Dünyanın En Büyük Siber Saldırıları, Zararları ve Alınmakta olan Önlemler, Bireylerin Verilerinin ve Banka Hesaplarının Güvenliği? Türkiye'deki Durum?

Hazırlayan: Çeşitli kaynaklardan ve YZ ile yazışmayla Yüksel Atakan
ybatakan4@gmail.com **30.07.2025**

Bu yazı, bugüne kadar en büyük siber saldırılar, bu saldırıların yol açtığı zararlar ve özellikle bankacılık sektöründe günümüzde alınan önleyici önelemlerle ilgili ayrıntılı bilgiler sunmaktadır. Bu yazıda, 2017 öncesi ve sonrası gerçekleşen önemli siber saldırılar, geliştirilen yeni güvenlik yazılımları ve bireylerin kendi veri ve banka hesaplarını nasıl koruyabileceğiyle ilgili **öneriler** de yer almaktadır.

🌐 Dünyanın En Büyük Siber Saldırıları (2017 ve Öncesi)

Saldırı Adı	Yıl	Hedef	Tahmini Zarar
NotPetya (ExPetr)	2017	Küresel (özellikle sanayi ve altyapı)	~10 milyar USD
WannaCry fidye yazılımı	2017	Sağlık dahil birçok sektör	Yüz milyonlarca USD
Equifax veri ihlali	2017	Kredi derecelendirme kuruluşu	~1,4 milyar USD
Carbanak/Cobalt APT	2014-2015	Küresel finans kurumları	900 milyon - 1 milyar USD
Bangladeş Bankası SWIFT soygunu	2016	Merkez bankası (SWIFT ağı)	101 milyon USD
SWIFT ağ saldırıları (APT-38, Lazarus)	2015-2016	Birçok banka	Milyonlarca USD

2017 Sonrası Dünya'daki Büyük Siber Saldırılar

Saldırı & Tarih **Tahmini Zarar / Etki**

	Hedef / Etki	
Health Service Executive (2021)	İrlanda sağlık sistemi	Hizmet kesintisi, veri sızıntısı
Colonial Pipeline (2021)	Yakıt dağıtım altyapısı	4,4 milyon USD
MOVEit veri sızıntısı (2023)	2700 kurum, 93 milyon kişi	Geniş veri sızıntısı
Kyivstar saldırısı (2023)	Telekom altyapısı	~90 milyon USD
Kadokawa/Niconico (2024)	Japonya medya platformları	254.000 kullanıcı verisi
Aeroflot saldırısı (2025)	Rusya havayolu sistemi	On milyonlar USD
Volt Typhoon operasyonu (2023-2025)		AB

Bangladeş Bankası SWIFT Soygunu (2016)

Saldırganlar Bangladeş Merkez Bankası'nın iç sistemlerine sızarak SWIFT üzerinden sahte transfer talimatları göndermiştir. Toplamda 951 milyon USD'lik işlem denenmiş, 101 milyon USD başarıyla çekilmiştir. 81 milyon USD Filipinler'deki hesaplara aktarılmış, 18 milyon USD kurtarılmış, geri kalanı kumarhaneler aracılığıyla aklanmıştır.
Saldırının arkasında Kuzey Kore bağlantılı Lazarus/APT38 grubunun olduğu düşünülmektedir.

Çin Kaynaklı ABD Borsası İddiası

Basında 1 trilyon USD'lik piyasa değer kaybının Çin kaynaklı bir siber saldırı sonucu olduğu iddiaları yer almıştır. Ancak gerçekte bu kayıp, Çin merkezli DeepSeek adlı bir yapay zeka şirketindeki veri ihlalinin ve yapay zeka hisselerinde yaşanan satış dalgasının sonucudur. ABD borsa altyapısına yönelik doğrudan bir siber saldırı tespit edilmemiştir.

Bankacılık Sektöründe Siber Saldırıların Maliyeti

Bankacılık sektöründe bir veri ihlalinin ortalama maliyeti yaklaşık 5,9 milyon USD civarındadır. Çalınan her kayıt başına ortalama maliyet 181 USD'dir. Büyük ölçekli saldırılarda toplam zarar milyonlarca dolara ulaşmaktadır.

Bankaların Aldığı Önleyici Önlemler

- Düzenleyici denetimler (CBEST, SIMEX, ECB testleri)

- Çok faktörlü kimlik doğrulama (MFA)

- Yapay zeka tabanlı tehdit algılama sistemleri

- Zero-trust ağ güvenliği

- Tedarikçi ve üçüncü taraf risk yönetimi

- Olay müdahale planları

- Fidye ödemelerinin raporlanması

Günümüzde Kullanılan Yeni Siber Güvenlik Yazılımları

- ESET PROTECT Complete (2025) – Çok katmanlı koruma, AI tabanlı tehdit önleme

- Malwarebytes – Kötü amaçlı yazılım temizleme

- Avast / AVG Free Antivirus – Ücretsiz virüs koruma

- SUPERAntiSpyware – Spyware temizleme

- CISA ücretsiz siber güvenlik araçları – Kurumsal ve bireysel koruma

- AI destekli tehdit avı ve davranışsal analiz sistemleri

Kişisel Veri ve Banka Hesabı Koruma Önerileri

Kişisel Veri ve Banka Hesabı Korunması İçin Öneriler

1. **Güncel Kalmak**
   - İşletim sistemi, tarayıcı, antivirüs ve uygulamalarınızı **otomatik güncelleme** ile sürekli güncel tutun.
2. **Güçlü ve Ayrı Parolalar Kullanımı**
   - Benzersiz, karmaşık şifreler oluşturun; **parola yöneticisi** (Bitwarden, 1 Password gibi) kullanın.
3. **Çok Faktörlü Kimlik Doğrulama (MFA)**
   - Banka ve e-posta hesaplarında mutlaka SMS, uygulama ya da biyometriyle desteklenen MFA'yı etkinleştirin.
4. **Güvenilir Antivirüs & Anti-malware**
   - **Malwarebytes**, **Avast/AVG**, hatta **ESET Free** gibi çözümleri düzenli taramalarla destekleyin.
5. **Kimlik Avı ve Sosyal Mühendislik Farkındalığı**
   - Şüpheli e-postalara tıklamayın, bağlantılara şifre girilmeden önce mutlaka URL kontrolü yapın.
6. **VPN Kullanımı ve Açık Wi-Fi'lardan Kaçınma**

    - Güvenilmeyen ağlarda VPN kullanın; bankacılık ya da hassas işlemleri asla açık Wi-Fi üzerinden gerçekleştirmeyin.
7. **Veri Yedeklemesi ve Şifreleme**
    - Önemli dosyaları dış depolarda ya da güvenli bulutlarda yedekleyin; cihazları şifreleyin.
8. **Siber Sigorta ve Kimlik Hırsızlığı Koruması**
    - **Aura**, **IdentityForce**, **Experian IdentityWorks** gibi kimlik koruma hizmetleri, kredi izleme ve sigorta seçenekleriyle ek koruma sağlar techradar.com.
9. **Sosyal Medya ve Kişisel Bilgi Koruması**
    - Kişisel verilerini sınırlı paylaşımlarla koru, sosyal medya gizlilik ayarlarını kontrol et.

Türkiye'de Bilinen Siber Saldırılar ve Etkileri

(Kaynaklar yazı içinde)

1. TurkNet Veri Sızıntısı (Mart 2025)

- **Mart 2025'te**, TurkNet'e ait milyonlarca kullanıcının verisinin çalındığı iddiası gündeme geldi; kimlik numaraları ve IP bilgileri dahil edildi elazighakimiyethaber.com+1NTV Haber+1Reddit.
- Reddit kullanıcılarına göre fidye talepleri de olmasına rağmen firma reddetmiş; zarar net bir rakamla açıklanmadı fakat büyük kullanıcı kitlesi etkilendi Reddit.

2. Finans Kuruluşları ve BTC Türk Dolandırıcılığı

- **Mart 2025**'te BTC Türk kullanıcılarının bazı işlemlerinde, USDT adresleri saldırı sonucu değişmiş; kullanıcılar habersiz para kaybına uğramış. Yaklaşık 1.500 USD zarar eden kullanıcılar bildirildi Reddit.

3. Elektrik Sistemi Hedefli Siber Tehditler

- Enerji ve Tabii Kaynaklar Bakanlığı, **sistemlerine yönelik çok sayıda siber sızma girişimi** tespit edip engellediğini duyurdu. Ulusal elektrik şebekesine yönelik sabotaj planlaması olarak değerlendirildi. Özellikle 15 Temmuz sonrası bu tür tehditlerin arttığı, yılbaşı için benzer saldırı uyarıları alındığı bildirildi milliyet.com.tr+5NTV Haber+5cnnturk.com+5.

4. Anadolu Enerji ve Üretim Saldırıları (2022–2023 kapsamıyla)

- **2022 ikinci yarısında**; enerji, üretim ve bina otomasyonu gibi sektörlerde fidye yazılımları ve zararlı komut dosyalarına karşı önemli artış yaşandı. Türkiye, ICS

sistemlerine yönelik saldırılarda Orta Doğu'da öne çıkan ülkelerden biri oldu haber7.com.

5. Genel Durum: Günlük Saldırı Hacmi

- Ulaştırma ve Altyapı Bakanı'na göre, Türkiye genelinde "günde yaklaşık **500 siber saldırı** devlet ve finans sistemi hedeflerine karşı engelleniyor" cnnturk.com+2NTV Haber+2elazighakimiyethaber.com+2.
- 2023'teki genel siber tehdit sayısında %5 artış, özellikle banka kötü amaçlı yazılım saldırılarında %18 artış görülmüş; Türkiye dünya genelinde hedef ülkeler arasında üst sıralarda yer aldı elazighakimiyethaber.com+1NTV Haber+1.

Zararın Büyüklüğü

- **Ekonomik zararlar**: 2024 sonunda dünya çapında siber saldırıların maliyetinin 9.5 trilyon USD'nin üzerine çıkması bekleniyor. Türkiye bireysel ve kurumsal olarak giderek daha fazla zarar görüyor; küçük ve orta ölçekli işletmeler en fazla risk altında elazighakimiyethaber.commilliyet.com.tr.
- Finansal sektörde geçmişte fiduciary saldırılarda Türkiye'de **CryptoLocker** saldırıları sonrası yaklaşık 30 milyon USD fidye ödendiği kaydedildi aa.com.tr.

Siber Güvenlik Önlemleri: Devlet & Bankalar

Kamu Kurumları:

- 2025 yılı başında **Siber Güvenlik Başkanlığı** (Cumhurbaşkanlığı'na bağlı, Ankara merkezli) kuruldu. Siber strateji ve koordinasyon görevini üstlenen kurumla kamu güvenliği kuvvetlendiriliyor; personel sayısı başlangıçta 135 kişi olarak belirlendi Reddit.
- TR-CERT (USOM), **Ulusal Siber Olaylara Müdahale Merkezi** olarak faaliyet gösteriyor. Kritik altyapılara ve kamu sektörüne yönelik tehditleri analiz edip müdahale ediyor; birden fazla sektör CSIRT'i ile koordineli çalışıyor en.wikipedia.org+1NTV Haber+1.

Bankalar ve Finans:

- Bankalar ve finans kuruluşları **BRSA, CMB ve TRCB** düzenlemeleri kapsamında sıkı bilgi güvenliği yükümlülükleri altındadır. Tüm bankaların COBIT standardına uygun denetimden geçmesi ve ISO/IEC 27001 belgelerine yönlendirilmesi yaygın uygulamadır mondaq.com+1practiceguides.chambers.com+1.
- Payment Card Industry Data Security Standard (PCI DSS) gibi kart güvenliği standartlarına da uyum zorunluluğu var.

- 30 Haziran 2025'te yürürlüğe giren "Financial NIS" düzenlemesiyle, finansal kuruluşların kritik bilgi sistemlerinin izlenmesi, raporlanması ve yerel altyapıda tutulması gibi yükümlülükler belirlenmiştir practiceguides.chambers.com.

Özel Sektör:

- Büyük şirketlerde güvenlik yatırımları iyi durumda olsa da **KOBİ'ler ve bazı kamu kurumları** hâlâ yeterli önlemi almış değil. Türkiye'nin ilk 15 saldırıya maruz kalan ülke arasında yer aldığı vurgulanıyor milliyet.com.trhaber7.com.

Özet Tablo

Unsur	Durum ve Uygulamalar
Bilinen Saldırılar	TurkNet veri sızıntısı; finans dolandırmaları; enerji sektörü hedefli saldırılar
Zarar Büyüklüğü	Milyon dolarlık fidyeler ve kişisel veri kayıpları; günlük 500 saldırı engelleniyor
Kamu Güvenliği	TR-CERT / USOM operasyonel; Siber Güvenlik Başkanlığı kuruldu
Finansal Sektör	COBIT, ISO 27001, PCI DSS, Financial NIS ile sıkı güvenlik düzenlemeleri
Genel (Özel/Özel Sektör)	Büyük kurumlar iyi durumda; KOBİ'ler, e-ticaret ve belediyelerde eksikler var

✅ Sonuç

Evet, **Türkiye'de son dönemde ciddi siber saldırılar gerçekleşti**, özellikle telekom ve finans sektörü gibi alanlarda kullanıcı bazlı veri kayıpları ya da saldırılar raporlandı. Devlet ve bankalar **güvenlik önlemlerini sistematik olarak alıyor**, yeni kurumlar kuruyor ve global standartlara göre düzenlemeler yapıyor. Buna karşılık özellikle orta ölçekli özel kurumlarda hâlâ güvenlik yatırımlarında eksiklikler mevcut.

Türkiye'de bireylerin bankalardaki hesap güvenliği ve saldırı durumunda paralarının garanti altında olup olmadığı hem yasal hem de pratik açıdan birkaç boyutta ele alınabilir.

1. Banka Hesaplarının Siber Güvenliği

Bankalar, **Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)** ve **Türkiye Cumhuriyet Merkez Bankası (TCMB)** düzenlemelerine uymak zorunda. Bu düzenlemeler, bireysel müşteri hesaplarının korunması için şu teknik önlemleri kapsar:

- **Çift faktörlü kimlik doğrulama (2FA)**: Mobil onay kodu, biyometrik giriş (parmak izi, yüz tanıma).
- **PCI DSS ve ISO 27001 standartlarına uyum**: Kart ve müşteri verilerinin güvenli saklanması.
- **Gerçek zamanlı işlem izleme**: Şüpheli işlemleri anlık olarak durdurma (fraud detection).
- **Otomatik oturum kapatma** ve cihaz doğrulama.
- **Veri şifreleme** (hem saklama hem iletim sırasında).

Bu önlemler, bankanın kendi sisteminde oluşabilecek siber saldırı riskini en aza indirir.

2. Para Kaybı Durumunda Bankanın Sorumluluğu

Bankacılıkta, **hesaptan izinsiz işlem** tespit edilirse kural olarak **müşteri mağduriyeti bankanın kusuru oranında karşılanır**.

- Eğer **bankanın güvenlik açığı** nedeniyle saldırı olduysa, banka **tamamen zararı karşılamak zorundadır** (BDDK mevzuatı ve Türk Borçlar Kanunu gereği).
- Eğer **müşteri güvenlik kurallarını ihlal ettiyse** (şifre paylaşımı, sahte siteye giriş, cihaz virüslü vb.), banka tüm zararı karşılamayabilir. Ancak çoğu banka bu durumlarda bile müşteri lehine kısmi ödeme yapar.

Önemli: Türkiye'de **Mevduat Sigorta Fonu** (TMSF) sadece **bankanın batması** durumunda 2025 yılı itibarıyla **1,5 milyon TL'ye kadar mevduatı garanti eder**. Bu sigorta **siber saldırı zararları** için değil, **banka iflası** için geçerlidir.

3. Bankaların Fiili Uygulamaları

- **Ziraat, Garanti BBVA, İş Bankası, Akbank** gibi büyük bankalar, müşteriden onay alınmadan gerçekleşen işlemlerde genelde zararı hızlıca telafi eder.
- Bankalar, **"müşteri kusuru yoksa"** prensibiyle hareket eder; işlem sırasında bankanın fraud sistemleri uyarı verdiyse ve yine işlem yapılmışsa, bu genelde banka sorumluluğuna girer.
- Uluslararası kartlı işlemlerde (Visa, Mastercard) "**Chargeback**" (ters ibraz) hakkı vardır. Kartınızdan izinsiz çekim olursa 120 gün içinde itiraz edebilirsiniz.

Özet

- **Banka sisteminden kaynaklı saldırılarda** para kaybı %100 banka tarafından karşılanır.
- **Müşteri dikkatsizliği** varsa (şifre paylaşımı, oltalama linkine tıklama vb.) banka yine zararın bir kısmını karşılayabilir, fakat garanti değildir.
- **TMSF** siber saldırı için değil, **banka iflası** için teminat sağlar.
- Kredi kartı ve online işlemlerde **chargeback** ve **itiraz hakkı** mevcuttur.

EK BİLGİLER

Türkiye'de Banka Hesabından İzinsiz Para Çekildiğinde İtiraz ve Para İadesi Süreci

1. İzinsiz İşlemi Fark Ettiğiniz Anda Yapılacaklar

✅ Adım 1: Banka ile Hemen İletişime Geçin

- Bankanızın **müşteri hizmetlerini arayın** (7/24 çağrı merkezi).
- Şüpheli işlemi bildirerek:
  - Hesabı geçici olarak **dondurtun**,
  - Kartınızı **iptal ettirin**,
  - İşlem hakkında detay isteyin.

✅ Adım 2: Mobil/E-posta Bildirimlerini Kontrol Edin

- İşlemin saatini, hangi cihazdan yapıldığını, IP adresini, işlem türünü kaydedin.

2. Resmî Başvuru Süreci

✅ Adım 3: Yazılı Şikayet Başvurusu Yapın

Bankanıza **e-posta, mobil uygulama veya şubeden yazılı başvuru** yaparak:

- İşlemin size ait olmadığını,
- Onay vermediğinizi,
- Para iadesi talep ettiğinizi açıkça belirtin.

Bankaların bu başvurulara **20 iş günü içinde yazılı cevap verme zorunluluğu vardır.**

3. Hukuki ve İdari Süreçler

✅ Adım 4: Savcılığa Suç Duyurusunda Bulunun

- E-devlet veya doğrudan Cumhuriyet Başsavcılığı'na başvurarak:
  - "Bilişim yoluyla dolandırıcılık"
  - "Kredi kartı ve banka dolandırıcılığı"
    suçlamasıyla **şikayet dilekçesi** verebilirsiniz.

✅ Adım 5: Bankanın Cevabı Olumsuzsa – Tüketici Hakem Heyeti

- Zararınız **104.000 TL (2025 limiti)** altındaysa, bankanın bulunduğu il/ilçedeki **Tüketici Hakem Heyeti'ne** başvurabilirsiniz.
- Daha yüksek miktarlar için **Tüketici Mahkemesi'ne** veya **bankaya karşı dava açabilirsiniz**.

4. Kredi Kartı İşlemiyse – Chargeback Hakkı (Kartlı İşlemler)

✅ Adım 6: Bankanızdan "Chargeback" (Ters İbraz) Talep Edin

Eğer işlem bir alışveriş, rezervasyon veya ödeme işlemiyse:

- İşlem tarihinden itibaren **120 gün içinde** bankanıza chargeback talebinde bulunabilirsiniz.
- Banka kartı sağlayıcısına (Visa, Mastercard) başvurarak işlemin iptalini talep eder.

Not: Dijital ürünlerde veya şifreli satışlarda chargeback başarısı daha düşüktür.

5. Gerekli Belgeler

Başvurularınızda şunları ekleyin:

- İşleme ait ekran görüntüsü (tarih/saat açık olmalı)
- Banka dekontları
- Kimlik fotokopiniz
- Varsa önceki banka yazışmaları ve çağrı merkezi kayıtları
- Savcılık şikayet belgesi

✅ Sonuç Ne Olur?

Durum	Banka Parayı Geri Öder mi?
Banka sisteminden sızma varsa	%100 iade zorunluluğu
Kart şifresi çalındıysa ama siz paylaşmadıysanız	Genellikle iade edilir
Linke tıkladıysanız, OTP verdiniz	Kısmi iade olabilir
Kartı kaybettiyseniz ve bildirmediyseniz	Müşteri sorumluluğunda kabul edilir

---

İpuçları ve Uyarılar

- **İşlemleri düzenli kontrol edin.**
- **Mobil bankacılığa biyometrik doğrulama koyun.**
- **Kredi kartlarını internete açık bırakmayın.**
- Şüpheli bir mesaj ya da link geldiğinde **asla tıklamayın**.
- Dolandırıcılık durumlarında **bilgi teknolojileri uzmanı (bilirkişi)** gerekebilir, avukattan destek alabilirsiniz.

Kaynaklar

- Wikipedia – Bangladesh Bank robbery
- Reuters – Cyber Heist Federal Investigation
- Wikipedia – Colonial Pipeline attack, MOVEit breach, Kyivstar cyberattack
- CISA – Free Cybersecurity Tools
- PRNewswire – ESET Protect Complete 2025
- TechRadar – Best Identity Theft Protection 2025