2025'te Güçlü Parola Güvenliği: En Son Teknikler ve Trendler

Proje Özeti:
Bu rapor, kullanıcıdan alınan parolaların güvenliğini analiz eden ve gerekirse daha güçlü parola önerileri sunan bir araç geliştirmek amacıyla, 2025 yılı ve sonrası için en son ve en etkili 10 parola güvenliği tekniği ve trendini derinlemesine incelemektedir. Araştırma, mevcut ve gelecekteki tehditleri ele alarak, kanıta dayalı ve uygulanabilir çözümler sunmayı hedeflemektedir.

Giriş: Parola Güvenliğinin Değişen Manzarası

Dijital Tehdit Ortamının Evrimi ve Parolaların Kritik Rolü

Dijital tehdit ortamı, siber suçluların parola saldırılarını hızlandırmak için yapay zeka (AI) gibi gelişmiş teknikleri giderek daha fazla kullanmasıyla hızla evrim geçirmektedir.[1] AI destekli parola kırma araçları, zayıf parolaları dakikalar içinde aşabilir ve milyonlarca tahmin denemesini rekor hızda gerçekleştirebilir.[1] Bu durum, AI'nın kaba kuvvet saldırılarını "ışık yılları" kadar hızlandırma potansiyeli taşıdığını göstermektedir.[1] Siber suçlular, AI'yı mevcut saldırı yöntemlerini, özellikle kaba kuvvet, sözlük saldırıları, kimlik avı ve sosyal mühendislik gibi teknikleri önemli ölçüde geliştirmek için kullanmaktadır.[1] AI, bu saldırıları daha hızlı, daha kişiselleştirilmiş ve daha ölçeklenebilir hale getirmektedir.[3] Bu, AI'nın tamamen yeni saldırı vektörleri yaratmaktan ziyade, mevcut olanları katlanarak daha etkili hale getirdiği anlamına gelmektedir. Bu nedenle, bir parola analiz aracı, sadece ham hesaplama gücünü değil, aynı zamanda AI'nın yaygın kalıplara ve sızdırılmış verilere dayanarak akıllı tahminler üretme yeteneğini de dikkate almalıdır.

Parolalar, çevrimiçi kimlik doğrulamanın birincil aracı olmaya devam etse de [4], zayıf parola seçimleri veri ihlallerinin yaklaşık %80'ine katkıda bulunarak önemli riskler oluşturmaya devam etmektedir.[2] 2025'te yaşanan, 16 milyar giriş bilgisini açığa çıkaran büyük bir siber sızıntı, geleneksel parola sistemlerinin devam eden güvenlik açığını ve

kimlik bilgisi doldurma (credential stuffing) ve kimlik avı (phishing) saldırılarının yaygınlığını vurgulamaktadır.[7] Bu emsalsiz sızıntı, sadece geri dönüştürülmüş ihlaller değil, aynı zamanda yeni, silahlandırılabilir istihbarat içermektedir.[7] Verizon'ın 2025 Veri İhlali Araştırmaları Raporu (DBIR), saldırıların %38'inin kimlik bilgisi kötüye kullanımı veya kimlik avı içerdiğini ortaya koyarak, parolaların hala en büyük tek hata noktası olduğunun altını çizmektedir.[5] Bu durum, bireysel parola zayıflıklarının hızla büyük ölçekli, sistemik güvenlik açıklarına dönüştüğünü göstermektedir. Bu nedenle, bir parola analiz aracı sadece bağımsız bir özellik değildir; bir kuruluşun genel siber güvenlik duruşunun kritik bir bileşenidir. Önerileri, güçlü bir parolanın bile diğer katmanlar zayıfsa yetersiz kalacağını göz önünde bulundurarak, çok faktörlü kimlik doğrulama (MFA) ve karanlık web izleme gibi daha geniş uygulamaları savunmak üzere parolanın ötesine geçmelidir.

2025 Yılına Yönelik Parola Güvenliği Zorlukları ve Fırsatları

Parola güvenliği alanındaki en büyük zorluklardan biri, güçlü güvenlik gereksinimleri ile kullanıcı kullanılabilirliği arasında hassas bir denge kurmaktır. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) gibi kuruluşların da belirttiği gibi, aşırı karmaşık veya sık sık değiştirilen parola gereksinimleri genellikle kullanıcıların tahmin edilebilir kalıplar oluşturmasına (örneğin, "p@ssw0rd" gibi) veya parolalarını fiziksel olarak bir yere yazmasına yol açar ki bu da güvenlik açıklarını artırır.[6] Bu durum, daha fazla karmaşıklığın her zaman daha fazla güvenlik anlamına geldiği sezgisel düşünceyle çelişmektedir. Bu nedenle, parola analiz araçları algoritmalarını bu yeni anlayışa göre uyarlamalıdır. Sadece karakter çeşitliliğini kontrol etmek artık yeterli değildir; araç, rastgele karmaşıklığın dayattığı tahmin edilebilir desenleri aktif olarak analiz etmeli ve engellemelidir. Bu, aracın "güç puanının" yeni NIST vurgusuna göre yeniden kalibre edilmesi gerektiği anlamına gelir.

Yapay zeka, kimlik avı ve sosyal mühendislik saldırılarını daha kişiselleştirilmiş, etkili ve ölçeklenebilir hale getirerek, kullanıcıların gerçek istekleri kötü niyetli olanlardan ayırt etmesini zorlaştırmaktadır.[3] AI destekli araçlar, hedeflenen bireyler hakkında yeterli kişisel veriyi toplayarak güven kazanır ve ardından daha hassas bilgileri elde etmek için bu güveni kötüye kullanır.[3] Deepfake teknolojisi gibi AI'daki çığır açan gelişmeler, sesleri, görünümleri ve vücut dilini doğru bir şekilde kopyalayarak son derece gerçekçi video ve ses parçacıkları oluşturulmasına olanak tanır, bu da kimlik avı kampanyalarını daha inandırıcı hale getirir.[3]

Kuantum bilişimin ortaya çıkışı, parola hashing dahil mevcut şifreleme yöntemlerine yönelik gelecekteki bir tehdit oluşturmakta ve kuantum sonrası kriptografiye (PQC) geçişi zorunlu kılmaktadır.[12] Kuantum bilgisayarlar, Shor algoritması gibi yöntemleri kullanarak geleneksel şifreleme algoritmalarını saniyeler içinde kırabilir, bu da RSA, ECC ve Diffie-Hellman gibi teknikleri tehlikeye atar.[12] "Şimdi Topla, Sonra Şifre Çöz" (Harvest Now, Decrypt Later - HNDL) saldırıları, siber suçluların bugün şifreli verileri çalıp gelecekte güçlü kuantum bilgisayarlar yaygınlaştığında şifrelerini çözmeyi planlamasıyla ortaya çıkmaktadır.[12] Bu, uzun vadeli veri güvenliği için PQC'ye geçişin aciliyetini vurgulamaktadır.

Ancak bu zorluklarla birlikte önemli fırsatlar da ortaya çıkmaktadır. Bunlar arasında, rastgele karmaşıklık yerine uzunluğu ve kapsamlı kara liste taramasını önceliklendiren yeni yönergelerin (NIST'in 2025 güncellemeleri gibi) benimsenmesi yer almaktadır.[6] Ayrıca, geçiş anahtarları (passkeys) ve davranışsal biyometrikler gibi gelişmiş kimlik doğrulama yöntemlerinin benimsenmesi, parola bağımlılığını azaltarak hem güvenliği hem de kullanıcı deneyimini iyileştirmektedir.[19] FIDO Alliance 2025 raporu, tüketicilerin %75'inin geçiş anahtarlarının farkında olduğunu ve en iyi 100 web sitesinin %48'inin geçiş anahtarı sunduğunu belirtmektedir, bu da parolasız bir geleceğe doğru önemli bir değişimi göstermektedir.[21] Bu gelişmeler, siber güvenlik uzmanlarının ve geliştiricilerin, parola güvenliğini yeniden düşünmeleri ve daha dayanıklı, kullanıcı dostu çözümler geliştirmeleri için bir yol haritası sunmaktadır.

2025 İçin En Etkili 10 Parola Güvenliği Tekniği ve Trendi

Aşağıdaki tablo, 2025 yılı ve sonrası için parola güvenliği alanındaki en önemli teknikleri ve trendleri özetlemektedir. Bu özet, her bir tekniğin temel özelliklerini, önemini ve bir parola analiz ve öneri aracındaki potansiyel uygulama alanlarını hızlıca kavramak için tasarlanmıştır.

Tablo 1: 2025 Parola Güvenliği Teknikleri ve Trendleri Özeti

Teknik/Trend Başlığı	Kısa Açıklama	2025 Etkileri ve Uygulama Alanları	Ana Kaynak/Referans
1. Uzunluk Odaklı Parola Politikaları	Parola güvenliğinde karmaşıklıktan ziyade	Daha güçlü güvenlik, daha az parola	NIST Special Publication 800-63B,

	uzunluğa odaklanarak, kullanıcıların hatırlaması kolay, ancak kaba kuvvet saldırılarına dirençli uzun parola ifadeleri oluşturmasını teşvik eder.	sıfırlama, kullanıcı dostu deneyim. Araç, entropi ve kaba kuvvet tahmininde uzunluğu önceliklendirmelidir.	Hive Systems [1]
2. Kapsamlı Kara Liste Taraması ve İhlal Edilmiş Kimlik Bilgisi Tespiti	Kullanıcıların bilinen zayıf, yaygın veya daha önce ihlal edilmiş parolaları seçmesini engellemek için yeni parolaları sürekli olarak genişletilmiş kara listelere karşı kontrol etme.	Kimlik bilgisi doldurma saldırılarına karşı önemli direnç. Araç, gerçek zamanlı ihlal edilmiş parola veritabanı kontrollerini entegre etmelidir.	NIST Special Publication 800-63B, Palo Alto Networks [8]
3. Çok Faktörlü Kimlik Doğrulama (MFA) ve Adaptif Kimlik Doğrulama	Erişimi sağlamak için birden fazla doğrulama faktörü gerektirir ve risk faktörlerine (konum, cihaz, davranış) göre güvenlik önlemlerini dinamik olarak ayarlar.	%45 MFA uygulamasının biyometriyi içermesi bekleniyor. Araç, MFA'yı temel bir uzantı olarak vurgulamalı ve bağlamsal risk değerlendirmesini genişletmelidir.	ISACA, Market.us Scoop [24]
4. Parolasız Kimlik Doğrulama ve Geçiş Anahtarları (Passkeys)	Geleneksel parolalara olan bağımlılığı ortadan kaldırarak kullanıcıların biyometrik veriler veya donanım anahtarları gibi alternatif yöntemlerle kimliklerini doğrulamalarını sağlar.	Parola tabanlı sistemlerden geçiş anahtarlarına doğru hızlanan endüstri değişimi. Araç, parolasız kimlik doğrulamanın nihai güvenlik hedefi olduğunu vurgulamalıdır.	FIDO Alliance 2025 Report, Descope [21]
5. Davranışsal Biyometrik Analiz	Kimliği sürekli olarak doğrulamak için klavye dinamikleri ve	Yetkisiz erişimi gerçek zamanlı olarak tespit etmek için parola	Specops Software, Market.us Scoop [20]

	fare hareketleri gibi benzersiz insan aktivite desenlerini analiz eder.	gücü analizine ek bir katman olarak uygulanabilir. Araç, bu teknolojinin potansiyelini vurgulamalıdır.	
6. Yapay Zeka Destekli Parola Gücü Tahmini ve Önerileri	Yapay zeka ve makine öğrenimi modelleri, insan davranışındaki kalıpları ve saldırgan taktiklerini hesaba katarak parolaların gücünü tahmin eder.	Araç, Zxcvbn gibi AI destekli algoritmaları entegre etmelidir. AI, kullanıcının bağlamına göre daha akıllı öneriler oluşturabilir.	ResearchGate, Bitwarden [26]
7. Kuantum Dirençli Kriptografi (PQC) ve Hashing Algoritmaları	Kuantum bilgisayar saldırılarına dayanıklı şifreleme algoritmaları geliştirme, özellikle parola hashing için.	Geçiş stratejileri ve altyapı yükseltmeleri hızlanacak. Araç, PQC uyumlu hashing algoritmalarının önemini vurgulamalıdır.	GeeksforGeeks, Specopssoft [12]
8. Kullanıcı Dostu Parola Oluşturma ve Yönetimi (NIST Uyumlu)	NIST'in 2025 yönergeleri, kullanıcı deneyimini iyileştirirken güvenliği artıran parola oluşturma ve yönetimi uygulamalarını teşvik etmektedir.	Daha az parola sıfırlama, daha iyi kullanıcı uyumu, azaltılmış riskli davranışlar. Araç, bu NIST yönergeleriyle uyumlu öneriler sunmalıdır.	NIST SP 800-63B, Cybersierra [6]
9. Gelişmiş Sosyal Mühendislik ve Kimlik Avı Tespiti	Yapay zeka, sosyal mühendislik ve kimlik avı saldırılarını daha sofistike ve hedefli hale getirerek, kullanıcıların bu tehditleri tanımasını zorlaştırmaktadır.	Kuruluşlar için siber güvenlik eğitimi ve saldırı simülasyonlarının artan önemi. Araç, kullanıcılara bu tür saldırıların tehlikeleri hakkında bilgi vermeli ve rehberlik etmelidir.	CrowdStrike, NCSC [3]
10. Sürekli İzleme ve Risk Değerlendirmesi	Parola güvenliği duruşunu proaktif olarak sürdürmek ve gelişen tehditlere	Kuruluşlar için gelişmiş siber güvenlik duruşu ve azaltılmış olay yanıt	StrongDM, TrustCloud [6]

	uyum sağlamak için parola politikalarının ve kullanıcı davranışlarının sürekli izlenmesi ve değerlendirilmesi.	süreleri. Araç, kullanıcılara parolalarını düzenli olarak ihlal edilmiş listelerde kontrol etmelerini önermelidir.	

1. Uzunluk Odaklı Parola Politikaları

2025 NIST yönergeleri, parola güvenliğinde geleneksel karmaşıklıktan ziyade uzunluğa öncelik veren önemli bir değişim sergilemektedir.[6] Bu yaklaşım, kullanıcıların hatırlaması daha kolay olan, ancak kaba kuvvet saldırılarına karşı çok daha dirençli olan uzun parolalar veya parola ifadeleri (passphrases) oluşturmasını teşvik eder.

Bu politika, geleneksel olarak büyük/küçük harf, sayı ve özel karakter zorunluluğu getiren karmaşıklık kuralları yerine, minimum 12-16 karakter uzunluğunu (ayrıcalıklı hesaplar için 15+ karakter) önermektedir.[6] Ayrıca, maksimum 64 karaktere kadar parolalara izin verilmesi tavsiye edilmektedir.[6] Bu değişim, parola gücünün nasıl tanımlandığı ve ölçüldüğünde temel bir değişikliği yansıtır. Daha önce "güçlü" genellikle karakter çeşitliliği anlamına gelirken, şimdi odak noktası, bir parolanın kaba kuvvet saldırılarına karşı koyma yeteneğini temelden artıran uzunluktur.

Uzun parolalar, kaba kuvvet saldırılarına karşı katlanarak daha fazla direnç gösterir. Örneğin, Hive Systems'ın araştırması, tam karakter tipli 18 karakterli bir parolanın günümüz teknolojisiyle kırılmasının tahmini olarak 463 kentilyon yıl süreceğini ortaya koymaktadır.[1] Buna karşılık, 8 karakterli bir parolanın kırılması dakikalar ila saatler sürebilir.[1] Bu, kullanıcıların tahmin edilebilir desenler oluşturmasını veya parolalarını fiziksel olarak bir yere yazmasını engeller.[6] Kullanılabilirlik, bu güvenlik stratejisinin önemli bir etkinleştiricisidir. Akılda kalıcı parola ifadeleri, kullanıcıların parolalarını yazma veya yeniden kullanma olasılığını azaltır; bu davranışlar önemli güvenlik riskleri taşır.[6]

2025'teki potansiyel etkileri arasında kuruluşlar için daha güçlü bir güvenlik duruşu ve parola sıfırlama taleplerinde azalma yer almaktadır.[17] Kullanıcı dostu bir deneyim ve parola yeniden kullanımının azalması da bu yaklaşımın doğal sonuçlarıdır.[6] Parola değerlendirme araçları için bu, entropi hesaplamalarını [4] ve kaba kuvvet tahminlerini [26] uzunluk faktörüne göre önceliklendirmesi gerektiği anlamına gelir. Araç, sadece

karakter çeşitliliğini kontrol etmek yerine, kullanıcıların zorlandığında başvurduğu tahmin edilebilir karmaşıklık desenlerini aktif olarak engellemeli ve önerilerini rastgele karmaşıklıktan ziyade uzunluğa ve akılda kalıcılığa (parola ifadeleri) odaklamalıdır.[9] Bu, aracın "güç puanının" yeni NIST vurgusuna göre yeniden kalibre edilmesi gerektiği anlamına gelir.

2. Kapsamlı Kara Liste Taraması ve İhlal Edilmiş Kimlik Bilgisi Tespiti

Bu teknik, kullanıcıların bilinen zayıf, yaygın veya daha önce ihlal edilmiş parolaları seçmesini engellemek için yeni parolaları sürekli olarak genişletilmiş kara listelere karşı kontrol etmeyi içerir.[6] Kuruluşlar, "123456" veya "password" gibi yaygın parolaları [5] ve ayrıca veri ihlallerinde açığa çıkan milyarlarca kimlik bilgisini içeren [5] kapsamlı veritabanlarına karşı parolaları tarayan yazılımlar kullanmalıdır.[6] Bu, Bitwarden'ın zxcvbn [32] veya Specops'un 4 milyardan fazla ihlal edilmiş parolayı içeren veritabanı [5] gibi araçlarla yapılabilir.

İhlal edilmiş kimlik bilgileri ve yaygın parolalar, kimlik bilgisi doldurma (credential stuffing) ve sözlük saldırıları (dictionary attacks) için birincil vektörlerdir.[23] 2025'teki 16 milyar parolalık sızıntı, bu tehdidin ciddiyetini vurgulamaktadır.[7] Bu teknik, saldırganların kolayca tahmin edebileceği veya elde edebileceği parolaların kullanılmasını proaktif olarak önler. Geleneksel sözlük saldırıları, yaygın kelimelerin derlenmiş listelerini kullanırken [23], güncel yaklaşım ihlal edilmiş kimlik bilgisi veritabanlarına ve bilinen sızdırılmış parolalara karşı taramayı vurgulamaktadır.[5] Bu, sadece sözlük kelimelerinden gerçek dünyada aktif olarak istismar edilen kimlik bilgilerine doğru önemli bir evrimdir.

2025'teki potansiyel etkileri arasında şirket ağlarında ve bulut tabanlı uygulamalarda kimlik bilgisi doldurma saldırılarına karşı önemli ölçüde direnç [23] yer almaktadır. Parola analiz aracı, kullanıcının girdiği parolayı gerçek zamanlı olarak ihlal edilmiş parola veritabanlarına karşı kontrol etmeli ve bir eşleşme bulunursa derhal daha güçlü bir öneri sunmalıdır. Bu yaklaşım, kullanıcıların kişisel bilgilerle (evcil hayvan adları, doğum tarihleri) veya klavye desenleriyle (qwerty) ilişkili tahmin edilebilir parolalar oluşturmasını engeller.[5] Zayıf parolaları ayarlandıktan sonra tespit etmek yerine, kara listeler onların baştan oluşturulmasını engeller.[8] Bu, güvenlik paradigmasını reaktiften proaktife kaydırır. Araç, parola oluşturma veya değiştirme sırasında gerçek zamanlı engelleme uygulamalı, kullanıcının seçtiği parolanın bilinen bir kara listede olması durumunda derhal bilgilendirmeli ve farklı bir parola talep etmelidir. Bu, sisteme

yalnızca gerçekten benzersiz ve ihlal edilmemiş parolaların girmesini sağlar.

3. Çok Faktörlü Kimlik Doğrulama (MFA) ve Adaptif Kimlik Doğrulama

MFA, kullanıcıların erişim sağlamak için birden fazla doğrulama faktörü (bildiği bir şey, sahip olduğu bir şey, olduğu bir şey) sağlamasını gerektirerek parola güvenliğine ek bir katman ekler.[24] Adaptif kimlik doğrulama ise, risk faktörlerine (konum, cihaz, davranış) göre güvenlik önlemlerini dinamik olarak ayarlar.[18]

MFA, bir parola (bildiği bir şey) ile birlikte mobil cihazdan tek kullanımlık kodlar, biyometrik veriler (parmak izi, yüz tanıma) veya donanım anahtarları gibi ikinci bir faktör gerektirir.[9] Adaptif kimlik doğrulama, olağandışı oturum açma etkinliğini (farklı konumdan giriş gibi) algılamak için bağlamsal verileri kullanır ve yüksek riskli senaryolarda ek doğrulama katmanları ekler.[18]

MFA, parola çalınsa bile yetkisiz erişimi %99,9'a kadar engeller.[10] Kimlik avı saldırılarına karşı özellikle etkilidir, çünkü bir saldırgan parolayı ele geçirse bile ikinci doğrulama faktörüne ihtiyaç duyar.[23] Adaptif kimlik doğrulama, kullanıcı deneyimini etkilemeden güvenlik önlemlerini gerçek zamanlı tehditlere göre uyarlayarak sürtünmeyi azaltır.[18] MFA, bir parolayı doğrudan daha güçlü yapmasa da, parola zayıflıklarını ve dış tehditleri telafi ederek kimlik bilgisi hırsızlığına karşı birincil savunma görevi görür.

2025 yılına kadar MFA uygulamalarının %45'inin biyometrik faktörleri içermesi beklenmektedir.[25] Ayrıca, AI ve davranışsal analitik, MFA sistemlerinin etkinliğini artırarak anormal davranışları tespit edebilecek ve ek güvenlik isteyebilecektir.[24] Bu, daha akıllı, dinamik ve daha az kolayca taklit edilebilir ikinci faktörlere doğru bir geçişi işaret etmektedir. Parola analiz aracı, kullanıcılara MFA'yı her yerde etkinleştirmelerini önermeli ve MFA'nın parola güvenliğinin temel bir uzantısı olduğunu vurgulamalıdır. Risk değerlendirmesi, kullanıcının cihazı, konumu ve geçmiş davranışları gibi bağlamsal faktörleri içerecek şekilde genişletilmelidir. Aracın MFA için önerileri, basit SMS tabanlı 2FA'nın ötesine geçerek bu gelişmiş yöntemleri vurgulamalıdır. Kurumsal kullanıcılar için araç, AI'yı gerçek zamanlı risk puanlaması için kullanan mevcut adaptif kimlik doğrulama çerçeveleriyle entegrasyon önerebilir ve kimlik doğrulamayı bağlamdan haberdar hale getirebilir.

4. Parolasız Kimlik Doğrulama ve Geçiş Anahtarları (Passkeys)

Parolasız kimlik doğrulama, geleneksel parolalara olan bağımlılığı ortadan kaldırarak kullanıcıların biyometrik veriler, donanım anahtarları veya sihirli bağlantılar gibi alternatif yöntemlerle kimliklerini doğrulamalarını sağlar.[29] Geçiş anahtarları (passkeys), FIDO standartlarına dayalı, cihazlara bağlı ve kimlik avına dirençli kriptografik anahtarlardır.[1]

Geçiş anahtarları, cihazlara bağlı kriptografik anahtarlar kullanarak çalışır; bu da kullanıcıların Face ID veya parmak izi gibi yerel cihaz biyometrisiyle oturum açmasına olanak tanır.[1] Bunlar, FIDO Alliance tarafından desteklenen FIDO2/WebAuthn standartlarına uygundur.[23] Geçiş anahtarları, yazılı bir parola ihtiyacını ortadan kaldırırken, doğal olarak "sahip olduğunuz bir şey" (cihaz) ve "olduğunuz bir şey" (biyometrik kilit açma) faktörlerini içerir.[21] Bu, onları tek eylemli bir MFA haline getirir, süreci kolaylaştırırken güçlü güvenliği korur.

Parolasız kimlik doğrulama, kimlik avı riskini ortadan kaldırır [31] ve parola yeniden kullanımını önler.[5] Kullanıcı deneyimini önemli ölçüde iyileştirir, oturum açma süreçlerini hızlandırır ve unutulan parolalardan kaynaklanan terk edilmiş satın alma işlemlerini azaltır.[21] 2025 FIDO raporuna göre, tüketicilerin %75'i geçiş anahtarlarının farkındadır ve en iyi 100 web sitesinin %48'i geçiş anahtarı sunmaktadır.[21] Bu durum, parolalarla ilişkili önemli iş maliyetlerini vurgulamaktadır: unutulan kimlik bilgileri nedeniyle terk edilen satın almalar (tüketicilerin %47'si), sıfırlama için artan destek maliyetleri ve çalınan kimlik bilgilerinden kaynaklanan riskler.[21] Geçiş anahtarları, bu sorunları doğrudan ele alarak daha hızlı oturum açma (parolalardan 3 kat, parola + geleneksel MFA'dan 8 kat daha hızlı) ve daha az müşteri kaybı sunar.[21]

2025'teki potansiyel etkileri arasında parola tabanlı sistemlerden geçiş anahtarlarına ve diğer parolasız yöntemlere doğru hızlanan bir endüstri değişimi yer almaktadır.[5] Yüksek değerli hesapların korunması ve kimlik bilgisi doldurma saldırılarının azaltılması, geçiş anahtarlarının sağladığı önemli faydalardandır.[21] Parola analiz aracı, parolasız kimlik doğrulamanın nihai güvenlik hedefi olduğunu vurgulamalı ve kullanıcılara mümkün olduğunda geçiş anahtarlarını benimsemelerini önermelidir. Mevcut parola gücü analizini, geçiş anahtarları gibi parolasız yöntemlere geçişin faydalarıyla ilişkilendirmelidir. Aracın geçiş anahtarları için önerileri, sadece güvenliği değil, aynı zamanda kullanıcı kolaylığı ve iş verimliliği için somut faydaları da vurgulamalı ve böylece benimsenmeyi daha çekici hale getirmelidir.

5. Davranışsal Biyometrik Analiz

Davranışsal biyometrikler, kimliği sürekli olarak doğrulamak için klavye dinamikleri, fare hareketleri ve dokunmatik ekran etkileşimleri gibi benzersiz insan aktivite desenlerini analiz eden yenilikçi bir kimlik doğrulama yöntemidir.[20] Fiziksel biyometriklerin aksine, davranışsal biyometrikler statik özelliklere dayanmaz. Bunun yerine, bir kullanıcının cihazlarla nasıl etkileşim kurduğunu gerçek zamanlı olarak sürekli izler ve analiz eder.[20]

Yapay zeka ve makine öğrenimi, sistemlerin zaman içindeki davranış değişikliklerine uyum sağlamasına olanak tanıyarak tespit oranlarını önemli ölçüde artırır.[20] Bu, mevcut güvenlik katmanlarına dinamik, bağlamdan haberdar bir katman ekler, kimlik bilgisi tabanlı saldırılara karşı genel savunmayı iyileştirir.[20] Dolandırıcılık tespiti ve risk puanlamasına yardımcı olur, potansiyel tehditlere proaktif yanıtlar verilmesini sağlar.[20] Statik kimlik bilgilerine (parolalar gibi) bağımlılığı en aza indirir.[20] Geleneksel kimlik doğrulamanın (parola, MFA) oturum açma sırasında tek seferlik bir olay olmasının aksine, davranışsal biyometrikler bir oturum boyunca sürekli doğrulama sunar.[20] Bu, ilk kimlik doğrulamasından sonra oturum ele geçirme veya içeriden gelen tehditleri tespit etmek için çok önemlidir.

2025 yılına kadar MFA uygulamalarının %40'ının yapay zeka destekli davranışsal analitik içermesi beklenmektedir.[25] Bu, yetkisiz erişimi veya hesap ele geçirmeyi gerçek zamanlı olarak tespit etmek için parola gücü analizine ek bir katman olarak uygulanabilir. Parola analiz aracı, bu teknolojinin ek bir güvenlik katmanı olarak potansiyelini vurgulayabilir, ancak bunun mevcut parolaların yerini tamamen almaktan ziyade onları tamamladığını belirtmelidir.[20] Kullanıcı davranışındaki değişkenlik ve yanlış pozitif olasılığı gibi sınırlamalar dikkate alınmalıdır.[20] Yapay zeka ve makine öğreniminin davranışsal biyometriklerle entegrasyonu, sistemlerin zaman içindeki kullanıcı davranış değişikliklerine sürekli öğrenmesini ve uyum sağlamasını sağlar.[20] Bu, statik kimlik doğrulamadan dinamik, akıllı bir sisteme geçişi temsil eder. Araç için bu, parola girişi sırasında yazma kalıplarını veya fare hareketlerini analiz ederek ek, ince bir gerçek zamanlı risk değerlendirmesi katmanı sağlayabilecek gelecekteki entegrasyon olanakları anlamına gelir. Bu, kullanıcı etkileşim kalıplarını dikkate alan daha "akıllı" bir parola gücü analizine yol açabilir.

6. Yapay Zeka Destekli Parola Gücü Tahmini ve Önerileri

Yapay zeka ve makine öğrenimi modelleri, parolaların gücünü tahmin etmek için geleneksel yöntemlerden (uzunluk ve karmaşıklık) daha gelişmiş analizler sunar, insan davranışındaki kalıpları ve saldırganların taktiklerini hesaba katar.[27] Zxcvbn gibi algoritmalar, yaygın kelimelerin, harf-sayı ikamelerinin ve klavye dizilerinin kullanımını dikkate alarak parola entropi hesaplamasından elde edilen düzenleme kalıplarına dayanarak parola gücünü ölçer.[26]

Adversarial machine learning (çekişmeli makine öğrenimi), modelleri kasıtlı olarak hazırlanmış aldatıcı parolalar üzerinde eğiterek güvenlik açıklarını ortaya çıkarır ve ele alır, sınıflandırma doğruluğunu %20'ye kadar artırır.[27] Gelecekte, üretken yapay zeka ağları (GAN'lar) daha kontrollü çekişmeli veri kümeleri oluşturmak için kullanılabilir.[27] Yapay zeka, parola kırma hızını "ışık yılları" kadar hızlandırabilir.[1] Geleneksel güç denetleyicilerinin sınırlamalarını (statik yaklaşımlar) ele alır ve daha doğru, bağlamdan haberdar bir değerlendirme sağlar.[4] AI destekli araçlar, kullanıcının seçtiği parolaların gerçek dünyadaki saldırı yöntemlerine karşı ne kadar dirençli olduğunu daha gerçekçi bir şekilde tahmin edebilir.

Parola güvenliğinde bir silahlanma yarışı söz konusudur; yapay zeka hem saldırganlar hem de savunmacılar için güçlü bir araçtır.[1] Bu nedenle, aracın yapay zeka destekli güç analizi, yapay zeka destekli saldırı kalıplarının önünde kalmak için sürekli olarak güncellenmeli ve düşmanca örneklerle eğitilmelidir.[27] Sadece yapay zeka kullanmak yeterli değildir; yapay zeka, diğer yapay zekalar tarafından üretilen gelişen saldırı kalıplarına karşı dirençli olmalıdır.

2025'teki potansiyel etkileri arasında parola analiz aracının Zxcvbn gibi AI destekli algoritmaları entegre etmesi yer almaktadır. Yapay zeka, kullanıcının bağlamına (örneğin, kişisel bilgilerle ilişkili kelimelerden kaçınma) ve bilinen saldırı vektörlerine göre daha akıllı ve kişiselleştirilmiş parola önerileri oluşturabilir.[44] Saldırganlar, AI'yı sözlük ve kaba kuvvet saldırılarını otomatikleştirmek ve optimize etmek için kullanacağından, AI destekli savunma kritik hale gelecektir.[1] Araç, sadece matematiksel entropi hesaplamalarının ötesine geçerek insan parola oluşturma eğilimlerini ve yaygın saldırı kalıplarını anlayan yapay zeka modellerini içermelidir. Bu, sadece rastgele değil, aynı zamanda yapay zeka saldırganlarının bağlama göre tahmin etmesini zorlaştıran daha "akıllı" önerilere olanak tanır.

7. Kuantum Dirençli Kriptografi (PQC) ve Hashing Algoritmaları

Kuantum dirençli kriptografi (PQC), kuantum bilgisayar saldırılarına dayanıklı şifreleme algoritmaları geliştirme alanıdır, özellikle parola hashing gibi kritik güvenlik işlevleri için.[12] Mevcut şifreleme yöntemleri (RSA, ECC, AES) ve hashing algoritmaları (bcrypt, scrypt, PBKDF2) kuantum bilgisayarların (özellikle Shor algoritması) tehdidi altındadır.[12] PQC algoritmaları (Kyber, Dilithium, SPHINCS+), bu tür saldırılara dayanacak şekilde tasarlanmıştır.[15] NIST, Ağustos 2024'te bu PQC standartlarını onaylamıştır.[15]

Bu teknolojinin önemi, "Şimdi Topla, Sonra Şifre Çöz" (Harvest Now, Decrypt Later - HNDL) saldırılarına karşı koruma sağlamasından kaynaklanmaktadır.[12] Bu saldırılarda, siber suçlular bugün şifreli verileri çalar ve gelecekte güçlü kuantum bilgisayarlar ortaya çıktığında şifrelerini çözmeyi planlar.[12] Kuantum bilgisayarlar, mevcut parola hashing sistemlerini eski haline getirebilir ve gelişmiş parolaları bile anında kırabilir.[12] Bu nedenle, PQC, uzun vadeli veri güvenliği için kritik öneme sahiptir.[12] Bu durum, bugün çalınan verilerin yıllar sonra şifresinin çözülebileceği HNDL tehdidini vurgular, bu da PQC'nin hemen şimdi benimsenmesinin aciliyetini ortaya koyar.

2025'teki potansiyel etkileri arasında kuruluşların PQC'ye geçiş stratejilerini (hibrit yaklaşımlar gibi) hızlandırması ve altyapı yükseltmelerini gerçekleştirmesi yer almaktadır.[15] Bir parola analiz aracı, PQC uyumlu hashing algoritmalarının önemini vurgulamalıdır. Ayrıca, kuruluşların "kripto-çevik" olmaları gerektiği, yani yeni kuantum tehditlerine yanıt olarak kriptografik bileşenleri hızla değiştirebilmeleri gerektiği de önemlidir.[16] Araç, parola depolama için PQC uyumlu hashing algoritmalarını tavsiye etmelidir.

8. Kullanıcı Dostu Parola Oluşturma ve Yönetimi (NIST Uyumlu)

NIST'in 2025 yönergeleri, kullanıcı deneyimini iyileştirirken güvenliği artıran parola oluşturma ve yönetimi uygulamalarını teşvik etmektedir.[6] Bu yönergeler, kullanıcı davranışına bir yanıt niteliğindedir ve aşırı katı kuralların kullanıcıların güvenlik açıklarını artırabilecek kestirme yollara başvurmasına neden olduğunu kabul etmektedir. Amaç, güvenliği kullanıcılar için daha kolay hale getirmektir.

Bu yönergeler, zorunlu parola değişikliklerini ortadan kaldırmaktadır.[6] Ayrıca, parola ipuçlarını ve bilgi tabanlı kimlik doğrulamayı (güvenlik soruları gibi) yasaklar, çünkü bunlar genellikle zayıf güvenlik sağlar ve kolayca tahmin edilebilir veya sosyal

mühendislikle elde edilebilir.[6] Parola yöneticilerinin kullanımını şiddetle teşvik eder.[5] Parola yöneticileri, kullanıcıların ezberleme yükü olmadan en iyi uygulamaları (benzersiz, uzun, karmaşık parolalar) takip etmelerini sağlayan temel araçlardır. Ayrıca, kopyala-yapıştır işlevine izin verilmesi de önerilir, bu da parola yöneticilerinin kullanımını kolaylaştırır.[10]

2025'teki potansiyel etkileri arasında daha az parola sıfırlama talebi, daha iyi kullanıcı uyumu ve kullanıcıların parolalarını yazma veya yeniden kullanma gibi riskli davranışlarının azalması yer almaktadır.[6] Parola analiz aracı, bu NIST yönergeleriyle uyumlu öneriler sunmalıdır. Bu, sadece güvenlik gereksinimlerini karşılamakla kalmayıp, aynı zamanda kullanıcıların güvenli parola uygulamalarını benimsemesini kolaylaştıran bir yaklaşımdır.

9. Gelişmiş Sosyal Mühendislik ve Kimlik Avı Tespiti

Yapay zeka, sosyal mühendislik ve kimlik avı saldırılarını daha sofistike ve hedefli hale getirerek, kullanıcıların bu tehditleri tanımasını zorlaştırmaktadır.[3] AI destekli araçlar, veri toplama ve analizi, otomasyon, ölçeklenebilirlik, deepfake oluşturma, gelişmiş kimlik avı kampanyaları ve iş e-postası uzlaşması (BEC) saldırılarını geliştirir.[3] AI, bir yöneticinin yazma stilini taklit edebilir ve mesajları birçok dile çevirebilir, bu da saldırıları daha inandırıcı ve tespit edilmesi zor hale getirir.[3]

AI destekli sosyal mühendislik, parolaların çalınması için artan bir risk oluşturmaktadır.[3] AI, saldırıları daha kişiselleştirilmiş ve ölçeklenebilir hale getirerek, daha az yetenekli saldırganlar için bile saldırı yüzeyini genişletmektedir. Bu nedenle, kullanıcıların bu gelişmiş saldırıları tanımak için eğitilmesi kritik öneme sahiptir.[3] Güçlü parolalar ve MFA olsa bile, kullanıcılar sosyal mühendisliğe karşı savunmasız kalırlarsa en zayıf halka olmaya devam ederler.

2025'teki potansiyel etkileri arasında kuruluşlar için siber güvenlik eğitimi ve saldırı simülasyonlarının artan önemi yer almaktadır.[3] Parola analiz aracı, kullanıcılara bu tür saldırıların tehlikeleri hakkında bilgi vermeli ve şüpheli istekleri nasıl tanıyacakları konusunda rehberlik etmelidir. Bu, kullanıcı eğitimini güvenlik stratejisinin hayati bir bileşeni olarak dahil etmeyi gerektirir.

10. Sürekli İzleme ve Risk Değerlendirmesi

Sürekli izleme ve risk değerlendirmesi, parola güvenliği duruşunu proaktif olarak sürdürmek ve gelişen tehditlere uyum sağlamak için parola politikalarının ve kullanıcı davranışlarının sürekli izlenmesi ve değerlendirilmesini içerir.[18] Bu yaklaşım, parola güvenliğinin tek seferlik bir kurulum değil, sürekli gelişen tehditler ve yeni veri ihlalleri nedeniyle devam eden bir süreç olduğunu vurgular.

Kuruluşlar, bilinen ihlal veritabanlarına karşı parola taramasını zorunlu kılmalı ve uyumluluk için parola politikalarını otomatikleştirmelidir.[6] Sürekli izleme ve denetim, şüpheli oturum açma girişimleri için gerçek zamanlı uyarıları ve kullanıcı erişiminin düzenli incelemelerini içerir.[33] Otomatik izleme ve politika uygulama, parola güvenliğini ölçekli olarak yönetmek, manuel yükü ve insan hatasını azaltmak için gereklidir.

Saldırıların %38'i kimlik bilgisi kötüye kullanımı veya kimlik avı içerdiğinden [5], sürekli izleme, ihlalleri önlemek ve riskleri azaltmak için kritik öneme sahiptir. Proaktif bir yaklaşım, kuruluşların ortaya çıkan tehditlerin önünde kalmasını sağlar.[18]

2025'teki potansiyel etkileri arasında kuruluşlar için gelişmiş siber güvenlik duruşu ve azaltılmış olay yanıt süreleri yer almaktadır. Parola analiz aracı, kullanıcılara parolalarını düzenli olarak ihlal edilmiş listelerde kontrol etmelerini ve hesap etkinliklerini izlemelerini önermelidir. Bu, kullanıcıların kendi güvenliklerini sürekli olarak değerlendirmeleri ve iyileştirmeleri için araçlar ve bilgiler sağlamayı içerir.

Sonuç ve Öneriler

2025 yılına girerken, parola güvenliği manzarası, yapay zeka destekli saldırıların artan sofistikeliği ve kuantum bilişimin ortaya çıkışı gibi önemli zorluklarla karşı karşıyadır. Bununla birlikte, NIST yönergelerindeki evrim ve parolasız kimlik doğrulama gibi yeni teknolojilerin benimsenmesi, daha sağlam ve kullanıcı dostu güvenlik çözümleri için önemli fırsatlar sunmaktadır.

Kullanıcıdan alınan parolaların güvenliğini analiz eden ve daha güçlü öneriler sunan bir araç geliştiren ekip için aşağıdaki temel öneriler sunulmaktadır:

1. **Uzunluğu Önceliklendirin, Karmaşıklığı Değil:** Aracın parola gücü

değerlendirme algoritması, NIST'in 2025 yönergelerine uygun olarak uzunluğa odaklanmalıdır. Kullanıcıları rastgele karakter dizilerinden ziyade, hatırlaması kolay ama tahmin edilmesi zor olan uzun parola ifadeleri oluşturmaya teşvik edin. Aracın "güç puanı" bu yeni paradigma ile uyumlu olmalıdır.

2. **Gerçek Zamanlı Kara Liste Taraması Entegre Edin:** Araç, kullanıcının girdiği parolaları gerçek zamanlı olarak bilinen ihlal edilmiş kimlik bilgisi veritabanlarına ve yaygın parola kara listelerine karşı kontrol etmelidir. Bir eşleşme bulunursa, kullanıcıya derhal bilgi verilmeli ve farklı bir parola seçmesi istenmelidir. Bu proaktif yaklaşım, kimlik bilgisi doldurma saldırılarına karşı kritik bir savunma sağlar.
3. **MFA'yı Temel Bir Öneri Olarak Vurgulayın:** Parola gücünden bağımsız olarak, MFA'nın yetkisiz erişimi önemli ölçüde azalttığı ve kimlik avı saldırılarına karşı birincil savunma olduğu açıkça belirtilmelidir. Araç, kullanıcılara mümkün olan her yerde MFA'yı etkinleştirmelerini önermeli ve biyometrik veya donanım tabanlı MFA gibi daha gelişmiş biçimlerini vurgulamalıdır.
4. **Parolasız Kimlik Doğrulamaya Geçişi Teşvik Edin:** Geçiş anahtarları gibi parolasız yöntemler, kimlik avı riskini ortadan kaldırır ve kullanıcı deneyimini önemli ölçüde iyileştirir. Araç, parolasız kimlik doğrulamanın nihai güvenlik hedefi olduğunu vurgulamalı ve kullanıcılara bu teknolojileri benimsemeleri için rehberlik etmelidir.
5. **Davranışsal Biyometrik Analizin Potansiyelini Keşfedin:** Gelecekteki geliştirmeler için, aracın parola girişi sırasındaki kullanıcı davranış kalıplarını (örn. yazma dinamikleri) analiz etme yeteneğini araştırması önerilir. Bu, parola gücü analizine ek, ince bir gerçek zamanlı risk değerlendirmesi katmanı sağlayabilir.
6. **AI Destekli Akıllı Öneriler Sunun:** Araç, Zxcvbn gibi AI destekli algoritmaları entegre ederek, sadece matematiksel entropi değil, aynı zamanda insan parola oluşturma eğilimlerini ve AI destekli saldırı kalıplarını da anlayan daha "akıllı" parola önerileri sunmalıdır. Aracın AI modelleri, gelişen saldırı kalıplarına karşı dirençli olmak için sürekli olarak güncellenmelidir.
7. **PQC'nin Uzun Vadeli Önemini İletin:** Kuantum bilişimin parola hashing'e yönelik gelecekteki tehdidi göz önüne alındığında, araç, kullanıcıları parola depolama için PQC uyumlu hashing algoritmalarının önemine karşı duyarlı hale getirmelidir. Bu, uzun vadeli veri güvenliği için proaktif bir duruşu teşvik eder.
8. **Kullanıcı Dostu Yönetimi Teşvik Edin:** Araç, parola yöneticilerinin kullanımını teşvik etmeli, zorunlu parola değişikliklerini desteklememeli ve parola ipuçları gibi eski güvenlik önlemlerinden kaçınmalıdır. Amaç, kullanıcıların güvenli parola uygulamalarını benimsemesini kolaylaştırmaktır.
9. **Sosyal Mühendislik Farkındalığını Artırın:** Araç, kullanıcılara AI destekli kimlik avı ve sosyal mühendislik saldırılarının artan sofistikeliği hakkında bilgi vermeli ve

şüpheli istekleri tanımak için pratik ipuçları sunmalıdır. İnsan faktörü, genel güvenlik duruşunda kritik bir bileşen olmaya devam etmektedir.

10. **Sürekli İzleme ve Değerlendirme Yetenekleri Sağlayın:** Araç, kullanıcılara parolalarını düzenli olarak ihlal edilmiş listelerde kontrol etme ve hesap etkinliklerini izleme yeteneği sunmalıdır. Bu, bireysel parola güvenliğinin sürekli, proaktif bir çaba olduğunu vurgular.

Bu tekniklerin ve trendlerin entegrasyonu, yalnızca kullanıcının girdiği parolanın güvenliğini doğru bir şekilde analiz eden değil, aynı zamanda 2025 ve sonrası için gelişen siber güvenlik tehditlerine karşı dayanıklı, uygulanabilir ve kullanıcı dostu öneriler sunan bir araç geliştirmek için kritik öneme sahiptir.

Alıntılanan çalışmalar

1. How fast hackers can break your password with AI might terrify you ..., erişim tarihi Haziran 20, 2025, https://m.economictimes.com/magazines/panache/how-fast-hackers-can-break-your-password-with-ai-might-terrify-you-the-math-behind-the-digital-threat/articleshow/120799779.cms
2. Forbes: AI Can Crack Your Passwords Fast—6 Tips To Stay Secure | FIDO Alliance, erişim tarihi Haziran 20, 2025, https://fidoalliance.org/forbes-ai-can-crack-your-passwords-fast-6-tips-to-stay-secure/
3. AI-Powered Social Engineering Attacks | CrowdStrike, erişim tarihi Haziran 20, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/ai-social-engineering/
4. (PDF) Analyzing Password Strength: A Combinatorial Entropy ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/377306367_Analyzing_Password_Strength_A_Combinatorial_Entropy_Approach
5. The cost of compromise: Why password attacks are still winning in 2025 - The Register, erişim tarihi Haziran 20, 2025, https://www.theregister.com/2025/05/28/specops_password_attacks_2025/
6. NIST Password Guidelines: 2025 Updates & Best Practices, erişim tarihi Haziran 20, 2025, https://www.strongdm.com/blog/nist-password-guidelines
7. 16 billion passwords exposed in unprecedented cyber leak of 2025, experts raise global alarm - The Economic Times, erişim tarihi Haziran 20, 2025, https://m.economictimes.com/news/international/us/16-billion-passwords-exposed-in-unprecedented-cyber-leak-of-2025-experts-raise-global-alarm/articleshow/121961165.cms
8. What's New in NIST Password Guidelines in September 2024?, erişim tarihi Haziran 20, 2025, https://cybersierra.co/blog/whats-new-in-nist-password-guidelines-in-septembe

r-2024/
9. What are the NIST password guidelines in 2025? - TrustCommunity, erişim tarihi Haziran 20, 2025, https://community.trustcloud.ai/article/nist-password-guidelines-2025-15-rules-to-follow/
10. Password Policy Best Practices 2025 For Strong Security - MetaCompliance, erişim tarihi Haziran 20, 2025, https://www.metacompliance.com/blog/cyber-security-awareness/password-policy-best-practices
11. The near-term impact of AI on the cyber threat - NCSC.GOV.UK, erişim tarihi Haziran 20, 2025, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
12. Quantum Computing Cybersecurity 2025 (Complete Guide) - GeeksforGeeks, erişim tarihi Haziran 20, 2025, https://www.geeksforgeeks.org/quantum-computing-cybersecurity/
13. Post-quantum cryptography: Password security in the quantum era - Specops Software, erişim tarihi Haziran 20, 2025, https://specopssoft.com/blog/post-quantum-cryptography-passwords/
14. erişim tarihi Ocak 1, 1970, https://www.geeksforgreeks.org/quantum-computing-cybersecurity/
15. Post-Quantum Cryptography 2025: The Enterprise Readiness Gap, erişim tarihi Haziran 20, 2025, https://www.cio.inc/post-quantum-cryptography-2025-enterprise-readiness-gap-a-27367
16. Strong Authentication in a Post-Quantum World | EIC 2025, erişim tarihi Haziran 20, 2025, https://www.kuppingercole.com/events/eic2025/blog/strong-authentication-in-a-post-quantum-world
17. 2025 NIST Password Guidelines: Enhancing Security Practices, erişim tarihi Haziran 20, 2025, https://scytale.ai/resources/2024-nist-password-guidelines-enhancing-security-practices/
18. NIST password guidelines 2025: what you need to know to stay secure - TrustCommunity, erişim tarihi Haziran 20, 2025, https://community.trustcloud.ai/docs/grc-launchpad/grc-101/governance/nist-password-guidelines-2025-what-you-need-to-know-to-stay-secure/
19. Biometrics vs. Passwords: Securing Authentication in 2025, erişim tarihi Haziran 20, 2025, https://www.soma.com.au/blog/biometrics-vs-passwords
20. Behavioral biometric authentication: Could it replace passwords?, erişim tarihi Haziran 20, 2025, https://specopssoft.com/blog/behavioral-biometrics-authentication-passwords/
21. 2025 FIDO Report: The Passwordless Future - Descope, erişim tarihi Haziran 20, 2025, https://www.descope.com/blog/post/2025-fido-report
22. FIDO Alliance Champions Widespread Passkey Adoption and a ..., erişim tarihi Haziran 20, 2025, https://fidoalliance.org/fido-alliance-champions-widespread-passkey-adoption-a

nd-a-passwordless-future-on-world-passkey-day-2025/
23. What Is a Dictionary Attack? - Palo Alto Networks, erişim tarihi Haziran 20, 2025, https://www.paloaltonetworks.com/cyberpedia/dictionary-attack
24. Industry News 2025 Will MFA Redefine Cyberdefense in the 21st Century - ISACA, erişim tarihi Haziran 20, 2025, https://www.isaca.org/resources/news-and-trends/industry-news/2025/will-mfa-redefine-cyberdefense-in-the-21st-century
25. Multi-Factor Authentication Statistics and Facts (2025), erişim tarihi Haziran 20, 2025, https://scoop.market.us/multi-factor-authentication-statistics/
26. (PDF) PASSWORD STRENGTH STUDY USING THE ZXCVBN ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/389902836_PASSWORD_STRENGTH_STUDY_USING_THE_ZXCVBN_ALGORITHM_AND_BRUTE-FORCE_TIME_ESTIMATION_TO_STRENGTHEN_CYBERSECURITY
27. Adversarial Machine Learning for Robust Password Strength Estimation - arXiv, erişim tarihi Haziran 20, 2025, https://arxiv.org/html/2506.00373v1
28. The Complete Guide to NIST Password Guidelines (2025 Update ..., erişim tarihi Haziran 20, 2025, https://drata.com/blog/nist-password-guidelines
29. Password Security Best Practices 2025: Business Guide & NIST Tips - iFeeltech, erişim tarihi Haziran 20, 2025, https://ifeeltech.com/password-security/
30. Password Security: Best Practices For Businesses In 2025 - QualityIP, erişim tarihi Haziran 20, 2025, https://qualityip.com/password-security-best-practices-for-businesses-in-2025/
31. Password Security Best Practices for 2025 | Crowe LLP, erişim tarihi Haziran 20, 2025, https://www.crowe.com/cybersecurity-watch/password-security-best-practices-2025
32. Password Tester | Test Your Password Strength - Bitwarden, erişim tarihi Haziran 20, 2025, https://bitwarden.com/password-strength/
33. Password Security 2025: Your Guide to Account Security - MSP Corp, erişim tarihi Haziran 20, 2025, https://mspcorp.ca/blog/password-security-2025-your-guide-to-account-security/
34. Estimating Password Strength - NIST Computer Security Resource ..., erişim tarihi Haziran 20, 2025, https://csrc.nist.rip/archive/pki-twg/y2003/presentations/twg-03-05.pdf
35. Create a Strong Password: Rules for 2025 - Cybernews, erişim tarihi Haziran 20, 2025, https://cybernews.com/best-password-managers/how-to-create-a-strong-password/
36. Strong Password Best Practices For 2025 - Cyble, erişim tarihi Haziran 20, 2025, https://cyble.com/knowledge-hub/strong-password-best-practices-2025/
37. The State of Password Security 2025 Report | Bitwarden, erişim tarihi Haziran 20, 2025, https://bitwarden.com/resources/the-state-of-password-security/
38. Most Common Passwords 2025: Is Yours on the List? - Huntress, erişim tarihi

Haziran 20, 2025, https://www.huntress.com/blog/most-common-passwords
39. How to analyze password lists for security risks in Cybersecurity - LabEx, erişim tarihi Haziran 20, 2025, https://labex.io/tutorials/hydra-how-to-analyze-password-lists-for-security-risks-in-cybersecurity-414529
40. (PDF) An analysis of password security risk against dictionary attacks, erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/366191170_An_analysis_of_password_security_risk_against_dictionary_attacks
41. Why multi-factor authentication is absolutely essential in 2025 - ZDNet, erişim tarihi Haziran 20, 2025, https://www.zdnet.com/article/why-multi-factor-authentication-is-absolutely-essential-in-2025/
42. Best Authentication Method for Your Business in 2025 | Paramount, erişim tarihi Haziran 20, 2025, https://paramountassure.com/blog/best-authentication-method-for-your-business-in-2025/
43. Essential Password Security Tips for 2025 - London Computer ..., erişim tarihi Haziran 20, 2025, https://www.lcs.com/2025/05/13/essential-password-security-tips-for-2025/
44. AI is coming for your passwords – better make them strong - Cybersecurity Insiders, erişim tarihi Haziran 20, 2025, https://www.cybersecurity-insiders.com/ai-is-coming-for-your-passwords-better-make-them-strong/
45. (PDF) Adversarial Machine Learning for Robust Password Strength ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/392335162_Adversarial_Machine_Learning_for_Robust_Password_Strength_Estimation
46. Adversarial AI for Password Security and Analysis in Digital ..., erişim tarihi Haziran 20, 2025, https://www.port.ac.uk/study/postgraduate-research/research-degrees/phd/explore-our-projects/adversarial-ai-for-password-security-and-analysis-in-digital-investigations
47. The best password generators of 2025: Expert tested | ZDNET, erişim tarihi Haziran 20, 2025, https://www.zdnet.com/article/best-password-generator/
48. Best Password Managers for AI Threat Protection in 2025 | iFeeltech, erişim tarihi Haziran 20, 2025, https://ifeeltech.com/password-managers-ai-threat-protection-comparison/
49. Top Password Managers for 2025: A Quick Review | Galaxy.ai, erişim tarihi Haziran 20, 2025, https://galaxy.ai/youtube-summarizer/top-password-managers-for-2025-a-quick-review-YNkQkoChcKA