün bu dosyayı indirmenize izin vermesi ve dosyayı bilgisayarınızdan kaldırmaması için İndirme Merkezi'ni kapatmanız gerekir.

İndirme Sicili'ni kapatmak veya açmak için **İndirme Bilgi Merkezi** seçeneğini kullanabilirsiniz.

İndirme Bilgi Merkezi özelliğini kapat veya aç

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'a tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklatın.
- 5 **İndirme Bilgi Merkezi** satırında, **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.
- 6 **Uygula** seçeneğine tıklayın.
- 7 İstenirse, İndirme Bilgi Merkezi özelliğinin kapalı kalmasını istediğiniz süreyi seçin ve ardından **Tamam** 'a tıklayın.
- 8 **Ayarlar** penceresinde, **Kapat** 'a tıklayın.

Spam filtresini aç veya kapat

Eposta kullanımının artması ile, birçok kullanıcı istenmeyen eposta olarak bilinen çok sayıda toplu ve izinsiz ticari e-posta iletileri almaktadır. Spam iletiler, geçerli e-posta iletilerinin fark edilmesini zorlaştırmakla kalmaz, bazı spam iletilerde rahatsız edici mesajlar ve görüntüler de bulunabilir.

İstenmeyen bu e-postaları kontrol etmek için, spam filtresi kullanabilirsiniz. Varsayılan olarak spam koruması etkin kalır. Eğer herhangi bir sebepten dolayı bunu engellemek isterseniz, programın kendisinden kapatabilirsiniz.

Not: Norton AntiSpam özelliğinin kapatılması, gönderilen istenmeyen e-posta iletilerine daha çok maruz kalmanıza neden olur.

Spam filtresini aç veya kapat

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde, **AntiSpam** 'i tıklatın.
- 4 **Filtre** sekmesinde, **AntiSpam** satırında, **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.
- 5 Spam filtrelemeyi kapatırsanız aşağıdakileri yapın:
 - **Güvenlik Talebi** penceresinde, **Süreyi seçin** açılır listesinden spam filtresi'ni kapatmak istediğiniz süreyi seçin.

- 6 **Uygula** 'yı tıklayın.
- 7 **Tamam** 'ı tıklayın.
- 8 **Ayarlar** penceresinde, **Kapat** 'ı tıklayın.

Norton'un İnternet kullanımını tanımlama

Ağ Kullanımı Sınırlaması, Norton'un kullandığı bant genişliğini kontrol etmenizi sağlar. Ağ Kullanımı Sınırlaması varsayılan olarak açıktır ve Oto olarak ayarlanmıştır. Windows 7 veya önceki bir versiyonu kullanıyorsanız varsayılan ayar **Sınır Yok** şeklindedir. İnternet bağlantınız yavaşsa Norton'un kullandığı bant genişliğini azaltabilirsiniz. Ayrıca Ağ Kullanımı Sınırlaması ayarlarını değiştirerek bilgisayarınızın kullandığı tüm ağ bağlantıları için iletişim politikalarını ayarlayabilirsiniz.

Norton'un İnternet kullanımını tanımlama

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.
- 4 **Genel Ayarlar** sekmesinde, **Ağ Kullanımı Sınırlaması** satırından **Yapılandır** seçeneğine tıklayın. **Yapılandır** seçeneği devre dışıysa **Açık/Kapalı** anahtarını **Açık** konuma getirin.
- 5 **Ağ Kullanımı Sınırlaması** penceresinde, **Politika** sütununun altında açılan listeden, ağ bağlantılarının yanından istediğiniz politikayı seçin.
- 6 Aşağıdakilerden birini seçin:
 - **Otomatik** Norton'un, Windows maliyet bilinci politikasına dayanan tüm ürünleri ve virüs tanımı güncellemelerini almasını sağlar.

Not: Otomatik seçeneği yalnızca Windows 8 ve üzeri versiyonlarda mevcuttur.

- **Sınır Yok** Norton'un tüm ürün ve virüs tanımı güncellemelerini almak için gerekli olan ağ bantı genişliğini kullanmasını sağlar. Windows 7 veya önceki bir versiyonu kullanıyorsanız varsayılan ilke **Sınır Yok** şeklindedir.
- **Ekonomi** Norton'un sadece kritik ürün güncellemelerini ve virüs tanımlarını alması için İnternete erişimini sağlar. Sınırlı bir İnternet bağlantınız varsa **Ekonomi** seçeneği kritik güvenlik tehditlerinden korunmanızı sağlar.
- **Trafik Yok** Norton'un İnternete bağlanmasını engeller. Eğer bu ilkeyi seçerseniz olası Norton, kritik virüs tanımlarını ve program güncellemelerini alamaz ve bu da tehlikelere ve virüs saldırılarına yol açabilir.

Norton'u uygulamaları izleyecek ve kötü amaçlı web sitelerinin bilgisayarınıza erişimini önleyecek şekilde ayarlayın

7 **Uygula** ögesini ve ardından **Tamam** ögesini tıklayın.

8 **Ayarlar** penceresinde, **Kapat** 'a tıklayın.

Ağ Kullanımı Sınırlaması'nı kapat veya aç

Norton internet kullanımını sınırlandırmak için ilkeleri ayarlayabilirsiniz. Norton ürününüzün İnternet kullanımını sınırlandırmak istemiyorsanız, **Ağ Maliyeti Bilinci** 'ni kapatabilirsiniz.

Eğer Norton ürününün çok fazla bant genişliği kullandığını düşünüyorsanız, **Ağ Maliyeti Farkındalığı** 'nı açabilirsiniz. Daha sonra Norton internet kullanımını sınırlandırmak için ilkeleri ayarlayabilirsiniz. **Ağ Kullanımı Sınırlaması** penceresinde ayarladığınız ilkeye bağlı olarak Norton ürünü internete bağlanır. **Ağ Maliyeti Farkındalığı** varsayılan olarak açıktır.

Ağ Kullanımı Sınırlaması'nı kapat veya aç

1 Norton'u Başlat.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

2 Norton ana penceresinde **Ayarlar** 'a tıklayın.

3 **Ayarlar** penceresinde, **Güvenlik Duvarı** 'na tıklayın.

Norton AntiVirus varsa, **Ağ** 'a tıklayın.

4 **Genel Ayarlar** sekmesinde, **Ağ Kullanımı Sınırlaması** satırında, **Açık/Kapalı** anahtarını **Kapalı** veya **Açık** konuma getirin.

5 **Ayarlar** penceresinde **Uygula** 'ya ve ardından **Kapat** 'a tıklayın.

Norton'u uygulamaları izleyecek ve kötü amaçlı web sitelerinin bilgisayarınıza erişimini önleyecek şekilde ayarlayın

Bazı kötü amaçlı web siteleri, herhangi bir ücretsiz yazılım veya paylaşılan yazılım yüklediğinizde ve açtığınızda cihaz bilgilerinize izinsiz erişim sağlamaya çalışabilir. Kötü amaçlı web siteleri, güvenlik açıklarını tespit edip bunlardan yararlanarak cihaz bilgilerinizi siber suçlulara sağlayabilecek **kripto madencilik** programları gibi zararlı programları indirebilir.

Uygulama URL İzleme açık olduğunda Norton, bilgisayarınıza yüklü tüm uygulamaları izler ve kötü amaçlı web sitelerinin bilgisayarınıza erişimini engeller. Norton, kötü amaçlı bir web sitesini engellediğinde sizi uyarır ve Güvenlik Geçmişi penceresini kullanarak saldırıyla ilgili bilgileri görebilirsiniz.

Not: Uygulama URL İzleme, tarayıcı uygulamalarını izlemez. Tarayıcı uygulamanızı kötü amaçlı web sitelerinden korumak için Norton tarayıcı uzantılarını eklemeniz gerekir.

Kötü amaçlı web sitelerini engellemek için Uygulama URL İzleme'yi açın

Varsayılan olarak **Uygulama URL İzleme** açıktır. Kötü amaçlı web sitelerine karşı korumayı sağlamak için Uygulama URL İzleme'yi açık tutun.

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 Ayarlar penceresinde **Güvenlik Duvarı** veya **Ağ** 'a tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesini tıklayın.
- 5 **İzinsiz Giriş Önleme** öğesinin altında, **Uygulama URL İzleme** satırında Açık/Kapalı anahtarını Açık konuma getirin.

Bir URL veya etki alanını izleme dışında tutun

İzinsiz Giriş Önleme, şüpheli web sitelerini tespit eden ve engelleyen kapsamlı bir saldırı imzaları listesini kullanır. Bazı durumlarda, aynı saldırı imzasına sahip olmasından dolayı, iyi amaçlı web siteleri de şüpheli olarak tanımlanabilir. Olası bir saldırı hakkında bildirimler alıyorsanız ve bildirimleri tetikleyen web sitesinin veya etki alanının güvenli olduğunu biliyorsanız imzayı izleme dışında bırakabilirsiniz.

Bir URL veya etki alanını uyarı bildirimi dışında tutun

- 1 Uyarı bildiriminde, **Ayrıntıları Görüntüle** 'ye tıklayın.
- 2 **Güvenlik Geçmişi - Gelişmiş Ayrıntılar** penceresinde, **Bu URL Engelini Kaldır** 'a tıklayın.

Norton'u kullanarak bir URL veya etki alanını dışarıda tutun

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde **Güvenlik Duvarı** veya **Ağ** 'ı tıklayın.
- 4 **İzinsiz Giriş ve Tarayıcı Koruması** sekmesine tıklayın.
- 5 **İzinsiz Giriş Önleme** altında, **Uygulama URL İzleme Dışlamaları** satırında **Yapılandır** 'a tıklayın.
- 6 **Ekle** düğmesini tıklayın ve izleme dışında tutmak istediğiniz URL veya etki alanı adını girin.
- 7 Bir URL veya etki alanını düzenlemek veya kaldırmak istiyorsanız aşağıdakileri uygulayın:
 - Listedenden bir URL veya etki alanı seçin ve **Düzenle** düğmesini tıklayın. URL veya etki alanı adını değiştirin.

- Kaldırmak istediğiniz URL veya etki alanını seçin ve **Kaldır** düğmesini tıklayın.

Engellenen URL ile ilgili bilgileri görüntüleyin

Uyarı bildirimindeki bilgileri görüntüleyin

- 1 Uyarı bildiriminde, **Ayrıntıları Görüntüle** 'ye tıklayın.
- 2 **Güvenlik Geçmişi - Gelişmiş Ayrıntılar** penceresinde, engellenen URL daha fazla ayrıntı görüntüleyebilirsiniz.

Güvenlik Geçmişi penceresini kullanarak bilgileri görüntüleyin

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **Güvenlik** ögesini çift tıklayın ve ardından **Geçmiş** ögesini tıklayın.
- 3 **Güvenlik Geçmişi** penceresinde, **Göster** açılan listesinde, listede **İzinsiz Girişi Önleme** 'yi seçin.
- 4 Öğeyle ilgili ayrıntıları görmek için bir satıra tıklayın.
- 5 Etkinlik hakkında daha fazla ayrıntı görüntülemek ve gerekirse etkinlikle ilgili bir işlem yapmak üzere Güvenlik Geçmişi Gelişmiş Ayrıntılar'ı açmak için bir satıra çift tıklayın veya **Daha Fazla Seçenek** 'e tıklayın.

Norton Bulut Yedekleme'yi kullanmaya başlama

Bulut Yedekleme, sabit sürücü bozulmaları, cihaz çalınması ve hatta fidye yazılımı gibi nedenlerle veri kaybına karşı koruyucu bir önlem olarak önemli dosya ve belgeleri saklar ve korur.

Not: Norton Bulut Yedekleme yalnızca Windows'ta kullanılabilir.

Norton Bulut Yedekleme'yi çalıştırmadan önce, yedeklemek istediğiniz dosyaları belirten bir yedekleme kümesi oluşturun. Ayrıca, dosyaların nereye yedeklenmesi ve yedeklemenin ne zaman çalışması gerektiğini de belirleyebilirsiniz. Norton Bulut Yedekleme'yi kullanarak dosyalarınızı buluta veya kendi harici sürücünüze yedekleyebilirsiniz.

Not: Yedeklemeyi ilk kez çalıştırdığınızda Norton'un bilgisayarınızdaki dosyaları incelemesi ve kopyalaması biraz zaman alabilir. İnternet bağlantınız yavaş ise bu süreç biraz daha uzayabilir.

Bir yedekleme kümesi oluşturma

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Yedekleme** 'yi çift tıklayın ve ardından **Yedekleme Kümeleri** 'ni tıklayın.
- 3 **Özet** sekmesinde, **Yapabilecekleriniz** 'in altında, **Yeni Yedekleme Kümesi Oluştur** 'u tıklayın.
Açılan pencerede, yedekleme kümenizin adını yazıp **Tamam** 'ı tıklayın.
- 4 **Ne** sekmesinde **Dosya Türleri** altında bir veya daha fazla kategori seçin.
- 5 **Yedekleme Kümelerini Yönet** penceresinde, **Ayarları Kaydet** 'i tıklayın.
- 6 **Nereye** sekmesinde **Hedef** sütununda yedeklemeniz için bir konum seçin.
Güvenli Bulut Depolama'yı seçerseniz Norton hesabınızda oturum açmak ve çevrimiçi yedeklemeyi etkinleştirmek için talimatları izleyin.
Bant Genişliği Valfi ayarı, Norton'un dosyalarınızı bulut depolamaya yedeklemek için kullandığı internet bant genişliğini yapılandırmanıza olanak sağlar. Aşağıdaki bant genişliği kısıtlayıcı durumlarından birini seçebilirsiniz:
 - **En Hızlı (Önerilir)**
 - **Yüksek Kullanım**
 - **Orta Düzeyde Kullanım**
 - **Düşük Kullanım**

Not: Önerilen ayarı seçtiğinizde, yedekleme, İnternet bant genişliğinin tamamını kullanır ve diğer İnternet etkinlikleriniz yavaşlayabilir.

- 7 **Ne Zaman** sekmesinden gereksinimlerinizi en iyi biçimde karşılayan yedekleme zamanlamasını seçmek için **Zamanlama** listesini kullanın.

Norton Bulut Yedekleme'yi Çalıştırma

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Yedekleme** ögesini çift tıklayın ve ardından **Yedeklemeyi Çalıştır** ögesini tıklayın.

- 3 **Yedeklemeyi Çalıştır** penceresinde ekrandaki talimatları izleyin.
- 4 **Kapat** 'ı tıklayın.

Not: Yedekleme tamamlanmazsa Norton yetersiz depolama alanı veya hız sınırlamaları gibi nedenler sunar. Yedekleme başlatmadan önce internete bağlı olduğunuza emin olun ve depolama cihazlarının bağlı ve açık olduğundan emin olun.

Yedekleme kümelerinize dosya ve klasör ekleme ya da dışlama

Norton, resim, müzik veya video dosyaları gibi farklı dosya türlerini yedekleme kümelerinize yedeklemenizi sağlar. Normalde yedekleme kümelerinize dahil edilen dosya türlerini içeren dosya veya klasörleri belirtebilir veya yedeklemeden dışlayabilirsiniz. Normalde varsayılan dosya türlerinin parçası olan dosya uzantılarını da ekleyebilir veya kaldırabilirsiniz.

Yedekleme kümesine dosyaları ve klasörleri ekleme veya dışlama

- 1 Norton'u başlatın.
Cihaz Güvenliği 'nin yanında **Norton Hesabım** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Yedekleme** 'yi çift tıklayın ve ardından **Yedekleme Kümeleri** 'ni tıklayın.
- 3 **Yedekleme Kümelerini Yönet** penceresinde **Özet** sekmesinde, yapılandırmak istediğiniz yedekleme kümesini seçin.
- 4 **Ne** sekmesinde **Dosya Türünü Düzenle** 'yi seçerek resim, müzik, video ve diğer dosya türlerinde dosya türüne dahil edilecek uzantıları değiştirin.
- 5 **Dosya Türleri** 'nin altında, dosya türünün karşısındaki **Yapılandır** 'ı tıklayın. Açılan pencerede aşağıdakilerden birini yapın:
 - Dosya türünden kaldırmak için listedeki uzantılardan seçim yapın:
 - Listeye yeni uzantılar eklemek için **Yeni Ekle** 'yi tıklayın.
 - **Kaydet** 'i tıklayın.
- 6 **Ne** sekmesinde **Dosyaları ve klasörleri ekle veya dışla** seçeneğini tıklayın. Açılan pencerede aşağıdakilerden birini yapın:
 - **Dosya Ekle** veya **Dosyayı Dışla** seçeneğini tıklayın. **Dosyalara Gözet** penceresinde, eklenecek veya kaldırılacak dosyaya gidin ve **Aç** 'ı tıklayın.
 - **Klasör Ekle** veya **Klasörü Dışla** 'yı tıklayın. **Klasörlere Gözet** penceresinde, eklenecek veya kaldırılacak dosyaya gidin ve **Tamam** 'ı tıklayın.
- 7 **Yedekleme Kümelerini Yönet** penceresinde, **Ayarları Kaydet** 'i tıklayın.

Windows Explorer'da dosya ve klasörleri yedekleme kümesine ekleme veya yedekleme kümesinin dışında bırakma

- 1 Windows Explorer'da klasöre veya dosyayı sağ tıklayın, **Norton Security** 'yi seçin ve **Yedeklemeye Ekle / Yedekleme Dışında Bırak** 'a gidin.

Kısayol menüsündeki **Yedeklemeye Ekle / Yedekleme Dışında Bırak** seçeneği yalnızca yedeklemenizi yapılandırmanızdan sonra ve **Yedekleme Kümelerini Yönet** ve **Dosyaları Geri Yükle** pencereleri kapalı olduğunda etkinleştirilir.

- 2 Dosya veya klasörü dışlamak istediğiniz Yedekleme Kümesin'i tıklayın.

Norton yedekleme kümelerinden resimleri, müzik dosyalarını veya diğer önemli dosyaları geri yükleme

Fidye yazılımı veya diğer kötü amaçlı yazılımların kurbanıysanız veya kurtarılamaz donanım sorunları yaşarsanız Norton Yedekleme verilerinizi kolayca geri yükleyebilirsiniz. Yedekleme kümesindeki tüm yedek kümelerini veya belirli dosyaları geri yüklemeyi seçebilirsiniz. Yedeklenmiş dosyaların nereye geri yükleneceğini de belirleyebilirsiniz.

Norton yedekleme dosyalarını veya tüm yedekleme kümelerini geri yükleme

- 1 Norton'u Başlat.

Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.

- 2 Norton ana penceresinde **Yedekleme** öğesini çift tıklayın ve ardından **Dosyaları Geri Yükle** öğesini tıklayın.

- 3 **Dosyaları Geri Yükle** penceresinde, **Geri Yükleme Kaynağı** 'nın altında, **Tümünü Görüntüle** 'yi tıklayın.

Yedekleme kümesini ve ardından **Tamam** öğesini tıklayın.

- 4 **Dosyaları Geri Yükle** penceresinde, **Dosyalar** 'ın altında, **Dosyalara ve Klasörlere Gözet** öğesini tıklayın.

Geri yüklemek istediğiniz dosyaları seçin ve **Tamam** 'ı tıklayın.

- 5 **Dosyaları Geri Yükle** penceresinde, **Geri Yükleme Hedefi** 'nin altında, **Orijinal Konum** 'u tıklayın.

Konumu Değiştir 'i tıklayın ve orijinal konuma geri yüklemek istemiyorsanız talimatları izleyin.

- 6 **Dosyaları Geri Yükle** 'yi ve ardından **Kapat** 'ı tıklayın.

Norton yedeklemeyi açma

Yedekle seçeneği açık olduğunda, bilgisayarınız boştayken Norton ürününüz dosyalarınızı otomatik olarak yedekler. Öte yandan, yedeklemeyi geçici olarak devre dışı bırakmak isterseniz, yedeklemeyi programın içinden kapatabilirsiniz.

Yedeklemeyi kapattığınızda, Norton ürünü ana penceresindeki yedekleme durumu **Korumalı** durumundan **Devre dışı** durumuna dönüşür. Devre dışı durumunda, Norton ürününüz tüm otomatik dosya yedeklemelerini devre dışı bırakır. Tüm yedekleme kümelerinden dosyalarınızı yedeklemek istiyorsanız, ana penceredeki **Yedeklemeyi Çalıştır** seçeneğini kullanabilirsiniz.

Yedeklemeyi **Ayarlar** penceresinden, **Yedekleme Ayarları** penceresinden veya **Yedekleme Ayrıntıları** penceresinden kapatabilir veya açabilirsiniz.

Ayarlar penceresinden yedeklemeyi kapatın veya açın

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde **Hızlı Denetimler** altında aşağıdakilerden birini yapın:
 - Yedeklemeyi kapatmak için **Yedekle** 'nin işaretini kaldırın.
 - Yedeklemeyi açmak için **Yedekle** 'yi işaretleyin.

Norton Yedekleme Ayarları penceresinden yedeklemeyi kapatma veya açma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Yedekleme Ayarları** 'nı tıklayın.
- 4 **Yedekleme Ayarları** penceresinde, aşağıdakilerden birini yapın:
 - Yedeklemeyi kapatmak için **Açık/Kapalı** anahtarını **Kapalı** konuma getirin.
 - Yedeklemeyi açmak için **Açık/Kapalı** anahtarını **Açık** konuma getirin.
- 5 **Ayarlar** penceresinde **Uygula** 'yı tıklayın.

Yedeklemeyi Yedekleme Ayrıntıları penceresinden kapatma veya açma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Yedekleme** ögesini tıklatın ve ardından **Ayrıntıları Görüntüle** ögesini tıklatın.
- 3 **Yedekleme Ayrıntıları** penceresinde, **Yapabilecekleriniz** ögesinin altında, aşağıdakilerden birini yapın:
 - Yedeklemeyi kapatmak için, **Yedeklemeyi Kapat** 'ı tıklatın.
 - Yedeklemeyi açmak için **Yedeklemeyi Aç** 'ı tıklatın.

Norton ürününüzün ayarlarını özelleştirme

Ayarlar penceresinde, aşağıdaki **Hızlı Denetimler** hizmetlerini etkinleştirebilir veya devre dışı bırakabilirsiniz:

- Etkileşimsiz Mod
- Yedekleme
- Yedekleme Durumu Yer Paylaşımları
- Otomatik LiveUpdate
- Akıllı Güvenlik Duvarı
- Norton Müdahale Koruması

Etkileşimsiz Mod haricinde tüm hizmetleri açık bırakmanız önerilir.

Hızlı Denetimler hizmetlerini etkinleştirmek veya devre dışı bırakma

- 1 Norton'u Başlat.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ana penceresinde **Ayarlar** 'a tıklayın.
- 3 **Ayarlar** penceresinde **Hızlı Denetimler** altında aşağıdakilerden birini yapın:
 - Bir hizmeti etkinleştirmek için, o hizmetin onay kutusunu işaretleyin.
 - Bir hizmeti devre dışı bırakmak için, o hizmetin onay kutusundaki işareti kaldırın. Bir uyarı veya ileti görünürse, açılan menüden süreyi seçin ve ardından **Tamam** 'a tıklayın.

Gerçek Zamanlı Koruma ayarlarını özelleştirme

Gerçek Zamanlı Koruma, bilgisayarınızda bilinmeyen güvenlik risklerini algılar ve bir risk algıladığında hangi eylemin gerçekleştirileceğini belirlemenizi sağlar.

Not: Çoğu kullanıcı için varsayılan ayarlar önerilir. Özelliği geçici olarak kapatmayı tercih ederseniz, mümkün olan en kısa zamanda özelliği açın. Düşük riskli öğelerin otomatik olarak kaldırılmasını isterseniz, SONAR Gelişmiş modunu yapılandırın. Bilgisayarınızda bir program çalıştırdığınızda Auto-Protect virüsleri ve diğer güvenlik risklerini arar. Her zaman Auto-Protect özelliğini açık tutun.

Çıkarılabilir medyayı taramak için Auto-Protect'i ayarlama

Çıkarılabilir Medya Taraması, çıkarılabilir medya taktığınızda virüs olup olmadığını kontrol eder ve tamamlanması birkaç saniye sürer. Çıkarılabilir medya tarandıktan sonra, yeniden takılana veya biçimlendirilene kadar taranmaz. Hala çıkarılabilir medyanızın virüslü olduğundan şüpheleniyorsanız, Auto-Protect'i açın, çıkarılabilir ortamı yerleştirin ve yeniden taramak için Windows Gezgin'i'nde Otomatik Koruma'yı açın. Çıkarılabilir medyayı manuel de tarayabilirsiniz.

Otomatik Koruma ayarlarını özelleştir

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'e tıklayın.
- 4 **Çıkarılabilir Medya Taraması** altında, kaydırıcıyı **Aç** 'a getirin.

Tehditleri otomatik olarak kaldırmak üzere SONAR'ı ayarla

Symantec Online Network for Advanced Response (SONAR), tehditlere karşı gerçek zamanlı koruma sağlar ve bilgisayarınızdaki bilinmeyen güvenlik risklerini proaktif olarak tespit eder. SONAR, yeni çıkan tehditleri uygulamaların çalışma biçimine göre teşhis eder. SONAR Gelişmiş Modu ayarlarını kullanarak SONAR'ın bir tehdidi nasıl kaldırdığını yapılandırabilirsiniz.

Tehditleri otomatik olarak kaldırmak üzere SONAR'ı ayarla

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'e tıklayın.
- 4 **Riskleri Otomatik Olarak Kaldır** 'ın altında, kaydırıcıyı **Her zaman** 'a ayarlayın.

- 5 **Uzaktaysam Riskleri Kaldır** 'ın altında, kaydırıcıyı **Her zaman** 'a ayarlayın.
- 6 **Uygula** seçeneğine tıklayın.

Norton taramalarından bilinen iyi dosyaları dışlamak için Auto-Protect'i ayarlama

Norton'un geçerli bir uygulamayı bir güvenlik riski olarak tanımladığını düşünüyorsanız, dosyayı Norton taramalarından dışlayabilirsiniz.

Dosyaları Norton taramaları dışında bırakma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde, **Antivirüs** 'ü tıklayın.
- 4 Antivirüs ayarları penceresinde, **Taramalar ve Riskler** sekmesine tıklayın.
- 5 **Dışlamalar / Düşük Riskler** penceresinde, aşağıdakilerden birini yapın:
 - **Taramaların Dışında Tutulacak Öğeler** satırında **Yapılandır** 'a tıklayın.
 - **Auto-Protect ve SONAR ve Download Intelligence Tespitinin Dışında Tutulacak öğeler** satırında **Yapılandır** 'a tıklayın.
- 6 Çıkan pencereden **Klasör Ekle** 'ye veya **Dosya Ekle** 'ye tıklayın.
- 7 **Öğe Ekle** iletişim kutusunda göz at simgesine tıklayın. Çıkan iletişim kutusunda, taramadan dışlamak istediğiniz öğeyi seçin.
- 8 **Tamam** 'a tıklayın.

Taramalar ve Riskler ayarları

Taramalar ve Riskler ayarları, Norton tarafından bilgisayarınızda gerçekleştirilen taramaları özelleştirmenize olanak sağlar. Bilgisayarınızdaki dosyaların dijital imzalarına ve güven düzeyine bağlı olarak bir taramayı yapılandırabilirsiniz. Norton programının e-posta iletilerini tararken nasıl davranacağını tanımlayabilirsiniz.

Aşağıdaki **Taramalar ve Riskler** ayarlarını kullanabilirsiniz:

Bilgisayar Taramaları

Bilgisayarınızdaki virüslü öğeleri tespit etmek ve virüslerin bulaşmasını önlemek için farklı türlerde tarama yapabilirsiniz. Taramalar, Hızlı Tarama, Tam Sistem Taraması ve özelleştirilmiş taramalar'dır. Norton programının bilgisayarınızda yaptığı taramaları özelleştirmek için, **Bilgisayar Taramaları** seçeneklerini kullanabilirsiniz. Sıkıştırılmış dosyaların taranmasını de belirleyebilirsiniz.

Bilgisayar Taramaları seçenekleri; kök araç setleri, diğer gizli öğeler, izleme tanımlama bilgileri ve bilinmeyen güvenlik tehditlerini tespit etmek için kullanılacak taramayı belirtmenize olanak sağlar. Seçenekleriniz şunlardır:

■ **Sıkıştırılmış Dosya Taraması**

Sıkıştırılmış dosyaların içindeki dosyaları tarar ve onarır.

Bu özelliği etkinleştirdiğinizde Norton programı tarama yapar ve sıkıştırılmış dosyaların içindeki virüsleri, diğer güvenlik tehditlerini tespit eder ve sıkıştırılmış dosyaları kaldırır.

■ **Kök Araç Kümelerini ve Gizli Öğeleri Tarama**

Kök araç setleri ve bilgisayarınızda gizli olabilecek diğer güvenlik risklerine yönelik tarama yapar.

■ **Ağ Sürücülerini Taraması**

Bilgisayarınıza bağlı olan ağ sürücülerini tarar.

Norton **Tam Sistem Taraması** ve **Özel Tarama** sırasında **Ağ Sürücülerini Taraması** gerçekleştirir. Varsayılan olarak, **Ağ Sürücülerini Taraması** seçeneği açıktır. Bu seçeneği kapatırsanız Norton ağ sürücülerini taramaz.

■ **Sezgisel Koruma**

Bilinmeyen güvenlik tehditlerine karşı korumak için bilgisayarınızı tarar.

Norton virüslü olarak sınıflandırabilmek üzere bir dosyanın şüpheli özelliklerini aramak için sezgisel teknoloji kullanır. Bir dosyanın özelliklerini bilinen bir virüslü dosya ile karşılaştırır. Dosyada yeterli düzeyde şüpheli özellik varsa, Norton o dosyayı tehdit içeren virüslü dosya olarak tanımlar.

■ **İzleme Amaçlı Tanımlama Bilgileri Taraması**

Programların bilgisayar etkinliklerinizi izlemek amacıyla bilgisayarınıza yerleştirebileceği küçük dosyaları arar.

■ **Tam Sistem Taraması**

Tam Sistem Taraması tüm bilgisayarınızı virüslere, casus yazılımlara ve çeşitli güvenlik açıklarına karşı kapsamlı biçimde inceler. Tam Sistem Taraması'nı zamanlamak için **Yapılandır** seçeneğini kullanabilirsiniz.

Korunan Bağlantı Noktaları

Korunan Bağlantı Noktaları ayarları, e-posta programınızın POP3 ve SMTP bağlantı noktalarını korur.

E-posta koruması için POP3 ve SMTP e-posta bağlantı noktalarınızı manuel olarak yapılandırmak için bu seçeneği kullanabilirsiniz. İnternet servis sağlayıcınızın (ISP) e-posta programı için sağladığı SMTP ve POP3 bağlantı noktası numaraları varsayılan SMTP ve POP3

bağlantı numaralarından farklı ise, bağlantı noktalarını yapılandırmak için Norton ürününü yapılandırmanız gereklidir.

E-posta Antivirüs Taraması

E-posta Antivirüs Taraması sizi e-posta ekleriyle gönderilen veya alınan tehditlere karşı korur.

Norton programının e-posta iletilerini nasıl tarayacağını tanımlamak için E-posta Antivirüs Taraması seçeneklerini kullanabilirsiniz. Belirttiğiniz seçeneklere bağlı olarak, Norton gönderdiğiniz veya aldığınız e-posta iletilerini otomatik olarak tarar.

Dışlamalar / Düşük Riskler

Dışlamalar seçenekleri, Norton taramalarının dışında tuttuğunuz klasörler, dosyalar ve sürücüler gibi öğeleri belirler. Tarama imzaları ve düşük riskli öğeler, tarama dışında bırakabileceğiniz öğelerden bazılarıdır.

Dışlama seçenekleri Norton programının tespit etmesini istediğiniz risk kategorilerini seçmenizi de sağlar. Seçenekleriniz şunlardır:

■ Düşük Riskler

Bilgisayarınızda bulunan düşük riskli öğeleri yönetmenize olanak verir.

Düşük riskli öğelere Norton tarafından nasıl yanıt verileceğini belirtebilirsiniz.

■ Taramaların Dışında Tutulacak Öğeler

Risk taramasının dışında tutulacak diskleri, klasörleri veya dosyaları belirlemenizi sağlar.

Dışlanan öğeler listesine yeni dışlama öğeleri ekleyebilir veya varolanları düzenleyebilirsiniz.

Ayrıca dışlanmış öğeler listesinden öğe kaldırabilirsiniz.

■ Auto-Protect, SONAR ve İndirme Bilgi Merkezi Tespitinin Dışında Bırakılacak Öğeler

Auto-Protect taramalarının ve SONAR taramalarının dışında tutmak istediğiniz diskleri, klasörleri veya dosyaları saptamanızı sağlar.

Dışlanması gereken yeni öğeler ekleyebilir veya zaten dışlanmış öğeleri değiştirebilirsiniz.

Ayrıca dışlanmış öğeler listesinden öğe kaldırabilirsiniz.

■ Tüm Tespitlerin Dışında Tutulacak İmzalar

Bilinen riskleri ada göre seçmenize ve bir risk adını dışlanan öğeler listesinden kaldırmanıza olanak sağlar.

Ayrıca performans, gizlilik, kaldırma ve gizli etkiyi temel alarak riskin etkisini de görebilirsiniz.

■ Taramalar sırasında dışarda tutulan dosya Kimliklerini temizle

Tarama dışında tutulmuş olan dosyaların güvenilirlik bilgilerini kaldırmanızı sağlar.

Tarama dışında tutulmuş olan dosyaların güvenilirlik bilgilerini temizlemek için **Tümünü Temizle** seçeneğini kullanabilirsiniz.

Not: Dışlamalar koruma düzeyinizi düşürür ve yalnızca özel bir ihtiyacınız olduğunda kullanılmalıdır.

İzinsiz Giriş ve Tarayıcı Koruması ayarları

İzinsiz Giriş Önleme özelliği, bilgisayarınıza giren ve bilgisayarınızdan çıkan tüm ağ trafiğini tarar ve bu bilgiyi bir grup saldırı imzasıyla karşılaştırır. Saldırı imzaları, saldırının bilinen bir işletim sistemi veya program güvenlik açığından yararlanma girişimini tanımlayan bilgileri içerir. İzinsiz Giriş Önleme, bilgisayarınızı en yaygın internet saldırılarına karşı korur.

Bilgiler bir saldırı imzasıyla uyuşuyorsa, İzinsiz Giriş Önleme özelliği paketi otomatik olarak atar ve verileri gönderen bilgisayarla bağlantıyı keser. Bu eylem bilgisayarınızı herhangi bir şekilde etkilenmekten korur.

İzinsiz Giriş Önleme, şüpheli ağ etkinliklerini tespit eden ve engelleyen kapsamlı bir saldırı imzaları listesini temel alır. Norton ürünü, saldırı imzaları listenizi güncel tutmak için otomatik olarak LiveUpdate'i çalıştırır. Otomatik LiveUpdate kullanmıyorsanız, LiveUpdate'i haftada bir kez çalıştırmanız önerilir.

Norton ürünü, aynı zamanda tarayıcınızı kötü amaçlı programlardan korumak için Tarayıcı Koruması özelliğini de sunar.

Not: Tarayıcı Koruması özelliği Google Chrome, Microsoft Internet Explorer, Mozilla Firefox ve Microsoft Edge tarayıcıları için kullanılabilir.

İnternet kullanımı arttıkça, tarayıcınız zararlı web sitelerinin saldırılarına maruz kalır. Bu siteleri Web tarayıcınızın açıklarını tespit eder ve bunları kullanarak izniniz ve bilginiz olmadan zararlı programları sisteminize indirir. Bu zararlı programlara istenmeyen indirme programları da denir. Norton ürünü tarayıcınızı zararlı web sitelerinden bulaşabilen etkin indirmelerine karşı korur.

İzinsiz Giriş ve Tarayıcı Koruması ayarları, indirdiğiniz güvenli olmayan dosyalara karşı bilgisayarınızı korumak için **İndirme Bilgi Merkezi** seçeneğini de içerir. İndirme Bilgi Merkezi, tarayıcısını kullanarak indirdiğiniz yürütülebilir dosyanın güvenilirlik düzeyi hakkında bilgi verir. İndirme Bilgi Merkezi yalnızca HTTPS protokolünü, Internet Explorer 6.0 tarayıcısını veya sonrasını, Edge 40.15063 tarayıcısını, Chrome 10.0 tarayıcısını ve Firefox 3.6 tarayıcısını veya bunların daha yeni sürümlerini kullanan indirme işlemlerini destekler. İndirme Bilgi Merkezi'nin verdiği güvenilirlik bilgileri, indirilen dosyayı yüklemenin güvenli olup olmadığını gösterir. Yürütülebilir dosyayı yüklemek isteyip istemediğinize karar vermek için bu ayrıntıları kullanabilirsiniz.

Norton'u korunan cihazlarınızı uzaktan yönetmenizi sağlayacak şekilde ayarlama

Norton **Uzaktan Yönetim**, cihazınızın sağlık durumunu ve diğer bilgileri Windows için Norton Studio uygulamasına gönderir. Bu uygulamayı kullanarak Norton ürünlerini görebilir, yönetebilirsiniz veya keşfedebilir ve cihazınızdaki bazı koruma sorunlarını uzaktan düzeltebilirsiniz. Varsayılan olarak Uzaktan Yönetim kapalıdır.

Uzaktan Yönetim özelliğini açma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Yönetim Ayarları** 'nı tıklatın.
- 4 **Uzaktan Yönetim** satırında, anahtarı **Açık** konuma getirin.
- 5 **Uygula** öğesini ve ardından **Kapat** öğesini tıklatın.

Norton cihaz güvenlik ayarlarını yetkisiz erişimden koruma

Norton cihaz güvenlik ayarlarınızda izin verilmeyen değişiklikleri önlemek için **Parola Koruması Ayarları** ve **Norton Tamper Protection** 'ı açın.

- **Parola Koruması Ayarları**, cihaz güvenlik ayarlarını görmek veya değiştirmek için bir parola belirlemenizi sağlar.
- **Norton Tamper Protection**, bilinmeyen veya şüpheli uygulamaların ayarlarınızda yaptığı değişiklikleri denetler.

Parola Koruması Ayarları ve Norton Tamper Protection'ı açma veya kapatma

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklatın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklatın.
- 3 **Ayarlar** penceresinde **Yönetim Ayarları** 'nı tıklatın.
- 4 **Ürün Güvenliği** bölümünden:
 - **Parola Koruması Ayarları** satırında, anahtarı **Açık** veya **Kapalı** konuma getirin.
 - **Norton Tamper Protection** satırında, anahtarı **Açık** veya **Kapalı** konuma getirin. İstenirse, özelliğin kapalı kalmasını istediğiniz süreyi seçin ve ardından **Tamam** 'ı tıklatın.
- 5 **Uygula** 'yı tıklatın.

- 6 **Parola Belirle** penceresinde bir parola yazın ve onaylayın. Bu özelliği kapattığınız ve açtığınız her seferde bir parola belirlemeniz gerekir.
- 7 **Tamam** ögesini tıklayın.
- 8 **Ayarlar** penceresinde, **Kapat** 'ı tıklayın.

Norton Parola Koruması Ayarları'nın kaybedilen veya unutulmuş parolasını sıfırlama

Ayarlara erişmek ve yeni bir parola belirlemek için Norton'u yeniden yüklemeniz gerekir.

Norton cihaz güvenliğinde bilgi aramak için kısayol tuşu belirleme

Norton cihaz güvenliği uygulamasında



simgesini kullanarak arama yaptığınızda Norton özelliği ve destek bilgilerinin yanı sıra genel konularda da çevrimiçi bilgi bulabilirsiniz. **Ctrl + F** varsayılan klavye kısayolunu kullanarak daha hızlı arama başlatabilir veya kısayol belirleyebilirsiniz.

Arama Kısayol Tuşu Belirleme

- 1 Norton'u başlatın.
Aygıt Güvenliği 'nin yanındaki **My Norton** penceresini görürseniz **Aç** 'ı tıklayın.
- 2 Norton ürünü ana penceresinde **Ayarlar** 'ı tıklayın.
- 3 **Ayarlar** penceresinde **Yönetim Ayarları** 'nı tıklayın.
- 4 **Kısayol Anahtarı Ara** satırında, anahtarı **Açık** konuma getirin.
- 5 Oku tıklayın, ardından üründe aramaya atamak istediğiniz anahtarı seçin.
- 6 Aşağıdakilerden birini yapın:
 - Kısayol anahtarının yalnızca Norton ürününüzün bir odağı varken çalışması için **Küresel** seçeneğinin **işaretini kaldırın**.
 - Kısayol anahtarının Norton ürününüzün bir odağı **yokken** dahi çalışması için **Küresel** seçeneğini **işaretleyin**.
- 7 Önce **Uygula** 'yı, ardından **Kapat** 'ı tıklayın.

Ek çözümler bulma

Bu bölümde aşağıdaki konular yer almaktadır:

- [Cihaz Güvenliğini Kaldırın](#)
- [Sorumluluk Reddi](#)

Cihaz Güvenliğini Kaldırın

Cihaz Güvenliğini bilgisayarınızdan aşağıdaki yollarla kaldırabilirsiniz:

- Windows **Denetim Masası** 'ndan.
- **Başlat** menüsünden.
- Windows **Başlat** ekranından (Windows 8/8.1).

Not: Kaldırma işlemine başlamadan önce bu yardım konusu yazdırmanızı öneririz. Kaldırma işlemi sırasında çevrimiçi Yardıma erişemezsiniz.

Cihaz Güvenliğini Windows Denetim Masası 'ndan Kaldırma

- 1 Aşağıdakilerden birini yapın:
 - Windows Görev Çubuğunda, **Başlat > Denetim Masası** 'na tıklayın.
 - Windows 8'de, **Uygulamalar** 'a gidin ve **Windows Sistemi** bölümünde **Denetim Masası** 'na tıklayın.
 - Windows 10'da, **Başlat > Tüm uygulamalar** 'a tıklayın, **Windows Sistemi** altında, **Denetim Masası** öğesine tıklayın.
- 2 Windows **Denetim Masası** 'nda aşağıdakilerden birini yapın:
 - Windows 8 ve 7'de **Programlar > Programlar ve Özellikler** öğesine tıklayın.

Programlar seçeneği **Görüntüleme ölçütü** açılır listesindeki **Kategori** seçeneğini seçtiğinizde kullanılabilir.

- Windows 10'da **Program kaldır** 'a tıklayın.
- 3 Yüklü programlar listesinde aşağıdakilerden birini yapın:
- Windows 7, Windows 8 veya Windows 10'da, önce Norton ürününüze ve ardından **Kaldır/Değiştir** 'e tıklayın.
- 4 Ekrandaki talimatları izleyin.
- Cihaz Güvenliği bilgisayarınız yeniden başlatılana kadar tam anlamıyla kaldırılmış olmaz.

Cihaz Güvenliğini Başlat menüsünden kaldırma

- 1 Windows görev çubuğunda, **Başlat > Tüm Programlar/Tüm uygulamalar > Norton > Norton Programını Kaldır ögesine** tıklayın.
 - 2 Norton Giriş Sayfası'nı varsayılan ana sayfanız ve Norton Safe Search'ü varsayılan arama sağlayıcınız olarak tutmak istemiyorsanız en altta görünen onay kutusunu işaretleyin.
 - 3 Ekrandaki talimatları izleyin.
- Cihaz Güvenliği bilgisayarınız yeniden başlatılana kadar tam anlamıyla kaldırılmış olmaz.

Windows 8/8.1'de Cihaz Güvenliğini Başlat ekranından kaldırın

- 1 **Başlat** ekranından Norton ürününüzü sağ tıklayın ve ardından **Kaldır** ögesine tıklayın.
 - 2 Şu anda yüklü programlar listesinde Norton ürününüzü tıklayın ve ardından **Kaldır/Değiştir** ögesine tıklayın.
 - 3 Ekrandaki talimatları izleyin.
- Norton ürününüz bilgisayarınızı yeniden başlatana kadar kaldırılmış olmaz.

Sorumluluk Reddi

Telif hakkı © 2019 Symantec Corporation. Tüm hakları saklıdır. Symantec, Symantec Logosu, Checkmark Logosu, Norton, Norton by Symantec, LifeLock ve LockMan Logosu ABD ve diğer ülkelerde Symantec Corporation şirketinin veya yan kuruluşlarının ticari markaları veya tescilli ticari markalarıdır. Firefox Mozilla Kuruluşunun ticari markasıdır. Google Chrome ve Android, Google, LLC'nin ticari markalarıdır. Mac, iPhone ve iPad, Apple Inc. şirketinin ticari markalarıdır. Microsoft ve Windows logosu, Microsoft Corporation şirketinin ABD'deki ve/veya diğer ülkelerdeki ticari markalarıdır. Android robot, Google tarafından üretilen ve paylaşılan işten çoğaltılır veya değiştirilir ve Creative Commons 3.0 Attribution License'a göre kullanılır. Diğer adlar ilgili sahiplerinin ticari markaları olabilir.