

İZMAD BİLİŞİM İNTERNET HİZMETLERİ BİLGİ TEKNOLOJİLERİ İTHALAT İHRACAT SANAYİ TİCARET LİMİTED ŞİRKETİ

Cumhuriyet Mahallesi, Demirel Sk. No: 25, 45400 Turgutlu / MANİSA

Doküman No: BF.01

Yayın Tarihi: 17.08.2026

Revizyon No/Tarih: 00

Sayfa: 1/2

ABONE BİLGİ GÜVENLİĞİ BİLGİLENDİRMESİ Zararlı Yazılımlara (Malware) Karşı Korunma ve Müdahale Rehberi

1. Amaç ve Kapsam

İZMAD olarak, abonelerimizin internet hizmetini kesintisiz ve güvenli biçimde kullanabilmesi önceliğimizdir. Bu bilgilendirme metni; kişisel bilgisayar, telefon, tablet ve ağ cihazlarınızın zararlı yazılımlarla (virüs, truva atı, fidye yazılımı, casus yazılım vb.) karşılaşması durumunda yapmanız gerekenleri ve bu tür tehditlerden korunmak için almanız gereken önlemleri açıklamak amacıyla hazırlanmıştır. İşbu metin, İZMAD internet sitesinde yayımlanır, talep eden abonelere iletilir ve abonelik sözleşmesinin ayrılmaz bir eki olarak kabul edilir.

2. Zararlı Yazılım (Malware) Nedir?

Zararlı yazılım; cihazlara sahibinin bilgisi ve izni dışında bulaşarak verileri çalan, şifreleyen, cihazın performansını düşüren veya cihazı üçüncü kişilerin kontrolüne açan yazılımların genel adıdır. Başlıca türleri şunlardır: virüsler, truva atları (trojan), fidye yazılımları (ransomware), casus yazılımlar (spyware), reklam yazılımları (adware) ve oltalama (phishing) yoluyla yayılan zararlı bağlantı/ekler.

3. Bulaşma Belirtileri

Cihazınızda aşağıdaki durumları fark ederseniz zararlı yazılım bulaşmış olabilir:

- Cihazın belirgin biçimde yavaşlaması, sık sık donması veya çökmesi,
- Kendiliğinden açılan reklamlar/pencereler, tanımadığınız program veya araç çubukları,
- Web tarayıcısının bilinmeyen/şüpheli sitelere yönlendirilmesi,
- Anormal derecede yüksek internet ve veri kullanımı,
- Parolaların çalışmaması veya hesaplara erişilememesi,
- Dosyaların şifrelendiğini belirten ve para (fidye) talep eden ekran uyarıları.

4. Zararlı Yazılımla Karşılaştığınızda Yapmanız Gerekenler

- Cihazı ağdan ayırın:** İnternet ve Wi-Fi bağlantısını kesin; zararlı yazılımın diğer cihazlara yayılmasını ve verilerinizin dışarı sızmasını önleyin.
- Fidye ödemeyin:** Fidye yazılımı durumunda ödeme yapmak verilerinizin geri geleceğini garanti etmez ve suçu teşvik eder.
- Tam tarama yapın:** Güncel bir güvenlik/antivirüs yazılımıyla cihazınızı baştan sona tarayın; tespit edilen tehditleri temizleyin veya karantinaya alın.
- Parolalarınızı değiştirin:** Başta e-posta, bankacılık ve sosyal medya olmak üzere parolalarınızı temiz/başka bir cihazdan değiştirin; mümkünse iki adımlı (2FA) doğrulamayı etkinleştirin.
- Finansal kontrol yapın:** Kart veya banka bilgilerinizi girdiyseniz derhal bankanızla iletişime geçin ve hesap hareketlerinizi takip edin.
- Verilerinizi kurtarın:** Etkilenmemiş yedeklerinizden geri yükleme yapın; yedeğiniz yoksa cihazı yetkili servise götürün.
- Profesyonel destek alın:** Sorun devam ederse konusunda uzman teknik destekten veya yetkili servisten yardım isteyin.

5. Korunmak İçin Alınması Gereken Önlemler

- İşletim sistemi, tarayıcı ve uygulamaları güncel tutun; güvenlik güncellemelerini ertelemeyin.
- Lisanslı ve güncel bir antivirüs/güvenlik yazılımı kullanın.
- Tanımadığınız kişilerden gelen e-posta eklerini ve bağlantıları açmayın; oltalama (phishing) girişimlerine karşı dikkatli olun.
- Korsan yazılım ve güvenilmeyen kaynaklardan program indirmeyin.
- Her hesap için güçlü ve farklı parolalar kullanın; mümkün olan yerlerde iki adımlı doğrulamayı açın.
- Modem/router cihazınızın varsayılan yönetici parolasını değiştirin ve cihaz yazılımını güncel tutun.
- Önemli verilerinizin düzenli yedeğini alın (harici disk veya güvenli bulut).
- Çocukların kullanımı için içerik/erişim filtreleme çözümlerinden yararlanın.

6. İZMAD Servis Sağlayıcısı Olarak İZMAD'ın Rolü

İZMAD, şebeke seviyesinde bilgi güvenliğini sağlamaya yönelik teknik tedbirleri (istenmeyen posta/spam, DoS/DDoS ve kötü amaçlı trafiğe karşı koruma, teknik zafiyet yönetimi) uygular ve 5651 sayılı Kanun ile ilgili mevzuata uygun olarak faaliyet gösterir. Bununla birlikte, abonenin kendi uç cihazlarının ve yerel ağının güvenliği (antivirüs kullanımı, güncelleme, parola yönetimi vb.) aboneye aittir. Bilgi güvenliği, İZMAD ile abonenin ortak sorumluluğudur.

7. İhbar ve Destek Kanalları

Şüpheli bir durumla karşılaştığınızda öncelikle İZMAD Müşteri Hizmetleri / Teknik Destek birimimizle iletişime geçebilirsiniz:

- Telefon: 0236 314 84 64 E-posta: guvenlik@waaynet.com.tr Web: waaynet.com.tr

Zararlı bağlantı, oltalama (phishing) sitesi ve siber güvenlik olaylarını ayrıca Ulusal Siber Olaylara Müdahale Merkezi'ne (USOM) bildirebilirsiniz.

8. Yürürlük ve Onay

Bu bilgilendirme metni yayımı tarihinde yürürlüğe girer ve gerektiğinde güncellenir.

İZMAD BİLİŞİM İNTERNET HİZMETLERİ BİLGİ TEKNOLOJİLERİ İTH. İHR. SAN. TİC. LTD. ŞTİ.

Üst Yönetim (Ad-Soyad / Unvan / İmza-Kaşe)